

**FINAL DRAFT**

# **INDIAN HEALTH SERVICE**



## **ENTERPRISE ARCHITECTURE**

**Version 4.0**

**August 22, 2001**

**Fiscal Year 2002 Plan**

**FINAL DRAFT**

modified 08/23/01

# FINAL DRAFT

## EXECUTIVE SUMMARY

The Indian Health Service (IHS) is developing an Enterprise Architecture (EA) as an integrated framework to align IHS information technology (IT) maintenance, development, and acquisition activities with IHS strategic business and information resource management goals and objectives. Therefore, this IHS EA applies to all IT activities performed and all assets deployed throughout IHS, including all information systems, software products, and infrastructure that support IHS management and operations.

This EA 2002's objectives are to do the following:

1. Institute an adaptive architecture that supports the IHS business mission, strategy, processes, and requirements
2. Provide a blueprint to help the Chief Information Office (CIO) evaluate existing and proposed IT investments, and plan and manage future IT acquisitions
3. Meet Clinger-Cohen Act of 1996 requirements and related Office of Management and Budget (OMB) expectations
4. Support and conform to the strategic vision, business objectives, and EA principles and guidelines documented in the EA of IHS' parent agency, the Department of Health and Human Services (DHHS)
5. Develop an IHS EA compatible with the technology directions proposed in the EAs of the Veteran's Administration (VA) and the Health Care Finance Administration (HCFA), two Federal agencies with which IHS has formed key partnerships

Specifically, this document does the following:

- Presents a high-level architectural vision of a future IHS EA
- Identifies tactical initiatives for strategic investment that support the architectural vision
- Establishes a reference architecture model for IHS
- Aggregates and establishes a set of broadly applicable technical and security standards
- Presents a set of architectural models that depict the technical, operational, data, and systems environments
- Provides guidance and recommendations for future development efforts to ensure their consistency with the architecture

Developing and refining this EA is an ongoing process. In addition, the IHS EA will influence, and be influenced by, IHS business plans, IT strategic initiatives, and specific implementation plans. New versions of the EA will be released annually, or as organizational and technology changes mandate.

# FINAL DRAFT

## TABLE OF CONTENTS

<b>EXECUTIVE SUMMARY</b> .....	<b>I</b>
<b>TABLE OF CONTENTS</b> .....	<b>II</b>
<b>INDEX OF EXHIBITS</b> .....	<b>VI</b>
<b>INTRODUCTION</b> .....	<b>1</b>
EA Definition, Purpose, and Benefits .....	3
Scope .....	3
Document Organization and Summary .....	5
Overview .....	6
Guiding Principles .....	7
<b>DIRECTION</b> .....	<b>18</b>
Future Business Views .....	18
DIR Vision, Goals, and Strategies .....	21
Business Drivers .....	26
Technology Drivers .....	28
Legislative Drivers .....	29
RPMS Growth Plan .....	32
Phase 1 .....	35
Phase 2 .....	38
Phase 3 .....	39
Phase 4 .....	39
<b>FRAMEWORK</b> .....	<b>40</b>
Critical EA Attributes .....	40
Health Care Information Principles .....	42
Health Care Information Infrastructure .....	43
IHS Technical Reference Model .....	48
Definition of Standards and Products .....	50
Purpose of Standards and Products .....	51
Benefits of Standards and Products .....	51
Overview of Standards .....	57
System Services .....	57
Communications Services .....	58
Information Services .....	62
Security Services .....	72
<b>CURRENT ENVIRONMENT</b> .....	<b>76</b>
Current Business Architecture .....	76
IHS Network Architecture .....	76
Details of the Network Architecture .....	79
Application Software Environment .....	82
RPMS Software Architecture & Environment .....	83
Operational Environment .....	87
NPIRS Software Architecture .....	90
RPMS Processing Platform Environment .....	90
IHS RS/6000 Configuration Overview .....	90

# FINAL DRAFT

<b>NEW &amp; EMERGING TECHNOLOGIES</b> .....	<b>96</b>
process improvement .....	96
Achieving IHS Goals by Implementing Data Management Practices.....	100
Distributed Architecture .....	101
Microsoft Tier Architecture.....	103
OMG Tier Architecture .....	104
Component-Based Software Engineering (CBSE).....	105
Internet Inter-ORB Protocol (IIOP).....	106
Storage Services .....	106
Semantics and Terminologies .....	112
Interface Technologies .....	114
XML-based Web Services Platform: Microsoft's NET.....	118
Service-based Architecture.....	123
Networking.....	124
Software Development Life Cycle Support .....	126
Operations and Maintenance.....	129
Secure Technologies .....	131
<b>IT PLAN</b> .....	<b>136</b>
Major Architectural Attributes.....	136
Patient Health-centered .....	136
Service-oriented.....	137
Standards-based .....	138
Secure .....	138
Component-based .....	139
Web-enabled .....	139
EIM-based .....	140
Target Business Architecture.....	142
IHS Technical Architecture Strategy .....	143
Enterprise Infrastructure Management .....	144
Information Presentation.....	147
Security.....	147
Integration Strategy .....	148
Information Representation .....	153
Network Architecture .....	154
Strategic Projects.....	157
Project Areas .....	157
Project Evaluations and Rankings .....	158
Data Representation Project Profiles.....	161
Data Exchange Project Profiles .....	165
Systems and Applications Project Profiles.....	169
Enterprise Infrastructure Management Project Profiles .....	175
<b>APPENDIX A - IT SECURITY ARCHITECTURE PLAN</b> .....	<b>177</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>178</b>
<b>TABLE OF CONTENTS</b> .....	<b>179</b>
<b>TABLE OF EXHIBITS</b> .....	<b>183</b>
<b>INTRODUCTION</b> .....	<b>184</b>
Scope .....	184

# FINAL DRAFT

Model.....	184
Document Use and Content .....	184
<b>POLICIES, PRINCIPLES, AND RESPONSIBILITIES .....</b>	<b>186</b>
IHS Security Principles .....	186
Security Architecture Policies .....	187
Privacy and Security .....	189
Agency Responsibility .....	191
Security Responsibilities .....	191
IHS Chief Information Officer (CIO).....	191
IHS and Area Information System Security Officers (ISSO).....	192
Area Director .....	192
Area Information Systems Coordinator (ISC).....	193
Subordinate ISSO .....	193
System Owner/Custodian.....	193
Records Management Officer .....	194
Privacy Act Officer/Coordinator .....	194
<b>ENVIRONMENT AND CURRENT ARCHITECTURE.....</b>	<b>195</b>
Information Users .....	195
Information Resources.....	196
Risks and Threats.....	196
Summary of Current Security Architecture and Business Requirements.....	198
<b>TARGET ARCHITECTURE .....</b>	<b>199</b>
Technical Protection Measures .....	199
Public Key Infrastructure (PKI) .....	199
Virtual Private Networks (VPN) .....	200
Confidentiality, Integrity, and Availability Services .....	200
Standards.....	204
Physical Protection, Contingency Planning, and Disaster Recovery .....	204
Physical Protection.....	205
Business Continuity and Contingency Planning (BCCP).....	205
Administrative Security, Personnel Security, and Procedures .....	205
Logging and Auditing .....	206
Training and Awareness .....	207
Incident Detection and Response Capability .....	208
<b>ARCHITECTURE MAINTENANCE AND COMPLIANCE .....</b>	<b>210</b>
Architecture Management.....	210
Architecture Compliance.....	211
<b>SUMMARY .....</b>	<b>212</b>
<b>SOURCES .....</b>	<b>213</b>
<b>HIPAA SECURITY SERVICES .....</b>	<b>214</b>
HIPAA Security Requirements.....	214
1. Administrative Procedures .....	214
2. Physical Safeguards .....	215
3. Technical Security Services.....	216
4. Technical Security Mechanisms .....	217
HIPAA Electronic Signature Requirements.....	217

**FINAL DRAFT**

**APPENDIX B - GLOSSARY OF TERMS .....218**  
**APPENDIX C-ACRONYMS.....265**

# FINAL DRAFT

## INDEX OF EXHIBITS

<i>Exhibit 1-1: IHS EA Guiding Principles.....</i>	<i>8</i>
<i>Exhibit 2-1: IHS Vision: Goals and Objectives.....</i>	<i>22</i>
<i>Exhibit 2-2: IT-Related Legislation.....</i>	<i>30</i>
<i>Exhibit 2-3: RPMS Information Exchange.....</i>	<i>34</i>
<i>Exhibit 3-1: HII Functional Services Model.....</i>	<i>45</i>
<i>Exhibit 3-2: IHS Technical Reference Model.....</i>	<i>48</i>
<i>Exhibit 3-3: Summary of TRM.....</i>	<i>50</i>
<i>Exhibit 3-4: Summary of Standards.....</i>	<i>53</i>
<i>Exhibit 4-1: IHSNET Backbone Network.....</i>	<i>78</i>
<i>Exhibit 4-2: Summary Level of IHS Network Architecture.....</i>	<i>79</i>
<i>Exhibit 4-3: AO-to-Health Care Facility Configurations.....</i>	<i>81</i>
<i>Exhibit 4-4: RPMS Components by Category and Site Type.....</i>	<i>84</i>
<i>Exhibit 4-5: RPMS File Relationships.....</i>	<i>89</i>
<i>Exhibit 4-6: Class I System Major Components.....</i>	<i>91</i>
<i>Exhibit 4-7: Class I System Minimum Configuration.....</i>	<i>92</i>
<i>Exhibit 4-8: Class I System Expanded Configuration.....</i>	<i>93</i>
<i>Exhibit 5-1: SW-CMM Maturity Levels &amp; Key Process Areas.....</i>	<i>97</i>
<i>Exhibit 5-2: CMM Maturity Levels and Key Process Areas.....</i>	<i>99</i>
<i>Exhibit 5-3: Tiered Architecture.....</i>	<i>102</i>
<i>Exhibit 5-4: Simple COM+ Application.....</i>	<i>104</i>
<i>Exhibit 5-5: Object Request Broker.....</i>	<i>105</i>
<i>Exhibit 5-6: Layered Decision Support Framework.....</i>	<i>107</i>
<i>Exhibit 5-7: Enterprise Data Warehouse (EDW) Process.....</i>	<i>109</i>
<i>Exhibit 5-8: EDW Logical View.....</i>	<i>109</i>
<i>Exhibit 5-9 Microsoft .NET Architecture.....</i>	<i>118</i>
<i>Exhibit 6-1: Components of EIM.....</i>	<i>141</i>
<i>Exhibit 6-2: HHS EIM Conceptual Architecture.....</i>	<i>146</i>
<i>Exhibit 6-3: IHS Notional Architecture.....</i>	<i>148</i>
<i>Exhibit 6-4: Conceptual Model of IHS National Data Warehouse.....</i>	<i>150</i>
<i>Exhibit 6-5: Future Movement of Data Within IHS.....</i>	<i>151</i>
<i>Exhibit 6-6: COM/CORBA Bridging.....</i>	<i>152</i>
<i>Exhibit 6-7: Document Management Architecture.....</i>	<i>154</i>
<i>Exhibit 6-8: IHS Network Architecture.....</i>	<i>155</i>
<i>Exhibit 6-9: Project Evaluations and Rankings.....</i>	<i>160</i>
<i>Exhibit 6-10: Strategic Projects.....</i>	<i>161</i>
<i>Exhibit A-1 Data Flow Types.....</i>	<i>196</i>

## INTRODUCTION

The Indian Health Service (IHS), a federal agency of the United States Public Health Service (USPHS), Department of Health and Human Services (DHHS), is responsible for delivering health services to federally-recognized American Indians and Alaska Natives (AI/AN) through a system of IHS, Tribal, and Urban (I/T/U) operated facilities and programs based on treaties, judicial determinations, and Acts of Congress. The Agency's mission is to raise the physical, mental, social, and spiritual health of AI/AN to the highest level, in partnership with the population served. The Agency's goal is to ensure that comprehensive, culturally acceptable personal and public health services are available and accessible to the service population. The Agency's four strategic objectives reflect the mission and goal:

1. Improve health status
2. Provide health services
3. Assure partnerships and consultation with I/T/U programs
4. Perform core functions and advocacy

The I/T/U facilities and programs serve a population of 1.46 million AI/AN residing on or near reservations and an additional 400,000 AI in urban areas.<sup>1</sup> Close to 15,000 IHS employees, including both USPHS Commissioned Corps and civil service, work with 557 federally recognized tribes in 35 states, from Point Barrow, Alaska to Hollywood, Florida. Direct and contract patient care, although a mainstay of the community-based primary care system is only part of the picture. With tribal participation, IHS also provides environmental planning and maintenance services, builds and maintains clean water systems, carries out educational outreach and preventive health programs, and assists in groundbreaking research and applying scientific information.

The Indian Health system integrates health services delivered directly through IHS facilities, IHS purchased through contractual arrangement with private sector providers, and delivered through Tribally operated programs and urban Indian health programs. A decentralized system of 12 Area Offices (AOs) and 84 service units administer IHS direct health care services. The IHS operates 36 hospitals ranging from 11 to 170 beds, 63 health centers, 44 health stations, and five residential treatment centers. Indian tribes, who have elected to administer their own health services, deliver IHS-funded services to their own communities through 60 service units that encompass 13 hospitals, 158 health centers, 160 Alaska village clinics, 76 health stations, and 28 residential treatment centers.<sup>2</sup>

---

<sup>1</sup> *IHS Year 2000 Profile* (as of 6/1/2000), based on 1998-2000 data & 2001 budget request.

<sup>2</sup> *Ibid.*

Additionally, there are 34 urban health care projects, ranging from community health to comprehensive primary health care. In locations where the IHS does not have its own facilities, or is not equipped to provide a service, the IHS contracts with more than two thousand private providers, including local hospitals, State and local health agencies, and individual health care providers.

IHS' organizational structure is based on a Headquarters (HQ) operation and twelve AOs that administratively support health care delivery nationwide. The twelve AOs serve as regional management offices with jurisdiction over local health services delivery system operation. Local administrative units, called Service Units, are the basic health organizations for a geographic area served by IHS.

Within the IHS, the Division of Information Resources (DIR) manages, directs, and has overall oversight responsibility for Agency-wide IT requirements. DIR is split organizationally and geographically. The Chief Information Officer (CIO), located in Rockville, Maryland, is empowered with overall Agency management on all information technology aspects. The primary sub-division of DIR, the Information Technology and Support Center (ITSC), is the technical support operation located in Albuquerque, New Mexico, with a small staff in Tucson, Arizona, and Rockville, Maryland.

IHS has an enormous, geographically dispersed client base for which it provides a comprehensive health services delivery system. Many reservations and Indian communities are located in isolated areas where impassable roads and populations spread over many miles challenge quality health care provision.

Extensive, effective, and efficient use of technology, particularly during periods of reduced funding, is critical to IHS successful mission achievement. A key activity is upgrading the DIR infrastructure and technological capabilities to improve and extend IT capabilities to all IHS sites; improve system performance and reliability; provide or augment office automation, electronic communications, and point-of-service data collection capabilities; and enhance IT users' skills and effectiveness.

## **EA DEFINITION, PURPOSE, AND BENEFITS**

---

The IHS EA is an integrated framework of principles, guidelines, and rules for aligning all IT development, maintenance, and acquisition activities with IHS business strategies, goals, and objectives, and IHS information resource management goals and objectives.

Four primary objectives are associated with this EA:

1. Institute an adaptive architecture that aligns with and enables IHS business requirements
2. Provide a blueprint to guide the CIO in planned and future work
3. Meet Clinger-Cohen Act requirements and related Office of Management and Budget (OMB) expectations
4. Demonstrate harmony between HHS' and IHS' EAs

Specifically, this document does the following:

- Presents a high-level architectural vision of a future IHS EA
- Identifies tactical initiatives for strategic investment that support the architectural vision
- Establishes a reference architecture model for IHS
- Aggregates and establishes a set of broadly applicable technical and security standards
- Presents a set of architectural models that depict the technical, operational, data, and systems environments
- Provides guidance and recommendations for future development efforts to ensure their consistency with the architecture

## **SCOPE**

---

This EA applies to all IHS personnel engaged in any activity associated with evaluating, developing, maintaining, or acquiring IHS IT assets. The DIR has overall responsibility to develop and maintain the IHS EA, including the following:

- Communicating the IHS IT direction and information contained in the EA to all IHS members and offices engaged in the evaluation, requirements analysis, development, operations and maintenance, and acquiring IT assets
- Assuring that the IHS EA reflects and supports IHS business requirements
- Evaluating IHS IT activities in terms of their support of and compliance with the IHS EA
- Coordinating IHS EA development and maintenance activities with other IHS offices responsible for IT assets

- Effecting a repeatable process to solicit stakeholder feedback and continuously improve the EA
- Coordinating the annual EA review and update with IHS offices responsible for IHS IT assets
- Establishing and administering Change Management processes to assure that EA updates are reviewed, coordinated, and managed effectively
- Facilitating compliance with the Clinger-Cohen Act and other legislative mandates as they relate to the EA
- Disseminating EA updates to all IHS offices responsible for IHS IT assets

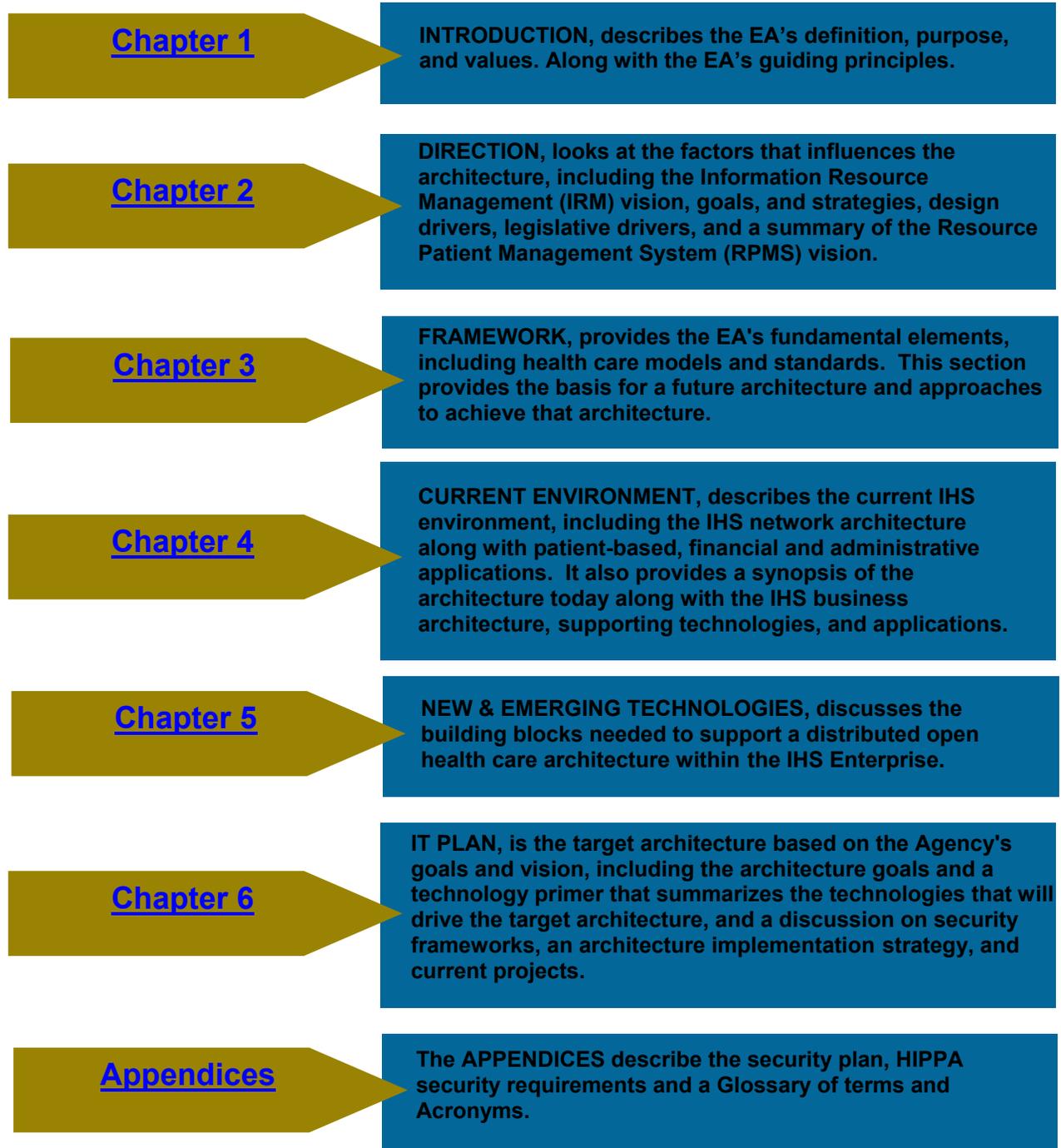
This IHS EA encompasses all IHS IT assets, including but not limited to the following:

- IHS-developed applications and systems
- VA-developed applications and systems
- Commercial-off-the-shelf (COTS) products
- Applications and systems acquired through sharing agreements
- Corporate applications information systems
- Network, communications, hardware, and software infrastructures

## DOCUMENT ORGANIZATION AND SUMMARY

---

This IHS EA is organized into the following chapters:



## OVERVIEW

---

The 2002 to 2004 IHS *Information Resources Management (IRM) Plan* conforms to guidance set forth in the Department of Health and Human Services (DHHS) call for five-year IRM Plan and other DHHS- and OMB-issued guidance. The IRM Plan will be linked to strategic and performance objectives and activities. The Resource Patient Management System (RPMS) will support performance indicators in the *IHS Annual Performance Plan* by collecting support data in the National Patient Information Reporting System (NPIRS). The IHS DIR program's core challenge is to align IT products and services with Agency mission and direction, whose strategies largely depend on IT.

Technology improvements and implementation are affecting how IHS is realizing its strategic objectives. It is increasingly evident that expanding the use of IT has the potential to allow the IHS to do more with less at all levels. Equally significant, technology improvements are accruing benefits in treating and preventing diseases. Such improvements in consumer services have already been demonstrated through applied research in IHS and tribal clinics in collaboration with several research institutions, and the potential for more collaboration is very real. For instance, the impact of a break-through technology to prevent or control diabetes could be significant, both economically and in terms of reducing human suffering.

In the most fundamental ways, IT is transforming how we work. Front-line workers access vast information quantities instantaneously. Decision support systems take employees through complex decision trees and logic. Customers access remote information directly through integrated voice response systems, electronic bulletin boards, and the World Wide Web. Senior executives communicate instantly with their entire staffs, without going through intermediate management layers. Moreover, IT enables radical and fundamental change in business processes.

The Indian Health System is moving into a new information systems environment because of the following:

- The tribal program takeover and the associated tribal option whether or not to report the same program data into the IHS central database as IHS providers report
- New reporting requirements mandated by other federal agencies, such as the HCFA and the States
- Changing information technologies

Accordingly, the IHS plan is to develop new information systems strategies and policies. Therefore, the current IHS information structure and network will change in the next 5 years, which will probably change how Government Performance and Results Act (GPRA) measures are calculated.

IT is mission critical and expensive. IT investments, especially with constrained resources, must be treated as major business decisions. Senior executives must make these decisions using a comprehensive and integrated capital planning and budgeting process and sound economic analysis. They must establish clear performance goals and measure progress against them to maintain accountability and ensure that these expensive investments achieve IHS' goals.

## **GUIDING PRINCIPLES**

---

The IHS EA is founded upon ten principles that govern IHS EA and related processes development, evolution, maintenance, and management. Therefore, adhering to these principles is one criterion against which all IT initiatives, such as analyzing, developing, maintaining, operating, and acquiring software applications, information systems, network and communications infrastructure, will be evaluated.

Exhibit 1-1, IHS EA Guiding Principles, lists the ten principles, describes each principle, and provides each principle's rationale and implications.

**Exhibit 1-1: IHS EA Guiding Principles**

<b>PRINCIPLE 1</b>	<b>THE IHS EA WILL SUPPORT IHS' STRATEGIC GOALS AND OBJECTIVES.</b>
<b>DESCRIPTION</b>	<p>Enterprise-wide, within the context of the IHS EA, includes all IT capital assets (hardware, software, licenses, &amp; interfaces) and services existing within the boundaries of the IHS enterprise.</p> <p>Establishing a common vision among the IT and business components across the Enterprise necessitates unifying the EA's planning, management, and governance.</p> <p>Maintaining a strategic EA outlook to support the IHS strategic business plans. The strategic plan defines the goals for IHS business, a set of objectives describing the direction in which we are headed, and the broad strategies we are using to attain these goals. Establishing long-term IT goals and objectives as part of the IHS strategic EA outlook is necessary to ensure proper business and IT alignment.</p>
<b>RATIONALE</b>	<p>In accordance with the Clinger-Cohen Act and subsequent OMB guidance, the EA ensures that IT investments are aligned with IHS' mission and goals. It further stipulates that IT investments must be technically aligned with the EA to promote interoperability and resource sharing.</p>
<b>IMPLICATIONS</b>	<p>Adhering to this principle will allow IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Play a strategic and vital role in health care</li> <li>• Have an Agency-wide, business-aligned, and integrated EA to fulfill its mission</li> <li>• Make strategic investment decisions</li> <li>• Increase interoperability, standardization, and operational effectiveness</li> <li>• Reduce long-term IT costs</li> <li>• Link IT to the business functions the Clinger-Cohen Act requires</li> <li>• Improve Enterprise data quality and give users easy access to that data</li> <li>• Share responsibility for deploying, operating, and managing technology with all components and stakeholders</li> <li>• Ensure operational effectiveness by investing in IT consistent with Clinger-Cohen Act requirements &amp; DHHS and OMB guidance (managing IT assets and expenditures at the Enterprise level)</li> <li>• Ensure business unit participation in evaluating and making IT investment decisions using consistent criteria</li> <li>• Share data, training, and tools across the Enterprise, thereby limiting potential effort duplication</li> <li>• Maximize IT resources use across the Enterprise and support a single Enterprise-wide EA</li> </ul>

<b>PRINCIPLE 2</b>	<b>DATA WILL BE ENTERED, EDITED, AND AGGREGATED CONSISTENTLY.</b>
<b>DESCRIPTION</b>	The probability of ensuring the accuracy of IHS data improves in inverse proportion to the number of data entry points; the smaller the number of data entry points the lesser the likelihood for introducing error or redundancy to the data.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• It is expensive to enter data more than once. The labor associated with data entry and quality control on an individual field is small, but when several systems are factored in over several years, IT becomes expensive.</li> <li>• With multiple entries of the same data from different sources, a question of which data source is correct or accurate arises.</li> <li>• Capturing data accurately at a single point is helping IHS move away from paper processes. Data important to completing the process are immediately available within the automated process support systems, reducing the need for important data to be kept in other forms, such as photocopies, facsimiles, handwritten notes, or creating printouts for re-entry into another information system.</li> <li>• With current information technologies, such as bar coding, relational databases, and electronic data interchange, exchanging data and information is relatively easy.</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Redundant data entry is eliminated, reducing data entry errors</li> <li>• Confidence in the data and quality is enhanced</li> <li>• Overall data entry and maintenance costs are reduced</li> <li>• The organization that enters the data has stewardship of the quality standard</li> </ul>

<b>PRINCIPLE 3</b>	<b>IHS WILL IMPLEMENT AN EA THAT DELIVERS DATA IN A TIMELY MANNER TO AUTHORIZED USERS, SYSTEMS, AND OTHER RECIPIENTS.</b>
<b>DESCRIPTION</b>	The value of the data resides not only in their accuracy but also in their timely availability.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Shared data are essential to the successful coordination of operations of the enterprise.</li> <li>• Timely access to data and information is essential for business operations.</li> <li>• Data accuracy and consistency enable optimal decision-making. People need access to the broadest range of information possible within the constraints of Agency policy and applicable law.</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Must determine how to apply the principle to other agencies and the public, which provides data to IHS</li> <li>• Deploy technology and give IHS employees access to information</li> <li>• Clearly state information classification; clearly define and publicize rules. Protect sensitive or confidential information in accordance with public laws and Agency policies</li> <li>• Consider shared data security</li> <li>• Expand the IHS library to provide a shared data central repository</li> <li>• Inter-OpDiv/Office collaboration and cooperation is necessary for data sharing</li> <li>• Centralize or distribute processes and resources. If data are stored in program areas where they are entered and validated, additional resources, such as backup capabilities and an uninterruptible power supply, may be needed to ensure availability to distributed systems.</li> <li>• Non-IHS participants' data formats may need to be considered.</li> </ul>

<b>PRINCIPLE 4</b>	<b>DEVELOP AND IMPLEMENT IT PROJECTS USING A COMMON SET OF METHODS, TOOLS, AND TECHNIQUES.</b>
<b>DESCRIPTION</b>	IHS IT projects must be developed, implemented, and operated using standard, Enterprise-wide policies, methods, tools, and techniques.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Maximize IT resources sharing benefits, such as people, hardware, design techniques, tools, languages, and documentation</li> <li>• Provide a comprehensive picture of resource use throughout the IT project development life cycle</li> <li>• Implement repeatable software development processes; promote re-deploying staff with minimal re-training, and minimize IT development, implementation, and maintenance costs</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Train staff and adjust resources to make them consistent with adopted methodologies</li> <li>• Change the organizational culture to embrace adopted methodologies</li> <li>• Employ modern systems development methods, such as rapid applications development and object-oriented design, tools, and techniques in addition to traditional structured practices</li> <li>• Document and promulgate adopted methodologies</li> <li>• Conduct methodology compliance reviews and use sanctions for non-compliance with established methodologies</li> <li>• Plan and budget for increased up-front development costs and time</li> </ul>

<b>PRINCIPLE 5</b>	<b>ADOPT OPEN SYSTEMS STANDARDS.</b>
<b>DESCRIPTION</b>	Open systems standards provide the best means to develop applications such that both the design and system implementation are independent of a specific vendor's hardware or software platforms. Products and technologies that are compliant with open systems standards use interface specifications that are readily available to all suppliers, service providers, and users, and are revised only with timely notice and public process. Open systems standards allow for continued access to technological innovation supported by many customers and a broad IT industry base.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Promote interoperability and take advantage of lower costs resulting from vendor competition to differentiate their products within the standards framework</li> <li>• Easily adapt technology solutions to satisfy changing business requirements while lowering the total cost of IT ownership</li> <li>• Provide IT solutions that are less susceptible to obsolescence</li> <li>• Employ standards that expand technology solution choices, thereby reducing dependence on single-vendor solutions</li> <li>• Design and develop application software components for reusability</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Focus on standards selection as the basis to select products and establish processes to evaluate products for standards compliance</li> <li>• Carefully track Federal and commercial IT industry standards development and evolution and their vendor product implementations</li> <li>• Formulate a workable, prioritized migration strategy to adopt and deploy IT using Federal and industry standards</li> <li>• Identify criteria to select products where no standards have been established; avoid implementing proprietary IT solutions unless they are key to providing critical business functionality and no acceptable standard or product alternative exists</li> <li>• Incorporate standards requirements into acquisition processes</li> <li>• Accept sub-optimization of product selections in favor of open systems standards</li> <li>• Establish policies, standards, and procedures to promote sharing and re-use of source code, application designs, and documentation</li> <li>• Identify the re-usable portions of application logic as distinct from logic specific to particular business processes</li> </ul>

<b>PRINCIPLE 6</b>	<b>ENABLE THE AUTOMATED, ACTIVE DELIVERY OF INFORMATION ACROSS THE ENTERPRISE.</b>
<b>DESCRIPTION</b>	Dynamic delivery of important information to a user's desktop is more efficient than requiring users to search for information. Users could subscribe to data services and receive information as soon as it becomes available. Software distribution and installation across the Enterprise could also be automated.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Enhance IHS' communication and information dissemination capabilities</li> <li>• Tailor information to the needs of specific individuals or user groups, thereby optimizing knowledge sharing</li> <li>• Give users information as soon as it becomes available, rather than requiring them to request the information</li> <li>• Provide reliable, current information, thereby enhancing IHS' program management decision-support capability</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires that IHS do the following:</p> <ul style="list-style-type: none"> <li>• Identify user information-access requirements that are best supported using an automated model</li> <li>• Define data stewards' roles and responsibilities to disseminate information</li> <li>• Implement adequate security mechanisms to ensure that users receive data and information only to which they are authorized</li> <li>• Develop policies and standards to disseminate information automatically and invest in appropriate IT infrastructure enhancements to implement the technology</li> </ul>

<b>PRINCIPLE 7</b>	<b>MANAGE INFORMATION AND DATA AS ENTERPRISE-WIDE ASSETS.</b>
<b>DESCRIPTION</b>	IHS program operations produce vast amounts of data that must be managed. This massive data management effort provides the raw material for creating valuable information to support a variety of management, analytical, and research needs throughout the Enterprise. Managing information and data as Enterprise-wide assets places greater significance on cooperative strategies for satisfying the common information needs of multiple business units across the Enterprise, rather than exclusively satisfying parochial component requirements.
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Foster information and data sharing, timeliness, and data integrity; increase sensitive information and data security and protection</li> <li>• Optimize resource use while eliminating redundant data management costs</li> <li>• Increase the quality and consistency of data and information used to support IHS programs</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Clarify the roles and expectations for stewards of Enterprise information and data</li> <li>• Clarify management policies and procedures to identify and classify Enterprise information and data and standardize access and security procedures</li> <li>• Encourage the cultural changes to evolve an Enterprise-wide information and data management environment</li> <li>• Implement an infrastructure that permits authorized access to information and data Enterprise wide; establish an Enterprise information resource catalogue of formal data assets, such as an Master Person Index (MPI), drug reaction data, and statistical data to support decision support activities</li> <li>• Employ aggressive safeguards to protect information and data security and privacy</li> <li>• Enhance the infrastructure to support advanced technologies for metadata management, data replication, and secure computing over the Internet; plan and budget for potentially increased costs to establish an Enterprise-wide data management infrastructure</li> </ul>

<b>PRINCIPLE 8</b>	<b>USE COTS OR GOVERNMENT OFF THE SHELF (GOTS) PRODUCTS EXCEPT FOR WHEN CUSTOM-DEVELOPED SOFTWARE IS COST OR MISSION-JUSTIFIED.</b>
<b>DESCRIPTION</b>	Preference will be given to acquiring COTS/GOTS software products in lieu of developing custom application solutions to business requirements. COTS and GOTS products can range in size and functionality from component functions that plug into the existing systems infrastructure, to entire application systems, to Enterprise resource systems. Industry trends toward increased software development costs are likely to continue, and the appropriate use of COTS and GOTS products is one way to acquire needed IT capabilities cost effectively. Where using existing components is both possible and feasible, it is no longer acceptable for Federal agencies to specify, build, and maintain comparable custom solutions.
<b>RATIONALE</b>	The following form the rationale for this principle: <ul style="list-style-type: none"> <li>• Enhance IHS' business and mission effectiveness by exploiting technology solutions that are widely available to customers, partners, and stakeholders</li> <li>• Leverage previous and future investments of public and private sector resources that are committed to providing working IT solutions for common business needs</li> <li>• Ease software maintenance burden, and reduce software development risk</li> <li>• Benefit from the continually expanding variety of COTS and GOTS technology solutions becoming available to all users</li> </ul>
<b>IMPLICATIONS</b>	Adhering to this principle requires that IHS do the following: <ul style="list-style-type: none"> <li>• Define software development methods and practices for IT staff to incorporate COTS and GOTS considerations into systems life-cycle processes</li> <li>• Re-train and re-tool IT staff to use new COTS-and GOTS-related skills</li> <li>• Define systems development life-cycle processes and procurement standards to be consistent with this principle</li> <li>• Define IT investment decision criteria to weigh more favorably funding for IT projects that employ COTS or GOTS solutions; acquire only those COTS and GOTS products that incorporate open systems standards-compliant interfaces; avoid the increased risk and cost associated with using purchased products that require changing the source code to be implemented</li> <li>• Acquire COTS and GOTS products only from stable, reliable vendor sources</li> <li>• Participate in user groups to influence product enhancements and priorities</li> <li>• Establish a comprehensive product-evaluation process to ensure that candidate solutions satisfy business requirements</li> <li>• Give up a measure of control and accept the risk of vendor product changes</li> </ul>

<b>PRINCIPLE 9</b>	<b>MIGRATE LEGACY AND EXISTING CLIENT SERVER APPLICATIONS TO WEB BASED TECHNOLOGIES.</b>
<b>DESCRIPTION</b>	<p>In a client/server model, application processes are divided among two or more logically partitioned environments, typically a client system, such as a program or intelligent workstation, and a server system. Client and server hardware and software components tend to be specialized to perform their functions, and typically introduce complexities such as software standardization, version control, and high bandwidth applications. When client/server computing is performed with distributed computing platforms over geographically dispersed locations connected by wide area networks, performance can be degraded, and these proprietary applications often require specialized ports and protocols to effectively communicate.</p> <p>The Internet and its related web-based technologies account for the most significant advances in information systems in the last 5 years. The Internet, Intranets, and Extranets offer new channels for enhanced communication directly between customers and suppliers. The rapid evolution of web-based technologies, introduction of more powerful servers and storage area networks, all provide compelling reasons to migrate legacy client-server applications to web based applications. In addition to simplifying existing complex business processes, the use of web technologies sets conditions for success through the use of a standard methodology for authentication, authorization and strong encryption. Where feasible, IHS will incorporate using secure web-based technologies when developing IT solutions.</p>
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Enhance information dissemination to customers, stakeholders, and partners</li> <li>• Associated cost reductions in software and reduced bandwidth utilization with the consolidation and migration of legacy client server applications to web based applications.</li> <li>• The opportunity for storage standardization, simplified authentication, authorization, and data integrity through the use of high encryption.</li> <li>• Web based applications simplify server administration and reduce expensive 'touch labor' costs associated with client server applications.</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires that IHS do the following:</p> <ul style="list-style-type: none"> <li>• Obtain IHS management approval and explicit endorsement that legacy client server applications will be migrated to web based technologies.</li> <li>• Identify ALL existing client server applications, level of effort required to migrate, and prioritize applications.</li> <li>• Develop a feasible project plan and timeline for migration, directly associated with allocated fiscal resources and skill sets.</li> </ul>

<b>PRINCIPLE 10</b>	<b>ENSURE ENTERPRISE-WIDE INTEGRATION OF IT SECURITY.</b>
<b>DESCRIPTION</b>	<p>Every IHS employee, agent, and business partner is responsible for security. Federal regulatory mandates and directives require IHS to implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of sensitive data and information against unauthorized access and use. IHS must protect the sensitive data and information it collects against anticipated threats or hazards that could result in substantial harm to any individual on whom the information is maintained. Without an integrated approach to security implementation, IHS cannot ensure that its policies, procedures, and technologies adequately protect the Enterprise against security threats.</p>
<b>RATIONALE</b>	<p>The following form the rationale for this principle:</p> <ul style="list-style-type: none"> <li>• Fulfill the requirement to safeguard sensitive information</li> <li>• Develop a comprehensive approach to security design and implementation adequate for the scope of a broadly distributed, networked environment, and IHS Business Enterprise</li> <li>• Provide access to information and data to authorized persons only, regardless of where they are located within the Enterprise</li> <li>• Improve auditing and accountability of access to sensitive data and information; uniformly implement security standards Enterprise wide</li> <li>• Use an Enterprise-wide approach to exploit available and emerging technologies to strengthen security</li> </ul>
<b>IMPLICATIONS</b>	<p>Adhering to this principle requires IHS to do the following:</p> <ul style="list-style-type: none"> <li>• Develop Enterprise-wide security implementation strategies</li> <li>• Define Enterprise-wide, consistent roles, responsibilities, and expectations for system managers, application developers, and security administrators</li> <li>• Develop programs to test security implementation measures effectiveness</li> <li>• Continually monitor the Enterprise for vulnerabilities and threats/risks as the IT environment evolves over time</li> <li>• Identify industry best practices for integrating systems security technology, methods, and procedures consistently throughout the Enterprise</li> <li>• Plan for the increased cost of implementing an Enterprise-wide security strategy</li> </ul>

## **DIRECTION**

This chapter examines the factors and forces that influence the EA, including IHS core business views; IHS DIR vision, goals, and strategies; business drivers; design drivers; legislative drivers; and the RPMS' planned evolution.

The future business views discussion describes the various ways data will be viewed within the Enterprise and who will view the information. The business views represent functional roles for which the EA was developed. The discussion on the DIR vision, goals, and strategies describes the Agency's obligation to establish an automated information system to facilitate health care delivery to the I/T/Us. Business drivers are discussed because the way the Agency performs its business impacts health care delivery. A discussion on design drivers highlights some EA technical goals.

Legislation drives how the Agency handles information; a discussion is provided to describe current EA-impacting legislation. Legislation that influences the EA mandates standards for health care data transmission and data protection.

RPMS is the Agency's core application and its use with distributed technologies is being extended. It must be accounted for as a driving force within the EA.

## **FUTURE BUSINESS VIEWS**

---

Business views set the stage for the Agency's architectural goals. They define who views data and how they view it. The Agency has shaped an architectural framework to reflect its missions and goals.

### **Patient View**

Patients are increasingly interested in getting involved with their medical care, and technology will increasingly enable patients to take a more active role in their own health care. Personalized access to on-line preventive and health care information will be provided to patients based on individual preferences and characteristics, including age, gender, and past medical history. Information on topics such as exercise, diet, diseases, drugs, and treatments will educate and empower patients. Preventive and health care knowledge sources will be rated to increase the use of credible information. On-line preventive and health care information will be combined with a patient's own health care information, including test results and treatment plans. Patients will have increased access to, and control of, their integrated longitudinal medical records.

## **Clinical View**

Technology gives physicians, nurses, and other clinical staff access to integrated, longitudinal patient records. Fundamental medical concepts will be presented in terms that have meaning and integrity to a clinician, based upon local standards and in locally accepted terms. Providers will be able to integrate various data and records and provide a complete view of the patient's health care. Integrated, seamless access to patient data will be provided across each point of care, independent of organizational or geographic boundaries.

Clinical staff are also being empowered with decision support tools, such as clinical repositories and data warehouses, to assist in diagnosis, predictions, and care recommendations. Physicians will be able to determine treatment outcomes and practice preventive medicine, in addition to obtaining guidelines on practice management and credentialing. Clinical practice guidelines will be provided at the point of care when the clinical decision-making process occurs. Providers will have electronic capabilities to verify insurance and eligibility, order tests and receive results, submit claims, and manage referrals. Physicians will also have the ability to offer remote “teleconsultation” to health management teams. The trend toward using pervasive devices, such as smart phones, Personal Digital Assistants (PDAs) and laptops, will continue to provide clinicians with location independence and connectivity to knowledge bases. Electronic prescriptions and continuous speech recognition services will be offered as an alternative to data entry by hand, especially in clinical settings such as operating rooms and radiology.

Collaboration services bridge the gap created by the physical distance separating users. Collaboration is an essential aspect of any service because it promotes social interaction and person-to-person information exchange. This service enables remote consultation sessions among health care professionals to compensate for the lack of experienced or specialized personnel, to address emergency situations, to evaluate the severity of a situation, etc. It effectively makes expertise a shared resource, wherever it exists. Telemonitoring services also establish collaboration between the patient and physician and enable health care delivery at the patient's home. Thus, patients receive timely attention, while reducing the operational costs of health care centers. Furthermore, for community care, collaboration among user groups that share the same chronic medical condition may provide comfort by sharing information and experience.

## **Administrative View**

Decision support services allow access to the distilled knowledge of digital libraries and specific medical procedures. Services in this class include a registered pharmaceutical company-provided drug interaction service, access

to diagnostic databases and epidemiological studies and reports, and evaluation tools and methods that special instruments can provide. Usually, specialized systems located at referral health care facilities provide these services. Despite their importance, small health care centers cannot afford these services, even though they may be critical in treating geographically isolated patients. Remote access to these services is usually restricted and charged. These services may be offered through an advanced network of digital medical libraries.

### **Financial View**

IHS will leverage business-to-business, electronic marketplace, and business-to-consumer infrastructures to reduce long-term costs and improve the quality of health care delivery systems. Such applications include online prescription/non-prescription medication orders processing; reimbursements; and procuring medical services and supplies via on-line catalogues and bid-quote options. Participation in e-business networks, including health networks with partners, such as HCFA, will result in lower transaction costs and personnel resource requirements because verifying eligibility, coordinating benefits, and paying claims will be performed electronically. IHS procurement specialists will be able to order supplies online; inventory systems will automatically generate orders for critical or frequently-used supplies when inventory levels reach designated levels; and suppliers, based on IHS inventory levels, consumption, and demographic data, will supply orders timely and cost effectively. IHS and Tribe financial staff will use decision support tools, such as data warehouses, to perform financial modeling, manage costs, manage contracts, and develop strategic plans.

### **Research View**

Basic clinical and outcomes research will be supported to prevent adverse effects and to improve clinical practice guidelines and deliver health care in general. Analytical tools will allow researchers to query, analyze, and discover patterns and relationships within large, integrated, clinical information repositories. This ability will allow doctors to diagnose and treat diseases as well as disability and restore function in veterans whom trauma or disease has disabled. The effects of population trending, such as diet, behavior, and aging, will be analyzed. Outcomes of groups of similarly afflicted patients treated with different drug regimens will be compared to determine which treatments statistically are most cost effective. In addition, studies will allow medical providers to predict the effects of diverse drug combinations and interactions.

### **Education View**

Health care professionals will be able to access the educational material of digital medical libraries. The public will be able to access information relevant to diseases common in their region. Medical students and health care

personnel should be allowed to interact with repositories of medical cases and remote teaching facilities. This increased access will improve health care for patients and the public, regardless of geographic location.

## **DIR VISION, GOALS, AND STRATEGIES<sup>3</sup>**

---

### **Vision**

The IHS DIR vision is to enhance customer health care by providing the world's premier health IT environment.

### **Mission**

The IHS DIR mission is to provide integrated IT solutions that exceed the I/T/U customers' needs.

### **Program Obligations**

Public Law 100-713, Indian Health Care Amendments of 1988, Title VI, Section 602, *Automated Management Information System*, mandates IHS to establish an automated management information system that includes the following:

- Financial Management System (FMS)
- Patient care information system for each Area the IHS serves
- Privacy component that protects the privacy of patient information held by, or on behalf of, the IHS
- Services-based cost accounting component that estimates the costs of specific medical treatments or services in each IHS AO

In addition, *P.L. 100-713* mandates that the Secretary provide automated management information systems to each Indian tribe and tribal organization that provides health services under a contract entered into with the IHS under the Indian Self Determination Act. These systems must meet the management information needs of these Indian tribes or tribal organizations with respect to treating IHS patients and the Agency's information needs.

### **Goals and Objectives**

Exhibit 2-1 lists the IHS goals and objectives that support this vision.

---

<sup>3</sup> *Information Resources Management Plan 2000-2004*, Indian Health Service, March 1, 2000 Version 1.

**Exhibit 2-1: IHS Vision: Goals and Objectives**

GOAL	OBJECTIVES
<p><b>1) Provide a quality Billing and Cost Accounting/General Ledger system that is integrated with our Health Information System.</b></p>	<ul style="list-style-type: none"> <li>a. In consultation with constituent groups, develop a report that evaluates commercial billing and accounting systems and examines the feasibility of enhancing our current systems to match their functionalities. The report will include a cost–benefit analysis of the alternatives.</li> <li>b. Develop and implement a generic HL7 data interface to existing RPMS applications (refer to Goal 1).</li> <li>c. The ISAC will submit a recommendation to IHS Director for an integrated Billing and Accounting System.</li> </ul>
<p><b>2) Facilitate the interoperability with commercial systems; institute an open standard-based health information system for the I/T/Us.</b></p>	<ul style="list-style-type: none"> <li>a. Develop HL7 interfaces to all applicable RPMS applications</li> <li>b. Use recognized and emerging data interchange, security, message handling, and data transmission standards.</li> <li>c. Report on the evaluations of current health open standards and other future relevant standards on the horizon to be interfaced with the RPMS (i.e., Government Computer-based Patient Record (GCPR)).</li> <li>d. Publish an open standards document that specifies alternatives to interfacing with the RPMS.</li> </ul>
<p><b>3) Develop an annual operational plan based upon a survey of the I/T/U customer’s wants</b></p>	<ul style="list-style-type: none"> <li>a. The CIO (HQ) will develop, print, and distribute a survey to IT customers.</li> <li>b. The CIO, with appropriate technical assistance, will analyze and rank the survey results.</li> <li>c. The CIO will report the survey results and recommendations to the ISAC.</li> <li>d. In support of the ELG work-plan, the CIO, with ISAC collaboration, will develop the operational plan incorporating the results and recommendations of the customer survey.</li> <li>e. The CIO will implement the annual operational plan.</li> </ul>
<p><b>4) Provide technical support for the current Health Information System.</b></p>	<ul style="list-style-type: none"> <li>a. Establish and maintain access controlled web site available to the I/T/Us for distributing RPMS applications and patches, with information retrievable by both application and date</li> <li>b. Establish a formal, web-based technical support feedback system between Health Information System developers and field support staff, with status reports viewable by both</li> <li>c. Establish a formal technical support training schedule (refer to Goal 5) for supported Health Information System hardware platforms (AIX, SCO, NT, etc.) and current Health Information System architecture, such as FileMan</li> </ul>

	<p>and Kernel</p> <ul style="list-style-type: none"> <li>d. Coordinate with specific provider groups the development of a training and support schedule and publish on a recurring basis—specific Health Information System applications</li> <li>e. Establish a mechanism to maintain hardware, peripherals, and operating system software for existing large (RS6000-based) RPMS operating platforms</li> </ul>
<p><b>5) Make accessible high-speed connectivity for all I/T/U customers to a secure common network that facilitates the transmission of voice, video, and data services.</b></p>	<ul style="list-style-type: none"> <li>a. Establish a Virtual Private Network (VPN) Gateway to the IHS that meets Health Insurance Portability and Accountability Act (HIPAA) data transfer standards</li> <li>b. Publish technical document detailing methods to connect to the IHS wide area network (WAN), detailing the costs and benefits for each connection</li> <li>c. Provide classes on LAN/WAN connectivity emphasizing the WAN connectivity to the IHS</li> <li>d. Publish guidelines for minimal acceptable service and obtain tools to measure and monitor network performance and availability</li> <li>e. Implement voice-over-data and video-conferencing solutions at HQ and each AO, which will save costs by enabling toll-free calls and travel-free meetings between the entities and will help promote and justify the technologies to the rest of I/T/Us</li> </ul>
<p><b>6) Promote adequate staffing at all levels to support IT functions</b></p>	<ul style="list-style-type: none"> <li>a. Develop a model Human Resource assessment profile for every level, such as large and small clinics, hospital, Area, and Urban Program that include:             <ul style="list-style-type: none"> <li>a. Number of staff</li> <li>b. Grade levels</li> <li>c. Position Description</li> <li>d. Contractor and personnel skill sets</li> <li>e. Types</li> <li>f. Roles</li> <li>g. Responsibilities</li> <li>h. Supporting contracts</li> </ul> </li> <li>b. Assess and report current capabilities comparing model to existing staff</li> <li>c. Assess and report on Recruitment and Retention (R and R) rates for targeted functions</li> <li>d. Develop R and R plan for those targeted functions</li> <li>e. Upon approval—Implement the R and R plan</li> </ul>
<p><b>7) Institute a GUI for the RPMS</b></p>	<ul style="list-style-type: none"> <li>a. Define an IHS standard GUI toolbox that includes a module-based framework to attach independently-developed modules</li> <li>b. Create a web access toolbox to interface with the RPMS</li> <li>c. Retool core RPMS applications to be GUI based</li> </ul>
<p><b>8) Provide effective IT and</b></p>	<ul style="list-style-type: none"> <li>a. Establish/Appoint National Technical Training</li> </ul>

<p><b>Data Management Training at all levels</b></p>	<p>Coordinator/Manager</p> <ul style="list-style-type: none"> <li>b. Assess and evaluate current IT training capabilities and capacities at all levels</li> <li>c. Define scope of training program i.e., target groups at fields and area levels</li> <li>d. Perform training assessment of I/T/U training needs</li> <li>e. Match current training need to existing capacity, such as site manager training and data entry training</li> <li>f. Through customer survey, identify new areas for training development, such as data management, data quality</li> <li>g. Decision to either build/buy training course work</li> <li>h. Expand existing and develop new training course work using both didactic and distance learning methodologies</li> <li>i. Evaluate target audience progress for program modifications</li> <li>j. Maintain training program</li> <li>k. Establish a web site that serves on-demand pre-recorded training sessions using streaming video technologies</li> </ul>
<p><b>9) Provide universally accessible decision support information that positively impacts health care management and delivery</b></p>	<ul style="list-style-type: none"> <li>a. Establish data warehouses, which use open standards-compliant Relational Database Management Systems (RDMS) with state-of-the-art tools available for on-line analysis.</li> <li>b. The data warehouses are scalable from a facility to regional levels and contain information aggregated from the I/T/U's administrative and health care systems, and other external data sources, such as Medicare, Medicaid, and Private Insurance entities.</li> <li>c. The integrated data warehouses are designed to help meet the I/T/U's cost accounting and health care management needs.</li> </ul>
<p><b>10) Ensure national comparability of public health data for all I/T/Us</b></p>	<ul style="list-style-type: none"> <li>a. Incorporate the findings and recommendations of the Public Health Support Workgroup, Charge #3</li> <li>b. Identify a Standard Data Set Manager responsible for maintaining/updating data sets</li> <li>c. Assess and compile completed work and recommendations regarding standard data sets</li> <li>d. Establish a constituent I/T/U workgroup to review recommendations and consult</li> <li>e. Prepare document to submit to <i>Federal Register</i> for publication, review, and comment</li> <li>f. At the completion of the <i>Federal Register</i> process, incorporate the new or modified data elements into RPMS and the GCPR development process</li> <li>g. Develop annual mechanism to review and obtain feedback on standard data sets</li> </ul>
<p><b>11) Ensure quality public health and administrative</b></p>	<ul style="list-style-type: none"> <li>a. Identify a Data Quality Coordinator responsible for data quality policy and procedures</li> </ul>

<p><b>data for all I/T/Us</b></p>	<ul style="list-style-type: none"> <li>b. Assess and compile completed work and recommendations regarding data quality efforts</li> <li>c. Develop model Data Quality Assurance program</li> <li>d. Establish a constituent I/T/U workgroup to review recommendations and provide consultation</li> <li>e. Implement plan by areas to monitor data quality from local sites, which must include training and assessment of needed activities at all levels</li> <li>f. Develop mechanism for feedback to the NPIRS in relation to data reports</li> <li>g. Develop annual mechanism for I/T/Us to review and provide feedback on “data quality policy”</li> </ul>
<p><b>12) Institute a state-of-the-art CPR with the ability to manage clinical alerts/pathways and contains data integrated from the various facilities that a patient has visited</b></p>	<ul style="list-style-type: none"> <li>a. Create a detailed cost-benefit analysis using the VA’s VistA Computer-based Patient Record System (CPRS), or a commercially-based system</li> <li>b. Continue supporting the GCPR project and establish a national implementation plan that would have it installed at those sites that desire to participate, within 1 year of its release</li> </ul>
<p><b>13) Institute a state-of-the-art administrative environment throughout the I/T/U</b></p>	<ul style="list-style-type: none"> <li>a. Pursue electronic commerce solutions to solicit contracts and purchase orders; transmit awards, notices, and payments; and accommodate online vendor inquiries</li> <li>b. Conduct a cost-benefit analysis to acquire an Enterprise Resource Planning (ERP) system that provides a uniform solution to the corporate administrative processes, such as human resources, payroll, finance, and procurement</li> <li>c. Promote a modern and efficient paperless office environment with document processing and workflow capabilities that integrate with the I/T/U’s financial and personnel systems</li> </ul>
<p><b>14) Promote adequate computer systems for all I/T/U employees to perform their jobs</b></p>	<ul style="list-style-type: none"> <li>a. Define and publish the technical standards and infrastructure for a recommended operating environment</li> <li>b. Provide a tool to assess and plan resources</li> <li>c. Insure that cost-effective procurement sources are known and accessible</li> </ul>
<p><b>15) Promote partnerships between I/T/U and other agencies to work collaboratively on projects of mutual benefit</b></p>	<ul style="list-style-type: none"> <li>a. Identify and prioritize areas with potential to establish partnerships</li> <li>b. Create a clearinghouse for information systems projects that will facilitate sharing locally-developed software</li> <li>c. Participate with other agencies and I/T/U entities in common benefit areas</li> <li>d. Involve I/T/U representatives in partnership activities</li> <li>e. Identify resources to support priority partnership activities</li> <li>f. Establish a competitive process, within I/T/U, to perform the projects contained in the <i>Annual Operational Plan</i></li> </ul>

## BUSINESS DRIVERS<sup>4</sup>

---

The paragraphs that follow list and describe IHS business drivers.

***Implementing the Indian Self-Determination and Education Assistance Act will expand.*** Joint efforts between tribes and the IHS to maintain and improve the information resources infrastructure will become especially important as Information Resource Management (IRM) funds are transferred directly to the tribes under Title I and Title III of the Indian Self-Determination and Education Assistance Act.

***Budget pressures will compel efficiency.*** The continuing struggle to contain the Federal budget deficit will place continuing pressure on IHS to improve efficiency. IHS must re-engineer its processes and use technology intelligently to meet service goals and objectives and maintain or reduce costs. Insufficient full time equivalents (FTE) and funding will complicate information resources management.

***Demand for information will increase.*** Information needs at all IHS levels will continue to grow, requiring more frequent access to current information and increasing the requirement for integrated databases to realize productivity gains, program improvements, and improved service delivery. Clients, service providers, and IHS end users will become more sophisticated in using information and technology and will expect improved access to information. Electronic information exchange among agencies and external organizations will increase. Availability of the IHS LAN and WAN technology, such as electronic mail and Internet access, will facilitate information and files internal and external to IHS sharing. Electronic information exchange with the public will increase because of continued use of the Internet and Web.

***IT infrastructure elements will require more intensive management.*** In general, IT requires organizational leadership, architecture standardization, and enterprise-wide strategic planning to promote a consistent and focused agency-wide IT resource management program. Initiatives that support these approaches will enable agency-wide IT resources to be applied in ways that promote using resources efficiently and support the Clinger-Cohen Act IT capital investment management guidelines. The IT management process must support IT performance measures and evaluation criteria development. These baseline measures and criteria will help IHS take a "return on investment" approach to IT investments Clinger-Cohen requires. This major challenge will affect strategic planning for IT resources application and development and in-place resources management.

---

<sup>4</sup> *Information Resources Management Plan 2000-2004*, Indian Health Service, March 1, 2000 Version 1.

**Information systems will focus on end users.** Re-engineering will intimately involve users in system development projects, and end user tools will provide them with technological support to access, analyze, and manipulate information.

**Access to training and reference information will increase and involve distant sources.** Access learning opportunities and distance learning is becoming vital to the Agency's efforts to maintain the expertise and accreditation of its geographically scattered human resources. Similarly, access to reference and consulting resources will increasingly involve dispersed resources.

**Public access to data will increase.** Clients will have direct access to information about IHS programs and to information about their specific records/benefits by means of technology-supported vehicles, such as personal computers, touch-tone telephones, and information kiosks.

**Electronic transfer of information and funds will increase.** HIPAA and other health care reforms mandate using Electronic Data Interchange (EDI), Electronic Benefits Transfer (EBT), and electronic identification to re-engineer IHS systems and services to support electronic exchange of financial and health care data, including procurement, medical billing, Electronic Funds Transfer, benefits payments, and computerized medical records. Demand for bandwidth to support EDI/EBT will also increase as telemedicine, teleradiology, and distance learning become common.

**Legislative requirements will influence changes to DIR technological needs.** GPRA, Clinger-Cohen, and reorganizing IHS components responsible for providing IT to IHS users require changing existing IT management processes, which will improve how IHS IT resources are managed.

**Standards will become increasingly important.** In an increasingly diverse computing environment, IHS will continue to develop new development standards, especially in networking where emerging standards for higher capacity network strategies will provide mechanisms to meet the demands of scientific computing and new workloads brought about by increased use of the Internet and the Web. Transferring images and other non-textual information objects will become more common.

**Standards-based approach leading to a more "open" systems environment.** Simplified plug and play interface standards between computer applications are reducing custom interface programming and program maintenance each time a new application is added. It is also stimulating the broadest possible commercial and public sector participation in IT solution development, benefiting IHS.

## TECHNOLOGY DRIVERS

---

The paragraphs that follow list and describe IHS design drivers.

**RPMS Enhancements.** Demand is increasing to re-engineer and modernize RPMS. Improved quality of medical care being provided to AI/AN will require an enhanced patient and resource management information system to provide timely, quality, and accurate data for decision-making and to improve health care services delivery.

**Share and Integrate Data.** RPMS provides IHS with an automated patient record within the confines of each of its facilities but currently cannot share and integrate data between internal IHS facilities or appropriate external ones electronically. Other agencies and health care organizations likewise have various types of computerized systems that communicate with varying degrees of success.

**Collaborate and Leverage Resources.** The DOD, the VA, and the IHS have embarked on the GCPR Program, a joint effort to improve information sharing and collaborative decision-making across the Federal health care continuum. The Program's goal is to improve public and individual health care by using existing technology to share patient health-related information securely at a level unachievable with a paper record. The IHS has been an active participant in the GCPR Program since its inception in January 1998. Successful implementation of the Framework Project will help IHS reach many technology goals. The IHS will garner the following benefits:

- Enhance our technical understanding of new techniques and technologies, such as Common Object Request Broker Architecture (CORBA) and CORBAMed, Unified Software Development Process (USDP), Health Level 7 (HL7), and others
- Keep current with solutions for similar organizations
- Participate in development and acceptance standards formulation

**Data at Point of Care.** Complete and accurate computer-based patient information will be accessible at the point of care. Practitioners need immediate access to patients' medical records to make informed judgments and recommendations when providing services and to avoid unnecessary visits and procedures. An electronic medical record must be accessible in wards, clinics, examining rooms, nursing stations, offices, and other locations where patients are seen. Desktop and portable workstations will serve as each clinician's window into the information world, capable of accessing and synthesizing health care information from a variety of sources.

**Access to consolidated repositories.** Distributed computing and related client/server database technologies will continue to increase in popularity and require pervasive, reliable networking and capacity management. Internet-based inputs will enhance the capabilities of non-RPMS users and increase the customer support requirements of the national data repository.

**Workload will grow.** Increased availability and daily use of automation is requiring additional training and technical support. IHS expects its major programs to serve an increasing client base.

**Interoperability is a requirement.** Over the next few years, implementation and universal acceptance of open systems standards will enable IHS to provide seamless connections (i.e., all users will have desktop access to every other employee and to all major IHS resources for which they are authorized). Technology advances are facilitating Agency information infrastructure improvements. A mix of DIR architectures, manufacturers, and equipment is required to support IHS' information needs.

## **LEGISLATIVE DRIVERS**

---

Over the past decade, Congress has passed legislation to clarify expectations about investing public funds in IT. Congress has also better defined Federal Department roles and responsibilities for the stewardship of its information resources. The most pertinent legislation is the IT Management Reform Act of 1996 (ITMRA or Clinger-Cohen Act), which requires Federal Departments to focus on the results achieved through IT investments while streamlining the Federal IT procurement process. This Act requires Departments, as one criterion to approve funding, to establish EAs and ensure that IT investments are consistent with them. This Act is further reinforced through OMB policy, Raines' Rules (October 1996), OMB Circular A-130, and the description of EA components, OMB M-97-16. As a result, DHHS has both a business need and a legislative mandate to establish a Departmental EA. Exhibit 2-2 depicts the more salient legislation.

**Exhibit 2-2: IT-Related Legislation**



Acronym	Legislation
CFO	Chief Financial Officers Act of 1990
GPRA	Government Performance and Results Act of 1993
GMRA	Government Management Reform Act of 1994
ITMRA	IT Management Reform Act of 1996 (Clinger-Cohen)
FASA	Federal Acquisition Streamlining Act of 1994
FARA	Federal Acquisition Reform Act of 1996
GPEA	Government Paperwork Elimination Act 1998
PRA	Paperwork Reduction Act of 1995
PDD 63	Presidential Decision Directive 63

**Chief Financial Officers Act of 1990 (CFO Act.)** The CFO Act was passed to improve accounting, reporting, and auditing practices; improve financial systems; and improve asset management policies. Under the CFO Act, Federal agencies are required to form financial management plans and annual progress reports, and to audit financial statements. The Act also mandates establishing a Government-wide CFO Council through CFO organizations in OMB and each agency.

**Government Performance and Results Act of 1993 (GPRA.)** The GPRA requires Federal agencies to develop strategic plans, performance measures, annual performance plans, and performance reporting. The strategic plans were to be submitted to Congress and the public by September 30, 1997. Beginning with Fiscal Year (FY) 1999, Federal agencies have developed annual performance plans parallel to their annual budget requests to Congress. In March 2000, agencies were to begin reporting on the results achieved in executing their FY1999 annual performance plans.

**Government Management Reform Act of 1994 (GMRA.)** The GMRA (P.L. 103-356) calls for a more effective, efficient, and responsive government through a series of Federal management reforms, primarily in human resources and financial management. The Act builds on certain earlier acts, including the CFO Act. GMRA requires Federal agencies to monitor, measure, and evaluate the performance of their IT programs and determine whether to continue, modify, or terminate programs or projects.

**IT Management Reform Act of 1996 (ITMRA or Clinger-Cohen Act.)** The ITMRA is the legislative driver that requires EA development. This driver defines IT as "integrated frameworks for evolving or maintaining existing IT and acquiring new IT to achieve the Department's strategic goals and information resources management goals." In addition, the Act encourages performance-based and results-based management; benchmarking performance against comparable processes and organizations in the public or private sectors; and process analysis and revision for mission-related processes prior to investing in IT to support those missions. The Act also establishes requirements to appoint a CIO within each Executive Agency, outlines the CIO's responsibilities, duties, and qualifications; and promotes streamlined IT acquisition processes that address risk, incremental acquisitions, and the need to incorporate commercial IT in a timely manner.

**Federal Acquisition Streamlining Act of 1994 (FASA.)** The FASA (S.1587) centers on revamping the Federal procurement system via policies that reduce paperwork for small acquisitions and justify certain commercial product acquisitions; promotes acquiring commercial items; establishes limitations on filing claims; and expands small disadvantaged business programs and women-owned small businesses.

**Federal Acquisition Reform Act of 1996 (FARA.)** The FARA establishes policies and procedures to manage Federal agency workforce acquisition, including staff accession, education, training, career development, and performance incentives.

**Government Paperwork Elimination Act 1998 (GPEA.)** The GPEA (S.2107) requires Federal agencies to provide electronic or on-line versions of their forms for electronic submission as a paper substitute and allows individuals and

businesses to use digital signatures to file these forms electronically by October 2003.

**Paperwork Reduction Act of 1995 (PRA.)** The PRA was chartered to ensure effective and efficient information resource management practices are implemented, minimizes Federal government paperwork; and identifies OMB's Office of Information and Regulatory Affairs (OIRA) responsibilities.

**Presidential Decision Directive 63 (PDD 63.)** PDD 63 builds on the President's Commission on Critical Infrastructure Protection recommendations. In October 1997, the Commission issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures, such as telecommunications, banking and finance, energy, transportation, and essential government services. The policy sets a goal of a reliable, interconnected, and secure information system infrastructure by the year 2003. It also calls for significantly increased government systems security by the year 2000 by doing the following:

- Immediately establishing a national center to warn and respond to attacks
- Ensuring the capability to protect critical infrastructures from intentional acts by 2003
- Addressing the Federal government's infrastructure vulnerabilities by requiring each department and agency to reduce its exposure to new threats
- Requiring the Federal government to serve as a model to the rest of the country for how infrastructure protection is attained
- Seeking public/private partnerships to protect critical systems

## RPMS GROWTH PLAN

---

The Massachusetts Utility Multi-Programming System (MUMPS)-based RPMS is IHS' core patient management system. Plans are in place to take advantage of new messaging technologies as well as distributed computing architectures to continue using RPMS. Current development in both the government and commercial sectors is being used to support RPMS.

RPMS<sup>5</sup> is well positioned to take advantage of technology and application developments in both the government and commercial sectors. One of the most significant IT architecture improvements is to enhance its interoperability capabilities. The main strategy that enterprises are taking is to move toward the widespread use of message-based inter-application and inter-site

---

<sup>5</sup> RPMS Growth Path Plan, May 2000, Vn. 1.0

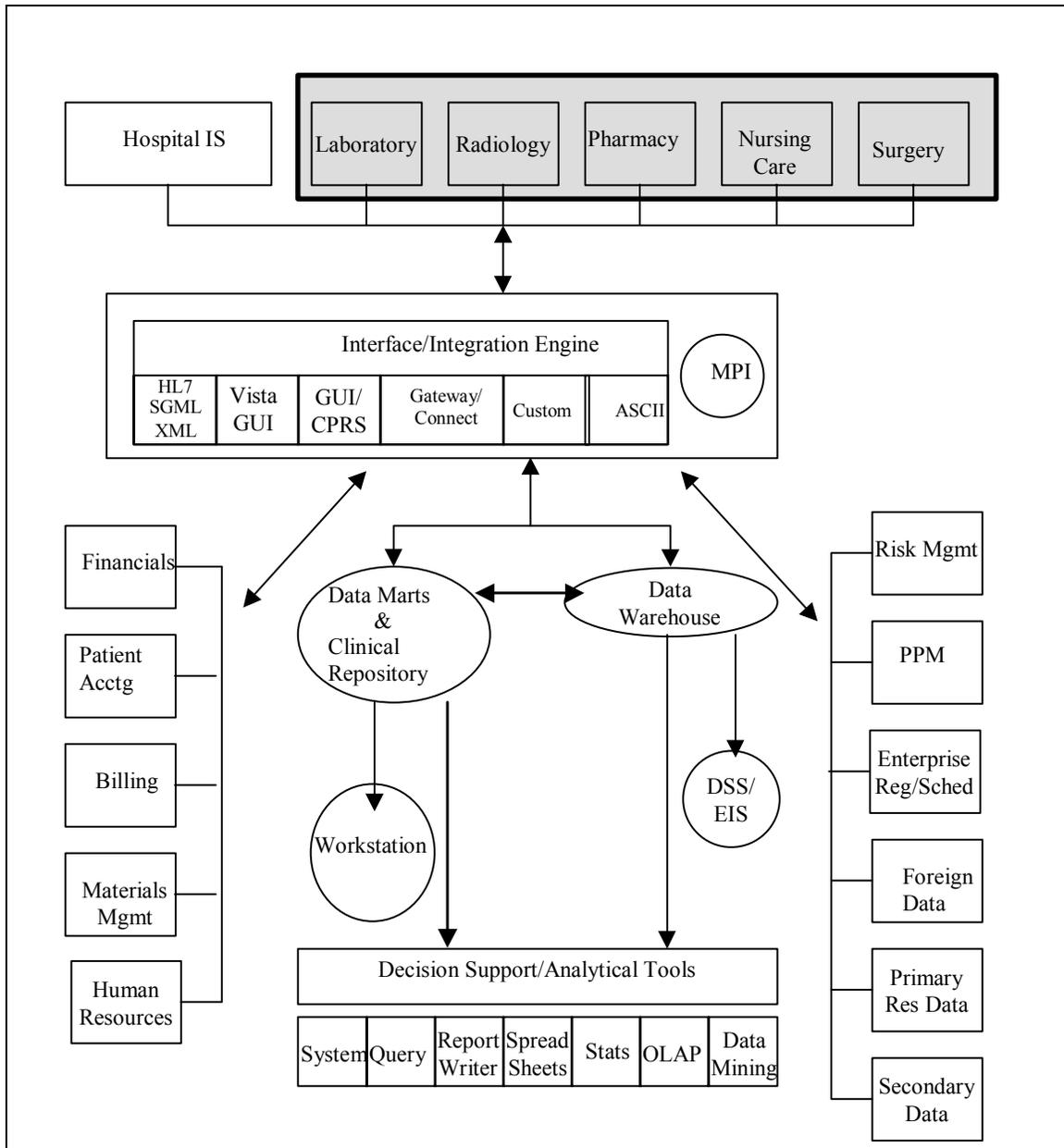
communication and data exchange. Improving the ability to exchange data is one of the primary strategies to achieve interoperability between RPMS and COTS solutions. Currently, RPMS can exchange data with COTS and GOTS through custom interfaces. Implementing standards to facilitate RPMS interoperability is fundamental.

Many commercial packages are interfaced or currently in the process of being interfaced with the RPMS using HL7 Version 2.X standards, including pharmacy, encoding, eligibility, patient identification, and billing packages. The ability to send data for an entire clinical encounter using an HL7 message has also been accomplished. In addition, adopting HL7 and X.12 messaging standards for data interchange will enhance the messaging capabilities and the ability to integrate COTS solutions. Future RPMS characteristics will include increased interoperability and the following characteristics:

- IHS-developed, VHA-developed, and COTS solutions, all communicating with each other and achieving interoperability via mature industry standards and technologies
- A fully optimized billing capability and will have introduced a CPR system for point-of-care entry by providers
- Full HIPAA compliance, including all E-Health being conducted over secure networks using a Public Key Infrastructure and standards-based messages to submit claims
- RPMS distributed applications will communicate with each other using various technologies such as CORBA, Component Object Model (COM)+, and the Extensible Markup Language (XML) and access services via a Common Service Architecture (CSA)
- State-of-the-art hardware and telecommunications technologies will be employed to provide required bandwidth
- Increased use of architectures, such as Symmetric Multi-processing (SMP) or clustering technology, will be required to handle increased workloads
- Wireless communications will be needed to provide improved point-of-care access, using hand-held entry and display devices to increase data access while increasing provider mobility

Introducing and using these technologies and standards will allow RPMS to respond faster to future business drivers, introduce new technologies as appropriate, and achieve the aforementioned IT goals. Exhibit 2-3 illustrates the RPMS information exchange.

**Exhibit 2-3: RPMS Information Exchange**



To achieve the architecture the EA describes, RPMS will use a phased development approach that includes the following four phases:

## PHASE 1

---

Phase 1 represents most projects' initial development stage. Highest priority projects that have few dependencies and a short development timeline will be fully deployed by the end of Phase 1. During Phase 1, RPMS will change in the following areas:

**Standards-based Data Presentation.** Current efforts to improve and move to standards-based data presentation will continue. This area is crucial to achieve common understanding and context for the information represented in our electronic systems by people using the information along with systems sharing the information.

**Monitor and Incorporate Specific VHA Projects.** The VHA projects in this area include the Corporate Data Registry that IHS will monitor and be ready to leverage and incorporate any applicable results from these projects.

**Information Modeling.** Information modeling will be key to achieving this common understanding and will be done incrementally, as a certain information area becomes a priority. Areas that will be modeled include patient demographics, laboratory, and medications. Areas other than those the GCPR project requires will be undertaken as resources allow. The GCPR Framework Project is a joint project between IHS, DOD, and VHA. The Framework Project develops a framework composed of industry standard services to allow interoperability and creating a virtual longitudinal computer-based record between the three agencies. This modeling and data representation will be based upon current and emerging health domain standards, such as those used in the HL7 and GCPR Reference Information Models.

**Clinical Repository and Lexical Services Analysis.** Analysis of VHA's Clinical Repository and Lexical Services will be conducted. This project will lead to a clinical repository and associated vocabularies that go beyond ICD9 and Current Procedural Terminology (CPT) to be either built or purchased. How the clinical repository represents information will be evidenced in the information models either directly or through some sort of mapping. IHS uses the Patient Care Component (PCC) as its clinical repository and VHA's project may lead to identifying enhancements or capabilities that PCC would benefit from, or IHS could leverage.

**Unique Health Care Identifiers.** Some legislative drivers, such as the HIPAA, establish unique health care identifiers for Providers, both individuals and organizations, and patients. During Phase 1, efforts to establish unique health care identifiers will begin. First, how names are represented within RPMS will be standardized. The process and mechanism to achieve this will be the same as VHA uses. Standardizing names ensures that the patient or provider is

identified correctly when sharing information between systems. Name elements are some of the criteria duplicate checking algorithms use to determine if a patient already exists within a system. Other elements include date of birth, sex, and Social Security Number. As the final ruling for identifying providers uniquely is issued, IHS will identify and start assigning these unique identifiers.

**Accessing, Transferring, and Using Information.** New standard ways along with increased use of industry standards to access, transfer, and use information will be developed and demonstrated in various projects.

**Implementing Interfaces with HL7.** The number of COTS products interfacing with RPMS using HL7 version 2.X standards will increase and demonstrate using an enhanced messaging infrastructure developed for the GCPR project and various business office projects. One key enabling strategy will be using an interface engine to exchange messages between systems and locations. The interface engine can support either an individual facility or individual regions, with the possibility of setting up a dedicated interface engine for National clearinghouse or E-commerce use.

**X.12 Implementation.** The X.12 standard will be used to submit claims attachment information according to HIPAA requirements. Projects, such as GCPR and Envoy, will demonstrate the first use of these X.12 messages. Projects that provide some of the underlying tools and infrastructure include the VHA and IHS Application Use of Messaging project.

**Data Transport Project.** The Data Transport Project will enhance and simplify the methods by which we obtain information from I/T/U. This Project initially consolidates many of our records into a single formatted file, which is then aggregated and moved to our Enterprise- or national-level data warehouses, such as National Patient Information Reporting System (NPIRS.) Transaction-based updating of these warehouses will be demonstrated. Movement from a batch to a transaction-based update will improve information timeliness and allow for flexible information use from prospective analysis to real-time decision support.

**MPI/MPIL Implementation.** Accurate patient identification is required to transfer patient information between locations or to build a longitudinal electronic health record from multiple locations. In this phase, the GCPR Framework Project will use and implement a Master Patient Index (MPI) and Master Patient Information Locator (MPIL) built upon an industry-accepted set of tools and specifications. NPIRS will either be enhanced to conform to these specifications or a COTS product will be chosen. The MPI/MPIL will be scalable to allow for multiple regional MPI/MPILs to manage patient identification and the location at which they have received service.

**Security Infrastructure.** A new security infrastructure compliant with new Agency and legislative mandates will be demonstrated for select applications. New security policies will be developed along with Public Key Infrastructure (PKI) and Virtual Private Network (VPN) implementation.

**PKI.** A PKI transparently manages keys and certificates allowing an organization to create and use a trusted networking environment. A trusted network allows IHS to provide coordinated and consistent authentication with authorization, confidential communication, non-repudiation, and integrity.

Authentication validates that the sender created the file. Recipients need to know who created the file. Confidential communication ensures that only intended recipients can read files. Files can not be intercepted. Non-repudiation prevents the sender from denying involvement in creating the file. Integrity guarantees the file was not altered during transmission.

**Virtual Private Network (VPN).** A VPN is one means to secure transmission over public networks. Organizations can use a VPN to enable field providers to communicate securely and confidentially with the clinical database to retrieve patient data. Integrating PKI and VPN will provide a security framework for trust and secure communications.

**Improved Telecommunications.** Telecommunications will change to accommodate the bandwidth and technologies that RPMS and other uses require:

- The telecommunications infrastructure will start incorporating ATM and other protocols
- Wireless technologies and appliances will be used to provide service at the point of care

**Information Capture, Storage, Transfer, and Analysis.** New or enhanced applications or systems will be developed or implemented to support information capture, storage, transfer and analysis. Many new applications or systems depend on the infrastructure and changes discussed above. Staying current with VHA for applications IHS has chosen will be a key strategy to deliver additional functionality and capabilities and leverage resources for RPMS.

**Third-party Billing.** RPMS will continue to be upgraded to support efficient third-party billing, including interfacing with COTS products, such as those by ENVOY, for eligibility information and billing services, and integrating outpatient pharmacy billing to the national fiscal intermediary.

**Update Infrastructure and Tools.** Much of the current infrastructure and supporting tools are taken from VHA's VistA infrastructure and tools, including

Kernel, FileManager, MailMan, ToolKit, and RPC Broker. In this phase, we will deploy these tools up to the latest release from VHA; and an effort to stay current with releases will be established.

**Update Application Releases.** In addition, core RPMS applications, such as Patient Registration, Laboratory, Scheduling, Outpatient and Inpatient Pharmacy, that were modified from older versions of VHA VistA will be brought up to the latest release version from the VHA and an effort to stay current with releases will be established.

**Deploy Additional VHA Applications.** Deploying current versions of the VHA Infrastructure and core applications will enable IHS to review and possibly deploy other VHA applications as the user community determines if said applications will meet their functional requirements. Prime examples include CPRS, Radiology, and Imaging.

**Add Functionality to IHS-Specific Applications.** Functionality will be added to IHS-authored RPMS applications modified VHA VistA applications such as CHS, A/R, PCC and Data Entry.

**Data Warehouses.** Enterprise and regional data warehouses will be established and information access will be improved via ANSI Standard Structured Query Language (SQL) interfaces.

Phase 1 work done in the areas of interoperability, GUIs, billing, and non-modified VHA VistA; enhanced RPMS applications will undergo testing and deployment. Development in the area of migrating VHA VistA software, such as PIMS and Pharmacy, will be completed and ready to start testing. Project Planning and development efforts for deploying CPRS will begin.

## PHASE 2

---

Phase 2 milestones are marked by demonstrating, at selected demonstration sites, the RPMS environment that builds on the infrastructure and functionality completed during Phase 1.

RPMS will incorporate VistA GUI and imaging functionality as well as the increased functionality available in other, current VistA applications, such as lab, pharmacy, and radiology. Implementation will be targeted to Area Demonstration Sites. In this Phase, a CPRS will be demonstrated at various demonstration sites along with the increased functionality that the GCPR Project and other underway projects are realizing.

RPMS will fully comply with HIPAA and any new security standards involving electronic commerce and patient consent. RPMS will have increased capabilities to retrieve information based on aggregate data or multiple points

of health care delivery. Enterprise data warehouses will be available to use. Web-based area data retrieval will be a reality. GUI interfaces will be available for multiple applications. Interface engines will be used to exchange data throughout IHS. Demonstrated use of XML for data presentation, storage, and exchange will occur.

### **PHASE 3**

---

Phase 3 represents deploying the RPMS configuration that was demonstrated or tested at selected sites during Phase 2 to the I/T/Us. As a result, RPMS, VistA, and COTS applications will gain additional functionality as it is implemented at I/T/U sites. Data can be exchanged between business partners, and GUIs are provided for appropriate applications. In addition, IHS-wide implementation of the new RPMS configuration will occur.

### **PHASE 4**

---

The majority of Phase 4 activities will concern maintaining the deployed RPMS environment.

- RPMS, VistA, and COTS will continue to gain functionality. Integrating packages will eliminate custom interfaces and triggered event transfers.
- By Phase 4, the pilot projects involving Web interfaces and the ability of web technology to support real-time applications will mature. GUI/CPRS is expected to become a Web-based interface. Many of the RPMS interfaces will have been demonstrated using Web browsers and technology, especially those dealing with information retrieval.
- The Patient Record Architecture will have matured and allow for creating and storing a standards-based electronic health record, including things necessary for meeting records evidentiality requirements.
- Messaging standards will have matured to allow for true standards-based data exchange.
- Package integration will allow transparent data, images, voice, and video exchange between and among partners, facilities, and agencies.

## FRAMEWORK

This chapter discusses the EA's foundational elements by presenting the health care models and standards. The framework includes the EA attributes that serve as the glue that binds the organizational aspects of business processes, information needs, application systems, data definitions, and delivery systems. It also describes a generic health care information infrastructure closely followed throughout the health care industry. This supports the framework by describing the various layers that make up a health care infrastructure.

Key to any informational architecture is the standards that make up the framework. The section also describes the components of a Technical Reference Model (TRM) that includes information transfer, information processing, integration services, data management services, application security services, systems management, and external environment. The standards that drive the architecture are derived from the TRM.

## CRITICAL EA ATTRIBUTES

---

A successful EA is the basis for good design. For an EA to be successful, it must possess eight prominent critical attributes. Each of these attributes has an associated performance measurement.

The critical attribute performance measures relate to the quality of architectural design and do not specify system performance. The characteristics of a good architecture can be qualitatively measured. These measurements occur through answers to the architectural performance measure questions associated with each critical attribute.

Eight prominent critical attributes of a successful EA are the following:

1. **Adaptable:** The information infrastructure is made up of easily replaceable components that can be adapted to changes in business requirements.

*Performance measure:* Is the EA agile enough such that major business initiatives can move forward without significant implementation delays caused by infrastructure barriers?

2. **Patient health centered:** IT systems should center on supporting the health of AI/ANs by contributing to maximizing patient information processing functionality, outcome measurements, and health value.

*Performance measure:* Are IT systems designed and developed from patient-centric and global perspectives?

3. **Accessible:** The architecture enables users to find, obtain, or supply the right information quickly and easily in the desired form based on user context and roles.

*Performance measure:* Does the architecture provide appropriate user interfaces that are available at the right access points and satisfy the needs of the various categories of users?

4. **Interoperable:** Indian Health Service (IHS) architecture provides a framework that enables reliable and seamless data exchange between heterogeneous applications throughout the business enterprise in a consistent manner.

*Performance measure:* Does the architecture use standards-based data interchange methods that maintain data integrity for multi-point sharing?

5. **Connected:** The architecture promotes participation and usage by the health care provider community and beyond.

*Performance measure:* Does the architecture enable secure data interchange among external and internal knowledge repositories, alliances, partners, administrations, and agencies?

6. **Secure:** The security architecture preserves and protects against loss, damage, or unauthorized disclosure of data while providing authorized data interchange.

*Performance measure:* Are continuous security architectural improvements made in anticipation of future business needs?

7. **Maintainable:** The architecture uses highly leveraged technologies that are cost effective, modular, certifiable, and readily available.

*Performance measure:* Does the architecture avoid unnecessary complexity, tightly coupled systems, native interfaces, and proprietary solutions where possible?

8. **Standards based:** The architecture makes extensive use of standards.

*Performance measure:* Does the architecture follow the standards identified in the IHS Architecture Framework?

An EA that incorporates these attributes will facilitate adaptation to changes driven by business needs and technology drivers.

## HEALTH CARE INFORMATION PRINCIPLES

---

Advances in IT during the past decade have resulted in a proliferation of clinical information systems dedicated to different user groups and clinical functional areas. This, in turn, has created the need for hospital-wide management and integration of information and has triggered major efforts to develop integrated hospital information systems as a building block of integrated regional health care networks.

The diversity of hospital organizations, the complexity of clinical protocols and procedures, and the different preferences of various user groups make it extremely difficult for a single monolithic information system to serve the needs of an entire health care organizational structure. Thus, information and telecommunications systems must, primarily, provide the infrastructure to support the integration of distributed and heterogeneous components, ensuring overall integrity in terms of functional and information interoperability. This approach to developing and managing regional health care networks, such as integrating heterogeneous, autonomous distributed systems, ensures the transfer and integration of consistent information between health care facilities, without imposing constraints on the operation of individual clinical units.

The explosive growth in network connectivity and the rapid advances in computing power are replacing the older notion of standalone information utilities with newer notions of interconnected systems. Users must simultaneously access multiple distributed information sources that differ in content, form, and source types. In this context, conventional notions of information retrieval limit the kind of interaction that is observed in actual work. The wide variety of ways in which information is arranged, sought, and used in physical workspaces strongly suggests the importance of providing an equally rich and flexible environment for interacting with information in electronic workspaces.

The current trend in health care IT is increasingly digital and multimedia oriented. The next generation of health care information systems will consist of a large number of heterogeneous, autonomous, and distributed information systems, knowledge-intensive applications, and large quantities of multimedia medical data. The health care provider and patient must rely on a comprehensive infrastructure that will be an enabler. Data must be presented efficiently to both provider and patient. Such an infrastructure may be termed Health care Information Infrastructure (HII).

## HEALTH CARE INFORMATION INFRASTRUCTURE

---

A key challenge facing system researchers and builders is to provide a new organizational framework that can integrate this heterogeneous collection of resources into what appears to be a uniform integration of data and knowledge. This new framework will increase the availability of previously inaccessible information. Many other researchers and relevant bodies are recognizing the requirement for developing an HII<sup>6</sup>, introducing concepts such as the Medical Image Informatics Infrastructure within the integrated hospital environment.

Creating the HII is driven by, among other things, the need for the following:

- Data on outcomes of medical cases that will enable effective choices and compensation of providers
- Automation of mundane tasks to place the focus on patient needs rather than paperwork
- Empowering patients to become more actively involved in their own health care
- Flexible, remote access to relevant information to ensure the continuity of care from an accident site to the health care centers and to the patient's home
- Continuous process improvement through integrated and distributed IT

The health care organizational structure is naturally distributed, consisting of geographically distributed medical centers in a hierarchy of regional hospitals down to individual general practitioners. This structure offers comprehensive medical care at a local and regional level with continuity across different levels of the hierarchy.

Moreover, because of the greater mobility of patients and the population as a whole, National and International health care networks are increasingly used to facilitate sharing health care-related information among the various health care personnel. This information resource sharing is generally accepted as the key to substantial improvements in productivity and improved service. Hence, although each health care facility is autonomous and devoted to delivering a particular set of services, continuity of care requires that different health care facilities, offering complementary services or different expertise levels, cooperate and exchange patient data.

---

<sup>6</sup> Towards a Virtual Electronic Health care Record: The Patient Clinical Data Directory, <http://arachne.ics.forth.gr/pcddall/report/PCDDv3.14.htm>.

During a single health care episode, many professionals involved in a variety of medical acts administer medical care. Health care administration personnel, health care professionals, social care professionals, as well as patients need to interact with health care-related information. Each user group has different requirements in terms of information access, security, and quality of service, and is involved in different tasks, medical acts, and health care procedures. In addition, the requirements of each user affect information retrieval and presentation strategies and the overall interaction with the information space.

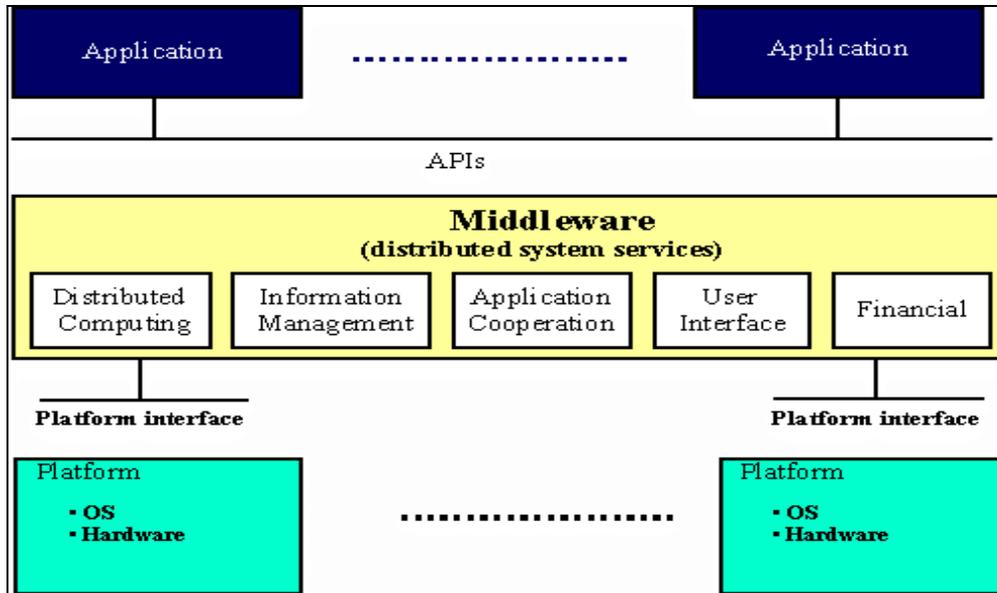
The evolving health care information infrastructure is also characterized by the fact that the bulk of medical data is managed by different specialized systems, designed to support the search for particular data types. For example, MRI scans, EKGs, laboratory reports, and administrative records of the same patient typically reside in separate, autonomous information systems. Thus, comprehensive information about a patient is difficult to obtain efficiently, unless these distributed segments of an electronic patient record can be integrated into a virtual patient record and viewed on-line through a unified user interface.

Current health care trends call for integrated user-oriented telematic services or end user services, which ensure prompt and secure access to information resources, provided proper authorization is available. To achieve this goal, complex problems and issues related to data heterogeneity, heterogeneity of platform and service requirements, complex protection and authorization policies, and interoperability protocols and for information exchange standards need to be addressed. Thus, the health care information infrastructure must primarily provide the framework for effectively integrating distributed and heterogeneous components, ensuring overall integrity in terms of functional and information interoperability. Advances in network technology are not limited to replacing current applications; they can revitalize older applications by enhancing and extending their functionality.

### **Health Care Functional Model**

A health care functional model is useful in identifying fundamental health care technology issues. The HII functional services model described in Exhibit 3-1, provides a logical model of the relationships among applications and the underlying services that support their development and use. The HII reference architecture model identifies the major functional elements of the infrastructure and their interfaces and protocols.

**Exhibit 3-1: HII Functional Services Model**



Users are primarily interested in information processing applications, which they may own or gain access to as end users via communications networks. These services are enabled by other underlying, transparent services that information and network service providers provide. Applications and enabling services will, in turn, employ certain information processing services and systems for data transport, which may be distributed throughout the HII. Thus, the HII consists of three basic components: applications, enabling (or Middleware) services, and physical infrastructure. These components can be mapped onto the functional services framework model shown in Exhibit 3-1 as a layered architecture.

The functional services model is similar to models of network protocols but is more generally intended as a way to think about the components of a feature-rich, flexible, open, and distributed infrastructure. The physical infrastructure contains the basic processing and communication components of an information system. The enabling services provide general system-related functionality for applications using the infrastructure. These services are those essential for the HII to fulfill its requirements and are categorized as follows:

- Distributed computing services provide the functionality that links multiple separate nodes into one distributed system (network services, location services, security services, etc.)
- Information management services organize, store, and retrieve information.
- Application integration services enable applications to cooperate to create common multiple end-user services. Typical services include messaging services, object request brokers, workflow managers, agents, and encapsulation facilities.
- User interface services present information to and acquire information from users, thus providing the link between users and the HII.
- Financial support services support all commercial and personal financial transactions.

Applications are information processing tools that give the user functionality. The underlying enabling services and physical infrastructure supply the means by which applications deliver their functionality.

### **Health Care Information Infrastructure Requirements**

Developing an HII to deliver customized, secure, integrated, user-oriented telematic services requires a heterogeneous, open, distributed and extensible, with multiple points of access, architectural framework. In developing an integrated framework to provide health telematic services, one must consider the heterogeneity of information sources, user needs and privileges, and tasks to be performed. Specifically, such a framework must dynamically encompass new applications and systems, including real-time monitoring and alarms, such as Intensive Care Units (ICUs); transaction systems, such as billing, office automation tools, and consumer-based interactive systems, such as the World Wide Web. Employing standardized health care components enables plug-n-play integration of distributed health care information systems.

Specific requirements for HII development are security and authentication, quality of service, integration, extensibility in terms of information sources and services, and support for task-oriented workflow and multiple overlapping views of the information space. Different user groups and individual users should acquire different privileges and authorities, in accordance with their need to know and the on-going medical act. The explicit enforcement of appropriate security and authentication policies is a critical factor in adopting new health care technology.

Service quality is another major requirement for information to be delivered in a timely manner, without compromising accuracy. Furthermore, one has to take into account timing requirements in determining the data precision and

quality to be transmitted, so that bandwidth is conserved and latency is reduced. Service quality is also closely related to priority issues. In the case that multiple service requests arrive at a service station, a priority should be assigned to each request based on properties such as emergency level, requester class, and requested service quality.

Integrating heterogeneous information sources should be facilitated through appropriate protocols and information exchange standards that ensure the interoperability of the underlying systems. Data, presentation, control, and functional integration issues come into play when users address heterogeneous information sources. Information integration should not require existing data repositories and applications changes to avoid costly data extraction, data conversion, or application conversion. Thus, the role of mediation services that bridge the semantic gap among non-uniform systems and services is very important. Overall, an integration architecture is judged by its operational effectiveness (cost, schedule), user performance (response, profile of information requests), supported information integration services (task, data, and syntax semantics), breadth of information coverage, and evolution.

Extensibility of information sources and services is also critical to the evolution of health care networks at a regional and national scale. As far as information sources are concerned, extensibility applies to the number and type of information sources in the form of information systems and data repositories that can be included in the information space. Information coverage is another important aspect of extensibility and refers to the precision and accuracy of the semantic mapping among the global information model and the information model of a particular information source. Information coverage frequently necessitates an iterative process, which may be at different stages for different user groups and tasks.

Thus, it is important that the architectural framework provides tools to assist this iterative information coverage process. Service coverage refers to interoperability among services and information sources. In this case, Middleware services enable new services and binding existing services to newly-attached information systems. Finally, task-oriented workflow defines a variety of contexts within which the aforementioned issues should be adequately addressed. Region wide, task-oriented workflow and the appropriate Middleware services enacting them, support handling medical acts and processes and tracking patients as they seamlessly move within the health care environment.

## **IHS TECHNICAL REFERENCE MODEL**

---

The Clinger-Cohen Act of 1996 (Public Law 104-106) assigns the CIOs of Federal Departments with responsibility to develop, maintain, and facilitate the EA implementation. A critical aspect of any EA is identifying and selecting technical standards and products to be used throughout the organization. In many technology classes, standards and products are well established and show great future promise.

By adopting vendor-neutral standards on a large scale, IHS hopes to reap the benefits of interoperability, decentralized decision making, economies of scale, substitutability, and scalability. Building dynamic and flexible information systems that meet the needs of an organization and allow the infusion of technology is crucial to IHS. By using standards and specialized COTS products, IHS can design and build information systems that satisfy new and evolving requirements, fostering the integration of new technologies. This section describes the set of standards and preferred COTS products to which IHS developers and/or contractors must adhere when building IHS information systems. The standards and products discussed in this document offer definitions and guidance to developers, procurement officials, managers, and engineers on how to implement standards that comply with IHS' EA.

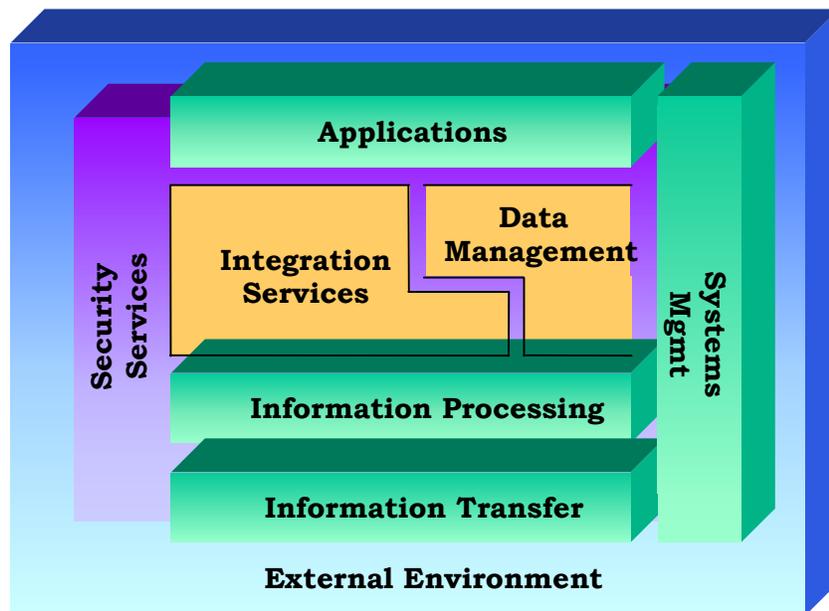
As Exhibit 3-2, IHS Technical Reference Model, illustrates a TRM is a conceptual framework that describes and discusses actual and proposed systems within a specific domain. It is based on descriptions of services, with related services grouped into entities. Relationships between these entities may be represented in the model; often this is done as part of the descriptions of the services.<sup>7</sup>

### **Exhibit 3-2: IHS Technical Reference Model**

---

<sup>7</sup> Carnegie Mellon Software Engineering Institute. *Department of Veterans Affairs Reference Models*. May 1998.

This TRM is a tool to promote integration and interoperability within the IHS IT infrastructure. It serves as a roadmap for consistent systems and technology solutions, evaluation selections, and development. The TRM provides a high-level framework and technology architecture guideline for IHS and does not target specific technologies. The standards, strategies, and guidelines identified in the following sections establish the fundamental technologies that enable IHS to meet many of its business and information system goals. Exhibit 3-3 describes each Major Service Area.



**Exhibit 3-3: Summary of TRM**

Section	MSA Description
<b>Information Transfer</b>	Technologies used to transfer information from an information source to an information user, including discussion of transmission media, access technologies, and network services
<b>Information Processing</b>	Technologies to provide computation and storage for IHS desktop and server environments, including platforms and operating systems
<b>Integration Services</b>	Technologies that link emerging client/server applications, legacy applications, and platforms
<b>Data Management Services</b>	Technologies to manage creating, updating, deleting, and accessing IHS data
<b>Applications</b>	Software systems that support IHS users in performing the Agency's business processes
<b>Security Services</b>	Technologies and practices that protect IHS information assets
<b>Systems Management</b>	Technologies and practices that enable IHS IT infrastructure monitoring and control
<b>External Environment</b>	Infrastructure technologies, typically supporting the transfer of information, don't fit conveniently within TRM's hierarchical structure. Examples include classical telephony.

**DEFINITION OF STANDARDS AND PRODUCTS**

Standards describe interfaces, services, protocols, and formats that enable the configuration and operation of a system. In simple terms, standards identify a common way that computer systems should behave. For example, Transmission Control Protocol/Internet Protocol (TCP/IP) is a networking protocol that allows users to send and receive information over a network. As long as each computer uses TCP/IP as its protocol, they can communicate easily. American National Standards Institute (ANSI) SQL is an example of a format protocol for retrieving data from a database. Any computer system using ANSI SQL to request data from an ANSI SQL-compliant database can access that data.

## **PURPOSE OF STANDARDS AND PRODUCTS**

---

This Standards and Products section provides the following:

- A first reference point for information and guidance pertaining to IHS-adopted standards and other sources of detailed information.
- A compendium of preferred COTS software products for IHS and contractor use. (It should be noted that the preferred COTS software products are not the standards but are products that satisfy the standards and are preferred for use in IHS.)
- Support to IHS development efforts by identifying the authorized standards and preferred products.

## **BENEFITS OF STANDARDS AND PRODUCTS**

---

The objectives of standards-based systems are to achieve the following: interoperability, decentralized decision-making, economies of scale, substitutability, and scalability. These objectives' benefits are detailed below.

**Increased Ability to Leverage Enterprise Software Licenses.** By coordinating Department-wide to purchase Enterprise software licenses, IHS can realize significant cost savings over purchasing smaller site or individual licenses.

**Discounts.** Allows IHS to purchase bulk hardware at significant discounts.

**Enterprise-Wide Training and Support.** As the Department moves closer to universal standards in particular product areas; it can provide more focused user training to larger groups. In addition, technical support becomes much more efficient, as technical support staff become proficient in a limited number of widely used technologies.

**Portability** Portability allows developers to move applications written for one system to another system without changing the code. This has several benefits. First, it reduces the costs associated with porting existing software products when the hardware platform changes. Second, portability makes users and application developers more interchangeable by providing the same look and feel across systems. This provision results in lower training costs because developers do not need training to develop a new application when they change systems. They do not need training because the environment that they write to, the Application Programming Interface (API), will not change. This provision also improves productivity and reduces user frustration associated with learning a new application. Portability reduces maintenance

costs by allowing software developers to support multiple hardware platforms from many vendors. For example, a developer can write an application in C without regard to the platform on which it will finally run because the code is portable to a variety of different platforms. To be fully portable, no vendor-provided extensions should be used.

**Substitutability.** Substitutability allows users to substitute one vendor's product for those of another vendor. One advantage is that it increases competition among vendors. For example, because it is possible for a user to swap one vendor's machine with another vendor's machine, both vendors work harder to keep their customers happy. As a result, vendors must find new ways to differentiate themselves from their competitors. One way they do this is by developing new technologies. In an effort to stay ahead of their competitors, vendors have cut the development life cycle and are constantly adding new features to their products. In addition, where they cannot differentiate themselves on technology alone, vendors reduce prices. This competition allows users to purchase increasingly powerful machines at much lower costs. Software should also be substitutable where possible. The less effect a change in vendor products has on other parts of a system, the greater the level of standards-based systems. Another advantage is the infusion of technology. IHS can decide upon vendor products based on technological features and avoid purchasing a product because it is the only one that integrates with its current system.

**Scalability.** Scalability allows the system to grow to meet user demands through increased hardware computing power. By implementing standards-based systems, software can be moved to a more powerful hardware platform without affecting the business application. For instance, a system can expand to meet an increase in user workload by moving to an Symmetric Multi Processing (SMP) system or mainframe from a single processor database server. This system is scaling up by using a more powerful hardware platform without modifying the business application.

Exhibit 3-4 lists system, communication, information, human/computer interaction, and security services.

**Exhibit 3-4: Summary of Standards**

<b>System Services</b>			
Language Services	Software development	M (MUMPS), Visual Basic, C++, JAVA, Delphi	
Core System Services	Client workstation	MS Windows NT 4.0, Windows 2000 (emerging)	
	Operating system	MS Windows NT Server 4.0, UNIX, Linux, Windows 2000 ( <i>emerging</i> )	
	System management services	MS SMS v2, MIB-II, RMON (IETF RFC 1155,1213, 1757). Tivoli, Peregrine	
<b>Communications Services</b>			
API Services	Client/server communication	RPC Broker, XML ( <i>emerging</i> )	
	Network management	SNMP v2 (IETF RFC 1157)	
	Collaboration-data communications (If needed)	<a href="http://www.itu.int/itudoc/itu-t/rec/t/">http://www.itu.int/itudoc/itu-t/rec/t/</a> for Series T Recommendations—Terminals for telematic services	
	Naming services	DNS (IETF RFC 1034, 1035, and <a href="http://www.dns.net/dnsrd/rfc/">http://www.dns.net/dnsrd/rfc/</a> for other DNS RFCs)	
	Directory services	ITU-T X.500, LDAP (IETF RFC 1777)	
EEI Services	Network connectivity	TCP/IP (IETF RFC 791, 793, 919, 922, 959, 1112), DHCP (IETF RFC 2131), ICMP (IETF RFC 792) DDP, DCP, IIOP	
	File transfer	FTP (IETF RFC 959)	
	Character-Based Connectivity	TELNET (IETF RFC 854, 855, 856)	
	Mail delivery	SMTP (IETF RFC 821, 1869, 1870), SMTP to X.400 Gateway (IETF RFC 1327, 1495), IMAP v4 (IETF RFC 1730, 1734, 2060)	
	Multimedia—video	<a href="http://www.itu.int/itudoc/itu-t/rec/h/">http://www.itu.int/itudoc/itu-t/rec/h/</a> for Series H Recommendations—Audiovisual and multimedia systems	
	WAN	WAN sub-network technologies	Frame Relay (ANSI T1.618)
	LAN	LAN wiring	100 Mb Fiber optic backbone (ISO 9314), Category 5 UTP cabling (CAT-5)
		Wireless LAN	IEEE 802.11
		Carrier Sense Multiple Access/Collision Detection (CSMA/CD)	10-Base-T Ethernet (IEEE 802.3:1985), 100-Base-T Fast Ethernet (IEEE 802.3u), 1000-Base-T Gigabit Ethernet (IEEE 802.3z, 802.3ab))

<b>Information Services</b>		
Supporting Applications	Office development	MS BackOffice
	Office automation	MS Office 2000
	Electronic mail	MS Exchange 5.5, MIME (IETF RFC 1521, 1522), S/MIME (IETF RFC 2311), MS Exchange 2000 (emerging)
Document Management Services	Document distribution format	Portable Document Format (PDF), Rich Text Format (RTF), MS Word (DOC)
Data Management Services, Database Services	Database Management System	FileMan, RDBMS, ORDBMS
	Repository	Interactive Clinical Data Repository
	Patient Record Architecture	HL7 PRA, GCPR PRA
Vocabulary Services	Lexicon	VistA Lexicon Utility, CORBAmed TQS (Terminology Query Service)
	Drug codes	NDC
	Dental codes	ADA Codes
	Lab and clinical observation codes	LOINC
	Multi-axial coded medical nomenclature	SNOMED
	Outpatient procedure codes	CPT-4
	Recording of patient diagnosis	ICD-9-CM, ICD-10 (emerging)
	Metadata	ISO 11179, ANSI X3.285, Extensible Metadata Interchange (XMI), Meta Object Facility (MOF)
Data Interchange Services Data Access Services	Clinical information (text-based)	HL7 2.3 (3.0 EMERGING)
	Insurance, eligibility, managed care information	ASC X12, HL7 2.3 (3.0 EMERGING)
	Medical images	DICOM 3.0
	SQL	SQL-based applications, environments and tool sets (ANSI X3.135-1992, ISO 9075:1992, FIPS Pub 127-2, FIPS Pub 193)
	Open Database Connect (ODBC)	ODBC (ISO/IEC 10027)

	Digital image compression	JPEG (ISO/IEC 10918.1-2), GIF, TIFF
	Video compression	MPEG1(ISO/IEC 11172.1-4), MPEG2 (ISO/IEC 13818)
	Documents and Hypertext documents	SGML (ISO 8879:1986), XML (W3C REC-XML-19980210), HyperText Markup Language (HTML) 4.0 (IETF RFC 1866)
	Electronic Data Interchange (EDI)	X.435 (1991), ANSI X12, FIPS Pub 161-2
	Computer-based training	AICC Guidelines and Recommendations AGR 006
	Patient identification	ASTM E1714, CORBAMED PIDS
Object Services	Object Management Architecture	ActiveX specification(Open Group ); CORBA (OMG 2.1:1997), COM (Microsoft)
Web Services	Server	MS Internet Information Server (IIS)
	Client	MS Internet Explorer (IE) 4.x, Netscape Navigator 4.x (external only)
	File sharing	HyperText Transfer Protocol (HTTP) (IETF RFC 2068:1997), CGI (ISO/IEC 9636)
	Computer-based training	AICC Guidelines and Recommendations AGR 010
<b>Human/Computer Interaction Services</b>		
User Command Interface Services	Native Operating System	MS NT 4.0, Windows 2000 (emerging)
Character-based User Interface Services		TELNET, TELNET 3270 (IETF RFC 854, 855, 856, 1576)
Windowing System Services	Native windowing environment	MS NT 4.0, Windows 2000 (emerging)
Graphics Services		Open GL, CGM (ISO/IEC 8632, FIPS Pub 128-2), GKS (FIPS Pub 120-1)
Application Software Development Support Services	Graphical representations of Enterprise and system functions	FIPS Pub 183 modeling techniques, UML 1.1 (OMG 1.1:1997)
	Logical model of information system data	FIPS Pub 184 modeling techniques
<b>Security Services</b>		
<b>Technical Security</b>		
Identification	Unique identifier(s)	ASTM E1714
Authentication	Access codes, electronic signature, digital	ASTM E1762, ASTM E1985, ASTM PS 101, ASTM PS 102, IETF RFC 2459, IETF RFC 2510, ISO/IEC

	signature	9594, IETF RFC 1767, FIPS Pub 112, FIPS Pub 181, FIPS Pub 190, ISO/IEC 9798-1, ISO/IEC 9798-2
Access Control	Access codes, access control lists and digital signature	ASTM E1762, ASTM E1869, ASTM PS 100, ASTM PS 101, ITU-T X.500, IETF RFC 1777 (LDAP), NIST SP 800-14, IETF RFC 2459, IETF RFC 2510 and ISO/IEC 9594, FIPS Pub 190.
Authorization	Enterprise directory and authorization system	ASTM E1985, ITU-T X.500, IETF RFC 1777(LDAP)
Accountability	Audit trails, alarms, logs, receipts	ASTM E1769, ASTM E1869, ISO/IEC 10164-4 through 10164-8, ISO/IEC 10181-7
Data Integrity	Audit trails, encryption and authentication	ASTM E1762, ASTM E1769, IETF RFC 2459, IETF RFC 2510, ISO/IEC 9594, and ASTM PS 100, ASTM PS 101, ASTM PS 102, FIPS Pub 140-1.
Non-Repudiation	digital signature (plus checksum) and encryption	ASTM E1762, ASTM PS 100, ASTM PS 101, IETF RFC 2459, IETF RFC 2510, ISO/IEC 9594, IETF RFC 1767, ISO/IEC 10181-4, FIPS Pub 196.
Availability	Fault tolerance and backup/recovery	ASTM E1769, FIPS Pub 87, FIPS Pub 140-1
Confidentiality	Encryption and key management	ASTM E1762, ASTM E1869, ASTM PS 100, ASTM PS 101, IETF RFC 2459, IETF RFC 2510, ISO/IEC 9594, IETF RFC 1767, IETF RFC 1422, IETF RFC 1423, IETF RFC 1424, FIPS Pub 41, FIPS Pub 185, NIST SP 800-14
Administrative Security Certification	Internal or external evaluation of systems	NIST SP 800-14, FIPS Pub 102, ISO IS 15408, JCAHO
Chain of Trust Partner Agreement	Agreements with third parties to ensure integrity and data confidentiality	ASTM E1869, NIST SP 800-14

## OVERVIEW OF STANDARDS

---

The standards associated with five types of services are described: system services, communication services, information services, human/computer interaction services, and security services.

## SYSTEM SERVICES

---

### Language Services

#### *Software Development*

Required Standard	Standard Overview
The M (the language formally known as MUMPS) and Delphi programming languages shall be used for all in-house application development. C++ will also be used for software development where appropriate. Java will be used as a development language for web applications.	M is available on most platforms, including PC and UNIX. Common capabilities are provided throughout the computer spectrum from desktop processors to enterprise-wide systems. M has a strong emphasis on text handling and database management, with multi-user and multi-tasking support. In addition to its portability, M is popular because it is simple and direct with a relatively small command set, providing the power and flexibility of a 3GL, with the programming ease of a 4GL. The M language has been an ANSI standard since 1977, with updates in 1984, 1990, and 1995. The identical standard has been adopted by ISO, BSI, and FIPS. (ANSI/MDC X11.1/1990, FIPS Pub 125-1, ISO/IEC 11756). <sup>8</sup> Compared to the C programming language whence it came, C++ incorporates an number of OO features that are lacking in C. Java as a programming language is primarily used in the development of web applications. The versions of these languages used in the IHS environment should adhere to the appropriate ANSI or ISO standards.

### Core System Services

#### *Client Workstation Operating System*

Required Standard	Standard Overview
Microsoft Windows NT 4.0 desktop workstation (Windows 98 selectively).	Windows 2000 is an emerging standard.

---

<sup>8</sup> M Technology Resource Center homepage: <http://www.mcenter.com/mtrc/minfomn.html>

*Server Operating System*

Required Standard	Standard Overview
Microsoft Windows NT Server 4.0, UNIX	Windows 2000 is an emerging standard.

*System Management Services*

Required Standard	Standard Overview
Microsoft Systems Management Server (SMS), Management Information Base-II (MIB-II), Remote Monitoring (RMON) (IETF RFC 1155, 1213, 1757), Peregrine and Tivoli software products.	IHS requires a specification for utility programs that will provide system and network administration functions. These administration functions include services such as system monitoring, user resource allocation, user access control, device configuration, file systems, job accounting, queues, system backup, and machine/platform profiles. Systems Management Server is designed to help systems administrators lower their management costs by helping them install and maintain operating systems and applications, discover system configurations, and perform helpdesk operations. <sup>9</sup>

**COMMUNICATIONS SERVICES**

---

**API Services**

*Network Management*

Required Standard	Standard Overview
Simple Network Management Protocol (SNMP) version 2.	IHS requires a standard protocol for network management. SNMP is the TCP/IP standard protocol for providing communications between a network management client program used by a human and a network device such as a gateway or router.

*Naming Services*

Required Standard	Standard Overview
Domain Name Service (DNS).	IHS requires a mechanism that maps domain names to IP (Internet Protocol) addresses for end systems to communicate easily with the IHS network. DNS is a set of distributed databases that enables people to easily identify individual end-system devices using a meaningful, descriptive name instead of an IP address. Domain names are a part of the machine name used in email addresses and in host names. <sup>10</sup>

---

<sup>9</sup> Microsoft SMS homepage: <http://www.microsoft.com/smsgmt/default.asp>

<sup>10</sup> DNS Resources Directory: <http://www.dns.net/dnsrd/>

*Directory Services*

Required Standard	Standard Overview
CCITT ITU-T X.500; ISO-9594 and Lightweight Directory Access Protocol (LDAP) (IETF RFC 1777).	X.500 is the set of ITU-T standards covering directory services. It is a "white pages" for the Internet--a directory of people, computers, services, and of course electronic mail addresses. LDAP is an Internet Engineering Task Force standard that implements a subset of the X.500 standard. LDAP has become more widely implemented than X.500 and it is the standard for directory services on the Internet. MS Active directory is an emerging standard.

***EEI Services***

*Network Connectivity*

Required Standard	Standard Overview
Transmission Control Protocol/Internet Protocol (TCP/IP) – TCP IAB Standard 7 and IP Standard 5 (IETF RFC 791, 793, 919, 922, 959, 1112); Dynamic Host Configuration Protocol (DHCP) (IETF RFC 2131); Internet Control Message Protocol (ICMP) (IETF RFC 792), IIOP.	IHS requires a set of communications protocols to enable its applications and automated information systems to operate, access, manage, and achieve interconnection and communications with global or public networks such as the Internet and Intranet. The TCP/IP protocol family includes transport, file transfer, terminal emulator, messaging, and network management definitions. It provides connection to the Internet, Intranet, or LANs. DHCP and ICMP supplement TCP/IP capabilities.

*File Transfer*

Required Standard	Standard Overview
File Transfer Protocol (FTP) IAB Standard 9 (IETF RFC 959).	IHS requires a standard protocol for transferring files between networked computers. FTP is part of the TCP/IP standard protocol for transferring files between networked computers.
Distributed Data Protocol (DDP)	Non-routable low-overhead fast network protocol used for moving data between RPMS databases. Used to synchronize data between systems.
Distribute CACHE Protocol (DCP)	Distributed CACHE Protocol dynamically caches information where it is needed.

*Character-Based Connectivity*

Required Standard	Standard Overview
Virtual Terminal Communications (TELNET) Standard 8 (IETF RFC 854, 855, 856).	IHS requires a standard protocol for character-based connectivity within a network. TELNET is the TCP/IP standard virtual terminal communications protocol. It allows a user to connect to any server (host) within the bounds of the network.

*Mail Delivery*

<b>Required Standard</b>	<b>Standard Overview</b>
Simple Mail Transfer Protocol (IETF RFC 821, 1869, 1870); Internet Message Access Protocol (IMAP) version 4 (IETF RFC 1730, 1734, 2060).	IHS requires a standard protocol for the exchange of mail between network computers. SMTP is the TCP/IP standard protocol that provides the exchange of mail between network computers. It specifies the exact format of the message to be sent from an SMTP client operating on one computer system to and from an SMTP server on another computer system. IMAP supports use of SMTP over the Internet.
Internet Message Access Protocol	The Internet Message Access Protocol, Version 4rev1 (IMAP4rev1) allows a client to access and manipulate electronic mail messages on a server. IMAP4rev1 permits manipulation of remote message folders, called "mailboxes," in a way that is functionally equivalent to local mailboxes. IMAP4rev1 also provides the capability for an offline client to resynchronize with the server.
Multipurpose Internet Mail Extensions (IETF RFC 2045, 2046, 2047, 2048, 2049)	This extension to Internet e-mail allows transmission of non-textual data, such as graphics, audio, video, and applications data (e.g., spreadsheets and word processing documents). MIME was designed to overcome the inability of SMTP to handle binary data. Message parts can also be labeled to identify to the recipient or to the mail software the type of data contained within the attachment to determine how it should be handled. It is the core Internet standard for multimedia E-mail and a building block of HTTP.

*Mail Message Handling Systems*

<b>Required Standard</b>	<b>Standard Overview</b>
SMTP to X.400 Gateway (IETF RFC 1327, 1495).	X.400 is the set of ITU-T (International Telecommunications Union) communications standards covering electronic mail services data networks provide. It is widely used in Europe and Canada. It is the International standard for a store-and-forward message handling system in a multi-vendor environment. The SMTP to X.400 gateway will be used to communicate with X.400 mail systems.

**WAN Services**

*Wan Sub-Network Technologies*

Required Standard	Standard Overview
Frame relay (ANSI T1.618) and Asynchronous Transfer Mode (ATM) (ANSI T1.627, T1.629, T1.630, and IETF RFC 1483).	IHS requires standards for sub-network technologies to support the variety of services and traffic types on the Network. The Network needs an environment that accommodates bandwidth requirements for complex networked applications such as those used for data, video, and voice communications. Frame relay and ATM technologies provide capabilities for a high-bandwidth network that can support telemedicine and teleradiology applications. ATM is a telecommunications standard that allows multiple services like voice, data, and video to be mixed over a network. ATM provides the opportunity to integrate LANs and WANs using one network solution. Frame relay is most commonly used for data communications, but supports voice communications as well. <sup>11</sup>

**LAN Services**

*LAN Wiring*

Required Standard	Standard Overview
100Mb backbone (ISO 9314) and Category 5 cabling (CAT-5).	Category 5 cabling is the recommended cable used for LAN wiring and has ANSI specifications. The name derives from the specifications for meeting the requirements of transmitting up to one hundred million bits per second (or 100mbps) across the cable. This is the speed at which a computer, connected to the network, sends data through the CAT-5 cable.

*Wireless LAN*

Required Standard	Standard Overview
T Wireless LAN (IEEE 802.11).	The IEEE 802.11 standard is recommended for wireless LANs. 802.11 defines three characteristics for wireless LANs - diffused infrared, and direct sequence and frequency hopping spread spectrum, the latter two networks operating at the 2.4 GHz band. The standard supports 1- and 2-Mbps data rates, and work is underway with the IEEE 802.11 Working Group for higher speed standards in the 2.4 GHz and 5 GHz frequency bands.

<sup>11</sup> Sub-Network Technologies References:

The ATM Forum homepage: <http://www.atmforum.com/>

Motorola's *Frame Relay Resources* homepage: <http://www.mot.com/MIMS/ISG/tech/frame-relay/resources.html>

CSMA/CD

Required Standard	Standard Overview
10-Base-T Ethernet (IEEE 802.3:1985), 100-Base-T Fast Ethernet (IEEE 802.3u), 1000-Base-T Gigabit Ethernet (IEEE 802.3z, 802.3ab).	<p>Short for Carrier Sense Multiple Access / Collision Detection, a set of rules determining how network devices respond when two devices attempt to use a data channel simultaneously (called a collision). Standard Ethernet networks uses CSMA/CD. This standard enables devices to detect a collision. After detecting a collision, a device waits a random delay time and then attempts to re-transmit the message.</p> <p>10-Base-T is one of several adaptations of the Ethernet (IEEE 802.3) standard for LANs. The 10-Base-T standard (also called twisted pair Ethernet) uses a twisted-pair cable with maximum lengths of 100 meters. The cable is thinner and more flexible than the coaxial cable used for the 10-Base-2 or 10-Base-5 standards.</p> <p>100-BASE-T is a networking standard that supports data transfer rates up to 100 MBPS (100 megabits per second). 100-BASE-T is based on the older Ethernet standard. Because it is 10 times faster than Ethernet, it is often referred to as Fast Ethernet. Officially, the 100-BASE-T standard is IEEE 802.3u.<sup>12</sup> 1000-Base-T is the newest standard. It is referred to as Gigabit Ethernet.</p>

**INFORMATION SERVICES**

**Infrastructure Applications**

*Office Development*

Required Standard	Standard Overview
Microsoft Back Office.	IHS requires an integrated server environment for traditional back office services such as messaging, Internet, and network/desktop management. The family of BackOffice products provides capabilities for fast file and print, communications, messaging and GroupWare, database, host connectivity, systems management, Internet, secure proxy, content creation and web site management, and information retrieval and search services. The BackOffice applications have been designed to integrate into and work with existing legacy systems. <sup>13</sup>

*Office Automation*

Required Standard	Standard Overview
Microsoft Office	IHS requires a suite of office automation applications that support day-to-

<sup>12</sup> CSMA references:

CSMA: [http://webopedia.internet.com/TERM/C/CSMA\\_CD.html](http://webopedia.internet.com/TERM/C/CSMA_CD.html)  
 10Base-T: <http://webopedia.internet.com/TERM/1/10BaseT.html>  
 100Base-T: [http://webopedia.internet.com/TERM/1/100Base\\_T.html](http://webopedia.internet.com/TERM/1/100Base_T.html)

<sup>13</sup> Microsoft BackOffice homepage: <http://backoffice.microsoft.com/>

2000.	day operations such as word processing, spreadsheet, and graphics presentations. MS Office is the most widely used office automation suite. It provides a range of services from word processing, spreadsheets, and database management to email, presentations, and web integration. <sup>14</sup>
-------	---

*Electronic Mail*

<b>Required Standard</b>	<b>Standard Overview</b>
Microsoft Exchange 5.5 using bi-directional SMTP-based Internet gateway connectivity.	<p>IHS business needs require an improved GUI interface to electronic mail and the ability to easily send and receive PC-generated documents. The electronic mail software must provide connectivity to Internet mails and be able to send and receive electronic mail from within and outside IHS.</p> <p>Microsoft Exchange is an enterprise email server. It provides built-in connectivity to the Internet. The Microsoft Exchange Internet Mail Connector provides high-performance SMTP connectivity for fast Internet mail. It combines email and GroupWare applications on a single platform that can be managed with a centralized administration program. It is the most reliable way to send email and access GroupWare applications over the Internet or any other network.</p>

**Document Management Services**

*Document Distribution Format*

<b>Required Standard</b>	<b>Standard Overview</b>
FileMan, Relational Database Final form document distribution should use the Adobe portable document format (PDF) or Rich Text Format (RTF) or Microsoft Word format (DOC).	PDF captures formatting information from a variety of desktop publishing applications, making it possible to send formatted documents and have them appear on the recipient's monitor or printer as they were intended. To view a file in PDF format, you need Adobe Acrobat Reader, a free application distributed by Adobe Systems. <sup>15</sup> RTF is a standard format that most word processors support. Microsoft DOC is a default format used by Microsoft Word.

---

<sup>14</sup> Microsoft Office homepage: <http://www.microsoft.com/office/default.asp>

<sup>15</sup> PDF references:  
<http://webopedia.internet.com/TERM/P/PDF.html>  
 Adobe Systems homepage: <http://www.adobe.com/>

**Database Management Services**

*DATABASE Services*

<b>Required Standard</b>	<b>Standard Overview</b>
FileMan, Relational Database Management System (RDBMS), Object Relational Database Management Systems (ORDBMS).	IHS requires a database environment that provides an interface to access data stored in diverse legacy databases and supports COTS products and the information sharing objectives of the organization. An RDBMS or ORDBMS platform provides data management services for definition, query, update, administration, and security of structured data. A relational database is appropriate for general-purpose data management, especially applications requiring flexibility in data structure and access paths. Most COTS products in the market today operate on RDBMS or ORDBMS platforms with SQL access capabilities.

**Vocabulary Services**

*Clinical Lexicon*

<b>Required Standard</b>	<b>Standard Overview</b>
VistA Lexicon Utility	The VistA Lexicon Utility provides a set of lexical capabilities for use by VistA applications. It contains a set of lexical tools and an extensive vocabulary of concepts and terms based upon UMLS.

*Drug Codes*

<b>Required Standard</b>	<b>Standard Overview</b>
National drug codes (NDC) will be used when identifying drug products.	The FDA and HHS with the support of drug manufacturers produce National drug codes. <sup>16</sup>

*Lab and Clinical Observation Codes*

<b>Required Standard</b>	<b>Standard Overview</b>
Laboratory and clinical observations shall be recorded using logical observation identifiers, names, and codes (LOINC) identifiers.	LOINC creates universal identifiers (result codes) for clinical observations to use in the context of ASTM, DICOM, and HL7 messages; 13,000 codes that are free and downloadable from the Internet. <sup>17</sup>

<sup>16</sup> FDA's NDC homepage: <http://www.fda.gov/cder/ndc/index.htm>

<sup>17</sup> LOINC References:

[www.cpri.org/terminology/loinc](http://www.cpri.org/terminology/loinc)

<http://nelle.mc.duke.edu/standards/HL7/termcode/loinc.htm>

*Dental Codes*

Required Standard	Standard Overview
<p>The CDT contains the American Dental Association's codes for dental procedures and nomenclature and is the nationally accepted set of numeric codes and descriptive terms to report dental treatments. CDT also describes the ADA Dental Claim Form; clinical and dental benefit terminology; and the tooth numbering system.</p>	<p>ADA Codes</p>

**Multi-axial Coded Medical Nomenclature**

*Recording of Patient Diagnosis*

Required Standard	Standard Overview
<p>The International Classification of Diseases, 9<sup>th</sup> Revision, Clinical SNOMED shall be used for recording multi-axial coded medical nomenclature.</p>	<p>SNOMED is the multi-axial coded medical nomenclature for medical vocabulary the College of American Pathologists (CAP) developed. Adherence to SNOMED enables full integration of all medical information in the electronic medical record into a single data structure.<sup>18</sup> CAP has a new effort underway called SNOMED-RT that has the potential to support a broader range of health care encoding needs and that may subsume other coding systems.</p>

*Outpatient Procedure Codes*

Required Standard	Standard Overview
<p>All outpatient procedures shall be encoded using standardized procedure codes (CPT-4).</p>	<p>The <i>Current Procedural Terminology, 4<sup>th</sup> Edition (CPT-4)</i> lists descriptive terms and identifying codes for reporting medical services and procedures. The CPT provides a uniform language that describes medical, surgical, and diagnostic services, and thereby serves as an effective means for reliable nationwide communication among physicians, patients, and third parties.</p> <p>This terminology system is the most widely accepted medical nomenclature to report medical procedures and services under public and private health insurance programs. CPT is also used for administrative management, such as claims processing and developing guidelines for medical care review. Using standardized procedure codes enables billing, which can increase non-appropriated funds available to IHS.<sup>19</sup></p>

<sup>18</sup> SNOMED homepage: <http://snomed.org/>

<sup>19</sup> CPT-4 References:

AMA's CPT site: <http://www.ama-assn.org/med-sci/cpt/process.htm>

HFMA's CPT site: <http://www.hma.com/98cptcodes.html>

Recording of Patient Diagnosis

Required Standard	Standard Overview
<p>The International Classification of Diseases, 9<sup>th</sup> Revision, Clinical Modification (ICD-9-CM) shall be used to record patient diagnosis and subsequent institutional billing.</p>	<p>ICD-9-CM is a classification system that groups related disease entities and procedures to report statistical information. The National Center for Health Statistics developed clinical modification of the ICD-9 to use in the United States. The Central Office on ICD-9-CM was created through a written Memorandum of Understanding between the American Hospital Association (AHA), the World Health Organization, and the National Center for Health Statistics (NCHS) in 1963. Responsibility for maintaining the classification system is shared between NCHS (diagnosis classification) and the Health Care Financing Administration, or HCFA (procedure classification).<sup>20</sup></p> <p>ICD-10, the successor to ICD-9, is under development and will become the preferred diagnostic coding system in the near future.</p>

Metadata

Required Standard	Standard Overview
<p>ISO/IEC 11179, ANSI X3.285, XML Metadata Interchange (XMI) and MOF standards shall be used to specify, exchange, and standardize data about data (metadata).</p>	<p>NCITS L8 is concerned with developing proposed standards (notably ISO/IEC 11179 and ANSI X3.285) that will facilitate the standardized naming, definition, and description of data elements. NCITS L8 on Data Representation is a technical committee of the National Committee on IT Standards (NCITS) Accredited Standards Committee X3. NCITS L8 establishes standards to specify and standardize data. The work's focus is to establish ways to describe data to facilitate human use and to enable intelligent computer processing. Metadata issues the committee covered include naming, identification, definitions, classification, and registration. The standards the committee developed are used in many areas, such as: Electronic Data Interchange (EDI); data administration; information management; application development for information systems; and data access/interchange via the World Wide Web (WWW) and National Information Infrastructure (NII).<sup>21</sup> XMI and MOF are OMG standards that support metadata exchange.</p> <p>The XML XMI format specifies an open information interchange model that is intended to enable developers working with object technology to exchange standardized programming data over the Internet, thus bringing consistency and compatibility to applications created in collaborative environments. The OMG's MOF specification defines a common framework to represent metadata. At the moment, the MOF is restricted to providing metadata for CORBA-based systems because the only defined way to interchange MOF metadata is to use the CORBA interfaces the MOF's IDL mapping produced. XML (in the form of XMI) provides a way to lift this restriction.</p>

<sup>20</sup> ICD-9-CM homepage: <http://www.icd-9-cm.org/>

<sup>21</sup> Ernest Orlando Lawrence Berkeley National Laboratory NCITS web site: <http://www.lbl.gov/~olken/X3L8/index.html>

**Data Interchange Services**

*Text-Based Clinical Information*

Required Standard	Standard Overview
Health Level 7 (HL7), version 2.3 (or later versions) shall be used for peer-to-peer exchange of clinical, text-based information.	<p>IHS requires a messaging capability for health information that provides the support, flexibility, efficiency, and ease of implementation required to meet the organization's information sharing objectives. IHS must be able to share information easily within its facilities and with external organizations at low cost and use COTS products when appropriate.</p> <p>HL7 is an ANSI approved standard messaging protocol that specifies the transactions and encoding rules for EDI between various health care computing systems. Its membership is directly focused on health care Informatics standards and cooperates closely with developers of other standards.<sup>22</sup></p>

*Insurance, Eligibility, Managed Care Information*

Required Standard	Standard Overview
Insurance, eligibility, and managed care information shall be exchanged using the ANSI Accredited Standards Committee (ASC) X12 standard along with HL7.	<p>HIPAA regulations will mandate the use of the ASC X12 standard to exchange business and administrative information. Through using the standard, all institutions can enjoy the efficiencies of a common interchange language, rather than experience the difficulties of a methods and procedures proliferation that could occur if each institution imposed its own format on every institution with which it does business.<sup>23</sup></p>

*Medical Images*

Required Standard	Standard Overview
DICOM 3 and HL7 2.3 (3.0 EMERGING).	<p>DICOM develops standards to support the exchange of medical images and related information. DICOM is used primarily in radiological and other imaging applications.<sup>24</sup></p> <p>Clinical images will be exchanged between imaging systems using DICOM 3. Data exchanges between imaging systems and health information systems will use HL7.</p>

*SQL Access*

Required Standard	Standard Overview
SQL-based applications and tool sets will comply with published national standards: ANSI X3.135-1992, ISO 9075:1992, FIPS Pub 127-2, FIPS Pub	Adherence to published national standards results in the increased portability of applications and the cross-application use of tool sets.

<sup>22</sup> HL7 reference: <http://www.hl7.org/>

<sup>23</sup> X12 reference: <http://polaris.disa.org/index.html>

<sup>24</sup> DICOM reference: [http://www.xray.hmc.psu.edu/dicom/dicom\\_home.html](http://www.xray.hmc.psu.edu/dicom/dicom_home.html)

193.	
------	--

*SQL and Open Database Connect (ODBC) Interfaces to Databases*

Required Standard	Standard Overview
Data management interfaces to RDBMS systems shall be uniform, consistent, and allow for SQL (ISO 9075:1992) and ODBC (ISO/IEC 10027) access.	Data management interfaces to RDBMS systems shall be uniform and consistent. Developed by Microsoft, Open Database Connectivity (ODBC) is a standard database access method. The ODBC's goal is to make it possible to access any data from any application, regardless of which DBMS is handling the data. <sup>25</sup>

*Digital Image Compression*

Required Standard	Standard Overview
Digital images shall be encoded using Joint Photographic Experts Group (JPEG) grayscale and color data compression formats (ISO/IEC 10918.1-2), Graphic Interchange Format (GIF) standard formats, or TIFF formats.	JPEG is a standardized method to compress and code continuous-tone (gray scale or full color) digital still image data. It is applicable to a wide range of applications that use compressed images. The primary use is as a standardized way of compressing and storing both 24-bit color and gray-scale images. With this specification, compressed formatted image files are more efficiently transmitted across networks. GIF is also a widely used standard format. TIFF is a loss-less compression scheme that will be considered for storing medical images.

*Video Compression*

Required Standard	Standard Overview
Video data shall be encoded using Motion Picture Experts Group 1 (MPEG-1) video data compression format (ISO/IEC 11172.1-4) or MPEG-2 (ISO/IEC 13818).	The MPEG compression standards are intended for full-motion image compression for high-performance entertainment-quality video. MPEG-1 provides video compression for multimedia applications. It addresses compressing video signals up to 1.5 megabits/second. MPEG-2 is a further enhancement over MPEG-1. The digital video, graphics, and moving image communities widely use MPEG compression techniques for both storing and transmitting digital moving images.

---

<sup>25</sup> ODBC references:  
 ODBC 3.0, SQL call level data management interface, SQL-3 part3  
 Microsoft's ODBC site: <http://www.microsoft.com/data/odbc/>

*Documents and Hypertext Documents*

Required Standard	Standard Overview
Document and hypertext document representation, structure, and exchange will meet the standard generalized markup language (SGML) standard (ANSI/ISO 8879:1986), the extensible markup language (XML) standard (W3C REC-XML-19980210), and the HTML 4.0) standard (IETF RFC 1866).	IHS needs to adopt a standardized electronic interchange format to manage mixed-mode document structure and content. SGML formally defines the grammar of languages for document markup. SGML provides a way to specify a particular allowed markup, what is required or optional, and how the markup is distinguished from the text. By defining the structure in a standard syntax, SGML enables document interchange across applications and computing platforms and provides a universal way to identify, manage, and share document elements. XML and HTML are subsets of SGML. They are used to exchange and display information on the WWW. The benefits of HTML and XML are their relative simplicity and independence from operating system, server, or client platforms. <sup>26</sup>

*EDI*

Required Standard	Standard Overview
CCITT ITU-T X.435 (1991), ASC X12, and FIPS Pub 161-2 standards shall be used for EDI.	EDI is the application-to-application electronic exchange of business data in a standardized, digital, computer-readable format. EDI is a procedure in which documents to be interchanged between separate organizations are converted to strictly formatted sequences of data elements and transmitted as messages between computers. EDI provides a mechanism for the electronic exchange of data that traditionally is conveyed on paper documents. EDI standards are available from a variety of organizations for specific data types.

*Unique Health Care Identifier*

Required Standard	Standard Overview
The IHS Master Person Index (MPI) system shall create and maintain unique health care identifiers <sup>27</sup> in accordance with the ASTM E1714 standard. The MPI system shall support application programming interfaces based upon the CORBAmed Person Identification Service (PIDS) standard and the HL7 standard. The MPI shall also federate with other MPI systems using the PIDS standard.	The term unique health care identifier should be understood to mean a number (or other identifying code) that identifies one, and only one, person, used to manage all health information.

<sup>26</sup> Gartner Group. *Strategic Analysis Report* (R-200-132). April 1996.

<sup>27</sup> ASTM. *Guide for the Properties of a Universal Health care Identifier*, E1714, 1995; ASTM E31 reference: <http://www.astm.org/COMMIT/e-31.htm>

**Object Services**

*Object Management Architecture*

Required Standard	Standard Overview
<p>A defined object management architecture and object request specification shall be used for peer-to-peer exchanges between object-based systems. Standards that shall be used are CORBA 2.1: 1997, the ActiveX (Open Group) specification (formerly object linking and embedding—OLE) and COM (Microsoft).</p>	<p>The Object Management Group (OMG) is an industry-independent consortium dedicated to developing object-based application integration standards. CORBA (common object request broker architecture)<sup>28</sup> is OMG's specification for providing network-based application services to facilitate data and logic sharing between applications.</p> <p>The component object model (COM) is Microsoft's specification for building applications that can share data and functionality using the Active X specification over a network.</p>

**Web Services**

*Server*

Required Standard	Standard Overview
<p>Microsoft Internet Information Server (IIS).</p>	<p>IHS requires ways to integrate, manage, and distribute its live and on-line web application information and functions. IHS needs a high-performance web server that addresses its information management needs.</p> <p>The MS Internet Information Server is built into the Windows NT Server operating system, which is also an IIS standard. MS IIS is a high-performance, secure, WWW platform for creating, managing, and intelligently distributing information and supporting live on-line applications.<sup>29</sup></p>

*Client*

Required Standard	Standard Overview
<p>MS Internet Explorer (IE) 4.x by Microsoft Corporation is required for Intranet and Internet access. Netscape Navigator 4.x by Netscape Communications Corporation</p>	<p>IHS requires browsers to provide client interconnection services to access global or public networks, such as the Internet and interconnection services to the IHS Intranet. The MS Internet Explorer<sup>30</sup> is built into the Windows NT 4.0 workstation, which also meets IHS standards. Both MS IE and Netscape Navigator<sup>31</sup> provide layout and page presentation capabilities to</p>

<sup>28</sup> CORBA reference: <http://www.omg.org/corba/beginners.html>

<sup>29</sup> Microsoft IIS homepage: <http://www.microsoft.com/ntserver/Basics/WebServices/default.asp>

<sup>30</sup> Microsoft IE homepage: [http://www.microsoft.com/products/prodref/206\\_ov.htm](http://www.microsoft.com/products/prodref/206_ov.htm)

<sup>31</sup> Netscape homepage: <http://www.netscape.com/>

is supported for accessing web applications external to IHS only.	any Internet client and are able to incorporate various multi-media capabilities, such as video, audio, and animation.
---	--

**Human/Computer Interaction Services**

*User Command Interface Services*

Required Standard	Standard Overview
Microsoft Windows NT 4.0 (or later versions).	Because MS Windows NT 4.0, or later versions, is the standard operating system on client workstations, by default it is also the user command interface. Windows 2000, the successor to NT 4.0, is currently becoming the standard operating system.

*Character-based User Interface Services*

Required Standard	Standard Overview
TELNET, TELNET 3270 (IETF RFC 854, 855, 856, 1576).	TELNET and TELNET 3270 are part of the TCP/IP suite of communication applications. They support character-based interfaces to applications across a network.

*Windowing System Services*

Required Standard	Standard Overview
Microsoft Windows NT 4.0 (or later versions).	Because MS Windows NT 4.0, or later versions, is the standard operating system on client workstations, by default it is also the windowing system interface. Windows 2000, the successor to NT 4.0, is currently becoming the standard operating system.

*Graphics Services*

Required Standard	Standard Overview
Open GL, CGM (ISO 8632.1-4) and GKS (ISO/IEC 8651-4).	Open GL is a widely used industry standard for developing portable, interactive 2D and 3D graphics applications. CGM is a robust vector graphics data format. GKS is an international standard that defines a basic two-dimensional graphics system. It provides applications programmers with standard methods to create, manipulate, and display or print computer graphics on different types of computer graphics output devices. It provides an abstraction to save programmers from dealing with the detailed capabilities and interfaces of specific hardware.

**Application Software Development Support Services**

*Graphical Representations*

Required Standard	Standard Overview
<p>Structured graphical representations of enterprise and system functions (modeling language, rules, and techniques) shall be maintained using the Unified Modeling Language (UML) 1.1:1997.</p>	<p>The Unified Modeling Language (UML) specifies, visualizes, constructs, and documents the artifacts of software systems, business modeling, and other non-software systems. The UML represents a collection of best engineering practices that have proven successful in modeling large and complex systems.</p>

**SECURITY SERVICES**

*Identification and Authentication*

Required Standard	Standard Overview
<p>ASTM 1714, Properties of a Universal Health Care Identifier; HHS regulations implementing HIPAA legislation for Individual, Provider, Employer, and Payer Identifiers; ASTM 1762, Standard Guide for Electronic Authentication of Health Information; ASTM 1985, Guide for User Authentication and Authorization; ASTM PS 101, Provisional Standard Guide on Security Framework for Health Care Information; ASTM PS 102, Provisional Standard Guide for Internet and Intranet Health Care Security; IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile; IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols; ISO/IEC 9594-8 (ITU-T Recommendation X.509), IT – Open Systems Interconnection: The Directory: Authentication Framework,; IETF RFC 1767, MIME Encapsulation of EDI Objects; FIPS Pub 112, Standard on Password Usage; FIPS Pub 181, Announcing the Standard for Automated Password Generator; ISO/IEC 9798-1, IT—Security Techniques—Entity Authentication Mechanisms—Part 1: General Model; ISO/IEC 9798-2, IT—Security Techniques—Entity Authentication Mechanisms—Part 2: Entity Authentication Using Symmetric Techniques.</p>	<p>Security in general and security as it relates to health care in particular, is complex. Simplification is achieved by viewing security as a set of services, but even then standards related to each security service proliferate. This section of the standards profile provides an overview of security standards as they relate to the rest of the standards in the profile. For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.</p>

*Access Control and Authorization*

Required Standard	Standard Overview
ASTM 1762, Standard Guide for Electronic Authentication of Health Information; ASTM 1869, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records; ASTM PS 100, Provisional Specification for Authentication of Health care Information Using Digital Signatures; ASTM PS 101, Provisional Standard Guide on Security Framework for Health Care Information; ASTM 1985, Guide for User Authentication and Authorization; ITU-T X.500, Directory Service; IETF RFC 1777, Lightweight Directory Access Protocol; IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile; IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols, ISO/IEC 9594-8 (ITU-T Recommendation X.509); IT – Open Systems Interconnection: The Directory: Authentication Framework; NIST SP 800-14, Generally Accepted Principles and Practices for Securing IT Systems.	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Accountability*

Required Standard	Standard Overview
ASTM 1769, Standard Guide for Properties of Electronic Health Records and Record Systems; ASTM 1869, Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records; ISO/IEC 10164-4 through 10164-8, IT—Open Systems Connection—System Management; ISO/IEC 10181-7, IT—Security Frameworks in Open Systems—Security Audit Framework.	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Data Integrity and Non-Repudiation*

Required Standard	Standard Overview
ASTM 1762, Standard Guide for Electronic Authentication of Health Information; ASTM 1769, Standard Guide for Properties of Electronic Health Records and Record Systems; ASTM PS 100, Provisional Specification for Authentication of Health Care Information Using Digital Signatures; ASTM PS 101, Provisional Standard Guide on Security Framework for Health Care Information; ASTM PS 102, Provisional Standard Guide for Internet and Intranet Health Care Security; IETF RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile; IETF RFC 2510, Internet X.509 Public Key Infrastructure Certificate Management Protocols, ISO/IEC 9594-8 (ITU-T Recommendation X.509); IT—Open Systems Interconnection: The Directory: Authentication Framework; IETF RFC 1767, MIME Encapsulation of EDI Objects; ISO/IEC 10181-4, IT—	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

Security Frameworks in Open Systems—Non-repudiation.	
--	--

*Availability*

Required Standard	Standard Overview
ASTM 1769, <i>Standard Guide for Properties of Electronic Health Records and Record Systems</i> ; FIPS Pub 87, <i>Guidelines for ADP Contingency Planning</i> ; FIPS Pub 140-1, <i>Security Requirements for Cryptographic Modules</i>	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA

*Confidentiality*

Required Standard	Standard Overview
ASTM 1762, <i>Standard Guide for Electronic Authentication of Health Information</i> ; ASTM 1869, <i>Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records</i> ; ASTM PS 100, <i>Provisional Specification for Authentication of Health Care Information Using Digital Signatures</i> ; ASTM PS 101, <i>Provisional Standard Guide on Security Framework for Health Care Information</i> ; IETF RFC 2459, <i>Internet X.509 Public Key Infrastructure Certificate and CRL Profile</i> ; IETF RFC 2510, <i>Internet X.509 Public Key Infrastructure Certificate Management Protocols</i> , ISO/IEC 9594-8 (ITU-T Recommendation X.509); IT—Open Systems Interconnection: The Directory: <i>Authentication Framework</i> ; IETF RFC 1767, <i>MIME Encapsulation of EDI Objects</i> ; IETF RFC 1422, <i>Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management</i> ; IETF RFC 1423, <i>Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers</i> ; IETF RFC 1424, <i>Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers</i> ; FIPS Pub 41, <i>Computer Security Guidelines for Implementing the Privacy Act of 1974</i> ; FIPS Pub 185, <i>Escrowed Encryption Standard (EES)</i> ; NIST SP 800-14, <i>Generally Accepted Principles and Practices for Securing IT Systems</i> .	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Certification*

Required Standard	Standard Overview
NIST SP 800-14, <i>Generally Accepted Principles and Practices for Securing IT Systems</i> ; FIPS Pub 102, <i>Guidelines for Computer Security Certification and Accreditation</i> ; ISO IS 15408, <i>The Common Criteria for IT Security Evaluation (CC) version 2.0</i> ; JCAHO.	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Chain of Trust Partner Agreement*

Required Standard	Standard Overview
ASTM 1869, <i>Standard Guide for Confidentiality, Privacy, Access, and Data Security Principles for Health Information Including Computer-Based Patient Records</i> ; NIST SP 800-14, <i>Generally Accepted Principles and Practices for Securing IT Systems</i> ; FIPS Pub 102, <i>Guidelines for Computer Security Certification</i> .	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Enumeration*

Required Standard	Standard Overview
ASTM 1986, <i>Standard Guide for Information Access Privileges to Health Information</i> .	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Credentialing*

Required Standard	Standard Overview
<i>IHS Policy</i>	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

*Privileging*

Required Standard	Standard Overview
IHS Policy	For an in depth discussion of security and security standards, refer to the Security Architecture Framework section of the EA.

## **CURRENT ENVIRONMENT**

This section describes the current IHS environment, including the business architecture, network architecture, application software environment, and hardware architecture.

### **CURRENT BUSINESS ARCHITECTURE**

---

The IHS, as the HHS Operating Division charged with administering the principal health program for AI/AN, provides comprehensive health services through a system of I/T/U facilities and programs. I/T/U facilities provide health services to 1.4 million AI/AN through 144 service units composed of 500 direct health care delivery facilities, including 49 hospitals, 190 health centers, 7 school health centers, and 287 health stations, satellite clinics, and Alaskan village clinics. Within this system, Indian tribes who have elected to administer their own health services deliver IHS-funded services to their own communities with over 30 percent of the IHS budget in 11 hospitals, 129 health centers, 3 school health centers, and 240 health stations. Tribes who retained the Federal administration of their health services or deferred tribal assumption of the IHS program until a later time deliver IHS-funded services to their communities with 65 percent of the IHS budget in 38 hospitals, 61 health centers, 4 school health centers, and 47 health stations. The services include traditional inpatient and ambulatory care and extensive preventive care, which focus on health promotion and disease prevention.

In addition, various health care and referral services are provided to Indian people in off-reservation settings through 34 urban programs. Another integral part of the program is purchasing services from non-IHS providers to support, or in lieu of, direct care facilities.

### **IHS NETWORK ARCHITECTURE**

---

The IHS data network is composed of two distinct parts: The Backbone network and the Area-to-Health-Facility network. The Backbone network (IHSNET) is composed of high-speed T1 point-to-point lines connecting the twelve IHS AOs, the California Rural Indian Health Board (CRIHB), and the HQ offices in Rockville, Maryland, and Albuquerque, New Mexico. The Area-to-Health-Facility Network (ATHFNET) connects 450 Health Care Facilities (HCF) located in the continental United States and Alaska. The network supports many agency activities including agency-wide email and Internet access, patient data access and entry, telemedicine, teleradiology, information posting, continuing education, distance learning, and productivity enhancement tools.

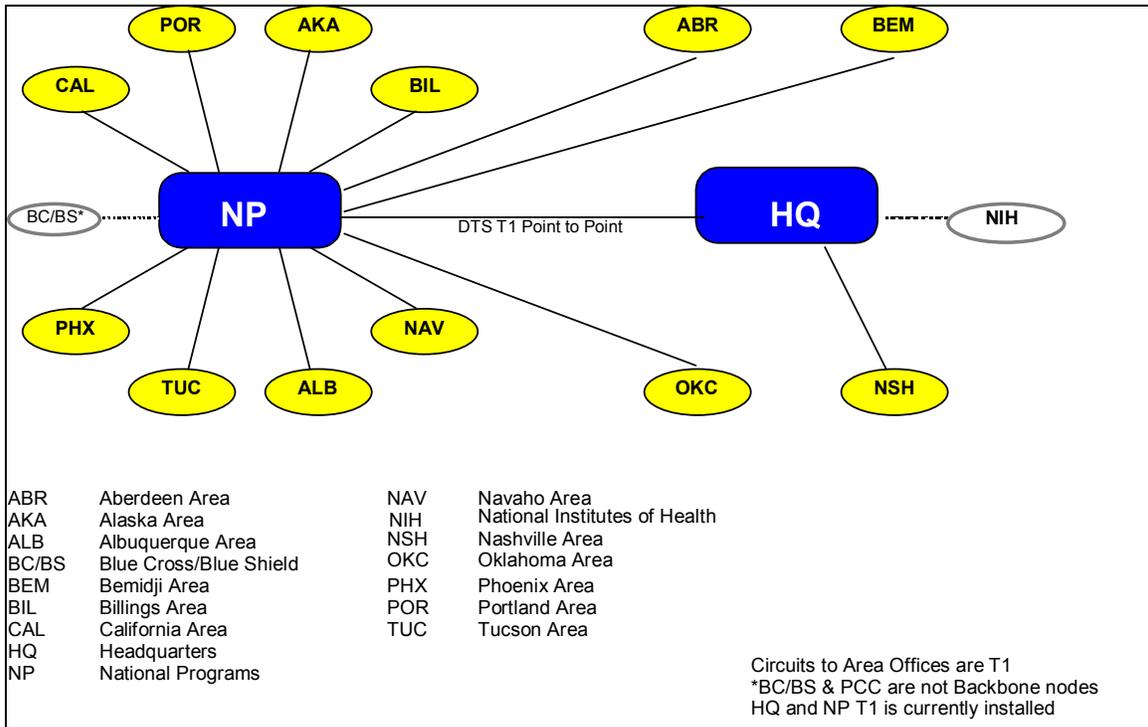
Two nodes of the network, HQ and the NP in Albuquerque, are connected to the VA, HHS, and other organizations to support patient statistical data, financial applications, third-party billing, external agency data collection, payroll distribution, and network sharing between the IHS and Tribal/Urban Sites.

The IHS maintains a network control center in the NP offices in Albuquerque. All network monitoring, programming, and tuning is conducted from the NP office. The following external services are provided using IHSNET:

- NIH Data Center - CIT in Bethesda, Maryland, supports IHS financial applications/management for RPMS and IHS payroll distribution.
- Social Security Administration (SSA) provides research and certification of social security numbers for RPMS patient identification.
- VA exchanges information with IHS.
- Blue Cross/Blue Shield (BC/BS) of Texas supports third-party billing for RPMS
- Blue Cross/Blue Shield of New Mexico is the FI for IHS Contract Health Services (CHS).

The IHSNET has a modified star/tree topology as shown in Exhibit 4–1. This Wide Area Network (WAN) forms the backbone network for the IHS and connects the twelve AOs and the CRIHB to HQ and the NP. AOs provide connectivity to Service Units, and Service Units support connectivity to local clinics. The external computer services are connected to HQ and the NP in Albuquerque. HQ offices are connected via a dedicated T1 link and the AOs connect to HQ/NP via dedicated T1 lines.

**Exhibit 4-1: IHSNET Backbone Network**



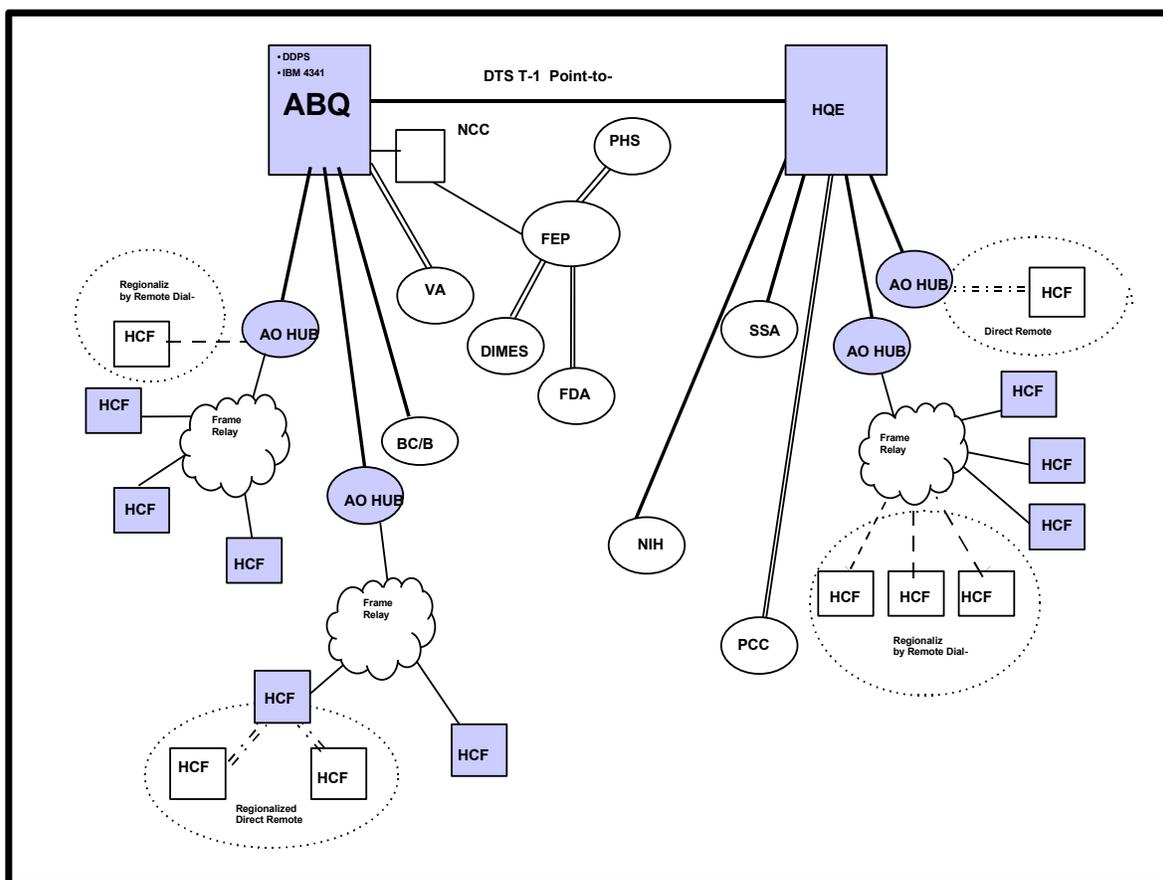
IHS HCFs are categorized using 1990 statistics:

- High Volume Health Facilities (HVHFs)—those with 5000 and over patient visits/year
- Low Volume Health Facilities (LVHFs)—those with less than 5000 patient visits/year

These categories were used to establish hardware needs for IHS HCFs.

Exhibit 4-2 provides a schematic representation of the IHS network, including details of the technical network components. Only representative facilities are shown.

**Exhibit 4-2: Summary Level of IHS Network Architecture**



A variety of communication equipment supports each local AO. The type of equipment used is based on cost and operational considerations, including data traffic volume, response time requirements, regional connectivity, and functional requirements. This creates a second tier system, the ATHFNET, which is constructed of Frame Relay and X.25 communications lines. The equipment located at the HCFs consists of TCP/IPs routers. This equipment supports protocols, which include System Network Architecture (SNA), TCP/IP, and asynchronous. Currently 56 KBPS to 256 KBPS Frame Relay lines support most HCFs. Most of these facilities contain LANs, which interface with the telecommunications equipment.

## DETAILS OF THE NETWORK ARCHITECTURE

### HQ Office Protocols and Equipment

IBM SNA protocols will continue to be supported from AOs to the NIH CIT. The TCP/IP is currently used to send data from AOs to external organizations, such as NIH CIT and the Blue Cross/Blue Shields of Texas and New Mexico. The

equipment at the AO hubs allows the IHS to support Point-to-Point, Frame Relay, X.25 lines. The protocols this combination of hardware supports are asynchronous, SNA, Synchronous Data Link Control (SDLC), 3270, TCP/IP and asynchronous protocols.

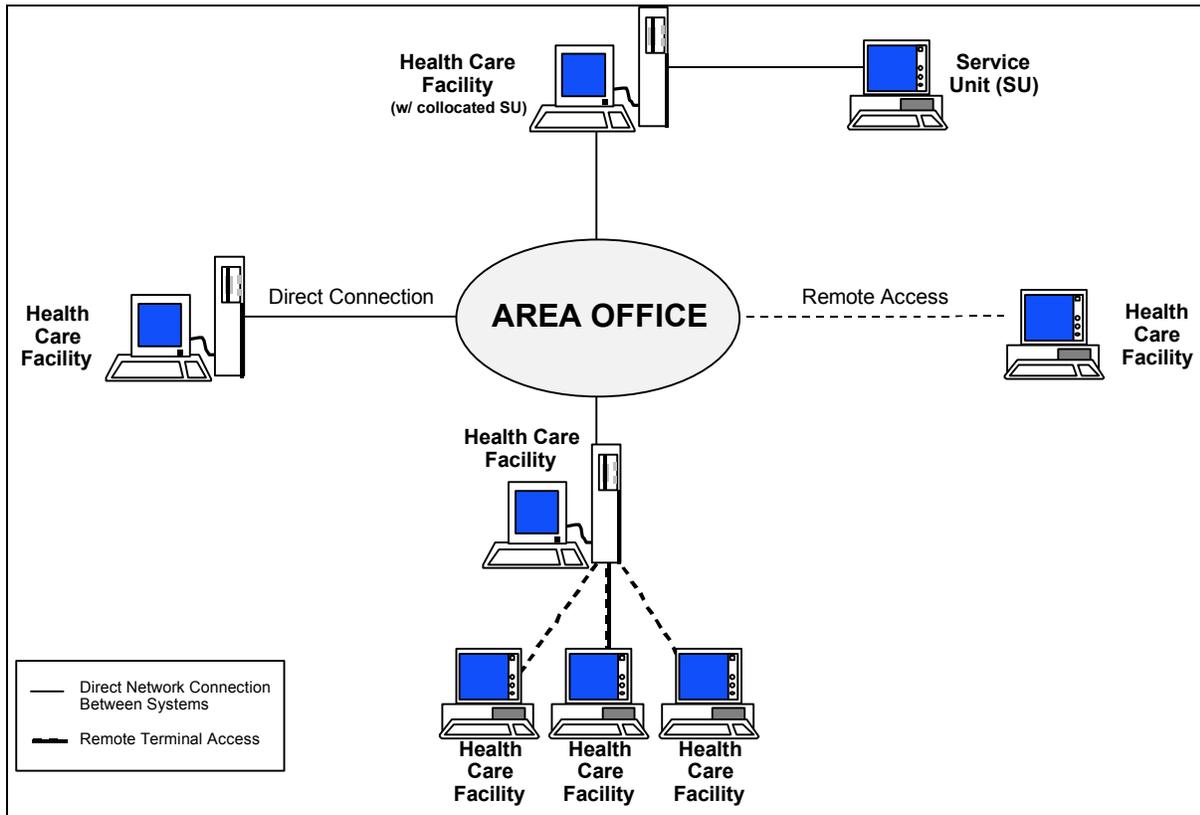
### **Area Regional Hub to HQ Office Connectivity**

AOs that connect to National Programs using T-1 circuits are Alaska, Portland, CRIHB, California, Phoenix, Tucson, Aberdeen, Albuquerque, Bemidji, Billings, Oklahoma, and Navajo. The Nashville AO connects to HQ then National Programs in Albuquerque. The hub sites are typically located at the region's AO. These hub sites have Cisco 4700/7500 series routers. This equipment supports LAN and Client/Server protocols including TCP/IP, Frame Relay, Serial Line Internet Protocol/ Point-to-Point Protocol (SLIP/PPP) and Integrated ISDN, as well as X.25, and SNA. A few of the regional hub sites also allow remote dial-up at speeds from 9.6 KBPS to 56 KBPS for those users who are on travel or require only limited access to the network.

### **Health Care Facility Protocols and Equipment**

The number of ACF WAN nodes has increased from 375 to 450 since 1990 IHS converted most of the dial-up X.25 connections to FTS 2000 network direct X.25 links, reducing circuit costs. HVHF and LVHF designations distinguish the standard communications equipment, which, in turn, defines the connectivity options to the X.25 IHS network. Exhibit 4-3 shows a range of AO-to-Health Care Facility network configurations.

**Exhibit 4-3: AO-to-Health Care Facility Configurations**



### HVHFs Protocols and Equipment

The majority of HVHFs are supporting TCP/IP over Frame Relay networks with 56 KBPS to 256 KBPS line speed. All of the HVHFs, as well as HQ and AOs, are configured to support TCP/IP routing and provide Internet access.

### LVHFs Protocols and Equipment

The LVHFs are largely limited to asynchronous traffic because of the type of communications hardware in use and the limited services local telephone companies provide. The LVHFs use low-end Cisco for X.25 but are typically capable of running Frame Relay or IP. Certain sites are expected to remain with their current equipment where low volume and workload do not warrant the cost of conversion to Frame Relay/IP. With current equipment, LVHFs can run 9.6 KBPS circuits to their X.25 network and support asynchronous traffic.

### External IHS WAN Protocols and Equipment

At least eight external organizations connect to the IHS WAN through 56 KBPS circuits. Most of IHS' needs for external mainframe connections are to support various Resource and Patient Management System (RPMS) applications. Other

access is for external data collection, used for otherwise unavailable information or for IHS approved research.

### **IHS Network Operations and Management Systems**

The primary Network Control Center (NCC) is in Albuquerque with the backup NCC in Rockville. The NCC performs central management and configuration functions needed for the IHS. The NCC uses Cisco network management systems with Sun workstations to provide graphical interfaces to program and monitor the entire network.

### **Internet Services**

IHS has a Domain Name (ihs.gov) and Class B address block (161.223.0.0 - 161.223.255.254) assigned by the InterNIC (Network Information Center).

The IHS supports three Internet Access Points with firewalls at Albuquerque, HQ, and Tucson, Arizona. The main access point is in Albuquerque, which provides domain-wide routing broadcasts. There is currently a gateway located at Tucson (which broadcasts two Class C address blocks—161.223.1-7) to provide access from IHS for Tucson AO. Additionally, a gateway at HQ broadcasts 161.223.223.0 at HQ (which broadcasts 161.223.223).

### **Network Service Applications**

IHS Network services currently support E-mail, Internet Access and File Transport Protocol (FTP) for data transmission and small volumes of images and video. There is limited desktop video and software application sharing. They also provide services such as Televideo, Telemedicine, and Teleradiology, facilitated by circuit sharing for voice, data, and video traffic.

## **APPLICATION SOFTWARE ENVIRONMENT**

---

The IHS application software environment consists of three major components:

- RPMS, a decentralized system of numerous, integrated software applications, which is the primary information system supporting IHS business operations
- NPIRS, the IHS centralized database
- Commercial-off-the-shelf (COTS) software products, such as the Microsoft Office suite, which provides office automation tools, and Internet Information Services (IIS), providing the IHS Web site environment.

The paragraphs that follow describe RPMS and NPIRS functions and software environments, and the RPMS processing platform architecture.

## **RPMS SOFTWARE ARCHITECTURE & ENVIRONMENT**

---

RPMS meets IHS' varying needs to provide information processing capability directly to end users and provides useful and quick access to information. RPMS goes hand-in-hand with the business requirements and mission of IHS because it supports health care delivery to AI/AN.

RPMS is a decentralized automated information system of numerous integrated software applications. Many RPMS applications can function in a stand-alone environment if necessary or appropriate. The system is designed to operate on micro and mini-computers located in I/T/U health care facilities. RPMS has numerous applications<sup>32</sup> with some applications in varying stages of production and development.

RPMS software modules fall into three major categories:

1. Patient-based administrative applications
2. Patient-based clinical applications
3. Financial and administrative applications

### **Patient-Based Administrative Applications**

The patient-based administrative applications include applications that perform patient registration, scheduling, billing, and linkage functions. The patient-based clinical applications include application packages that support the various health care programs within IHS, such as dental, laboratory, or pharmacy. The financial and administrative applications include application packages that track finances, billing, and equipment.

The DIR distributes the RPMS application suite to HQ and each AO, although these sites may only install and use a portion of the available functionality. The AO releases the RPMS application suite to the appropriate health care facilities, which may also use only a subset of the applications. For example, the patient-based administrative and the patient-based clinical applications are primarily used by health care facilities to support their health care service delivery. HQ and AOs do not administer patient care. Therefore, these sites do not need to run these applications. HQ, AO, and health care facilities use the financial and administrative applications. HQ and health care facilities run only a few selected financial and administrative applications, whereas the AO runs all of these applications. Exhibit 4-4 summarizes the major application categories used at various sites.

---

<sup>32</sup> <http://www.his.gov/cio/RPMS/index.asp>

**Exhibit 4-4: RPMS Components by Category and Site Type**

Site	Patient-Based Administrative	Patient-Based Clinical	Financial and Administrative
HQ			X
AO			X
Health Care Facilities	X	X	X

Different RPMS applications can be used at sites of the same type. In general, services, such as dental, laboratory, and inpatient, offered at that site determines the scope of RPMS applications the facility uses. With the health care facilities, hospitals will run more of the RPMS applications than other health care facilities because they deal with both inpatient and outpatient care, whereas the other health care facilities deal only with outpatient care. A typical larger health care facility may run the following applications, assuming all these services are available at the health care facility:

- Patient Registration
- Pharmacy
- Dental
- Maternal and Child Health
- CHS
- Laboratory
- Patient Care Component (PCC)

For the HQ and AO, the RPMS application suite typically is resident on site. For a health care facility, the RPMS application suite can reside on a system located at one of the following:

- The health care facility itself
- Another health care facility in the same service unit
- The health care facility's AO

Usually, RPMS and the application suite reside at high-volume health care facilities, such as hospitals and clinics, and the other health care facilities in that service unit access RPMS on the higher volume facility's system. If a health care facility does not have a local RPMS or is not linked to another health care facility with the RPMS application suite, then it links to the AO to use RPMS. Regardless of where the RPMS resides, the health care facilities always access certain financial and administrative applications on their AO's system.

## **Patient-Based Clinical Applications**

The Patient Care Component (PCC), along with the other clinical applications, makes up the patient-based clinical and service applications. The PCC provides for the local collection and storage of a broad range of health data on patients. IHS employees use this data to administer medical treatment to patients. The PCC also supports the IHS health care delivery, planning, management, and research. The patient-based clinical and service applications are broken out into five diagrams: data management; medications, nutrition, and pharmacy; laboratory testing; drug abuse and mental health treatment; and special services.

When a patient visits a health care facility, a PCC Ambulatory Encounter Form is filled out for that patient. After the patient's visit, the encounter form is entered into the PCC through the PCC Data Entry System, and the patient's data is stored in the PCC files. Other applications linked to the PCC, for example Surgery and Laboratory, update it automatically. The linked applications, such as Surgery and Laboratory, enter patient data into their system as services are provided. For example, when a patient goes in for surgery, information regarding the surgery is entered into the Surgery System at the time of the patient's surgery. The Surgery System creates a report and sends the patient's surgery data to the PCC files. The data from these applications (e.g., Surgery) are combined with the data from the Encounter Form to create a comprehensive record for a patient. Then the other applications in the PCC retrieve the data from the PCC files to perform specific operations. The PCC applications produce ad hoc reports using the PCC Q-Man, management reports and health summaries. Some of the applications use PCC data to create files and reports based on a patient's health record. The most important and comprehensive report is the Health Care Summary Report. The PCC also has the PCC Data Transmission System so the HCF can automatically send data to ITSC to be stored in the national database. All of the clinical applications can operate stand alone, and some are not linked to PCC, such as Anatomic Pathology.

Data that the HCF has entered into the RPMS is stored in each HCF's RPMS database. Routinely, selected data are transferred from the HCF to the AO via the Area Data Consolidation System. Each AO then consolidates all data received from the HCFs in their geographic area and sends the data to ITSC where it is stored in NPIRS and used for statistical analysis and reporting. The AO does not store any of the data received from the HCFs. For example, there is no area-wide consolidated health care database, although some AOs have an initiative to capture and store some data as it move through the AO. All patient information is stored in a database at the patient's local primary HCF, except those that are running RPMS remotely. If a patient is seen at an HCF

that is different from their primary facility, the primary facility is telephoned and that patient's health summary is faxed to the facility where the patient is being seen. Currently, there is no system-wide database integration/synchronization of patient data. There is no sharing of patient data between/among HCFs in the same or different areas. However, two IHS Areas are operating a Multi-Facility Integration (MFI) System that provides the capability to integrate Patient Registration and PCC visit/treatment data from multiple sites into an integration site. IHS also participates in the GCPR initiative to facilitate interoperability and information sharing within I/T/U and appropriate health care providers.

### **Financial and Administrative Applications**

The financial and administrative applications are structured to enhance administrative processing. The Administrative Resource Management System (ARMS) provides electronically processing requests, acquisitions, procurements, travel orders, training requests, and EFT using an electronic signature for approvals. The FDMS processes EFTs and Electronic Payments for reconciling financial obligations. The Supply Administration Management System (SAMS) allows for issuing and tracking supplies. The Third-Party Billing (TPB) system allows for generating an electronic medical bill. The Accounts Receivable (A/R) system tracks medical billing and an electronic remittance advice for posting payments received from private payers. Data flow through these systems in the same fashion as the other applications:

- An IHS employee enters data into the system for processing.
- The system receives data with external entities.
- The system manipulates the data and then produces reports.
- The system sends data to external entities and sends data to files.

IHS recognizes the cost benefit of using Electronic Data Interchange (EDI) financial and administrative functions. The financial applications exchange data with the Treasury Department to accomplish EFT and payments, the HHS Health Accounting System to maintain a formal commitment register, and third-party payers. The IHS and Treasury Department are participating in a pilot project to receive electronic medical claim remittance advice for reconciling third-party medical claims payments. IHS has tested the exchange of an electronic medical claim, 837 X12 3070 version, with the Medicare Fiscal Intermediary and is receiving a medical claim electronic remittance advice, 835 X12 3050 version, in collaborative project with the Treasury Department.

IHS plans further expansion of EDI. IHS is conducting technical analysis to become compliant with electronic data interchange standards for financial and health care transactions.

IHS intends full compliance with the Federal Acquisition Act, the Health Insurance Portability Accounting Act, as well as the HHS Office of the Secretary's direction to establish an Electronic Commerce Alternative to FACNET. IHS is now integrating clinical data with financial and administrative data to achieve a level of health care cost reporting with a limited level of financial and administrative decision support.

Health care reform and Managed Care will require further development of cost reporting toward a cost accounting system, which will provide comprehensive financial and administrative decision support. This will require integrating clinical, financial and administrative data from RPMS. In summary, RPMS is an integrated set of software applications designed to meet IHS' business needs. RPMS is essential to IHS delivery of quality health care to AI/AN.

## **OPERATIONAL ENVIRONMENT**

---

IHS recommends and supports a standard operational environment comprised of various components, such as operating systems, application languages, and a standard suite of application software. The Division of Information Resources (DIR) has developed the following set of standards for developing software applications:

- UNIX System V Operating System [Although some areas are using DOS platforms]
- MUMPS-ANSI/MDC X11.1 standard application language
- VA FileMan
- Kernel Version 8
- RPMS Applications

DIR standards ensure functional soundness and technical correctness of RPMS application programs, maintain software portability, and promote an open systems environment.

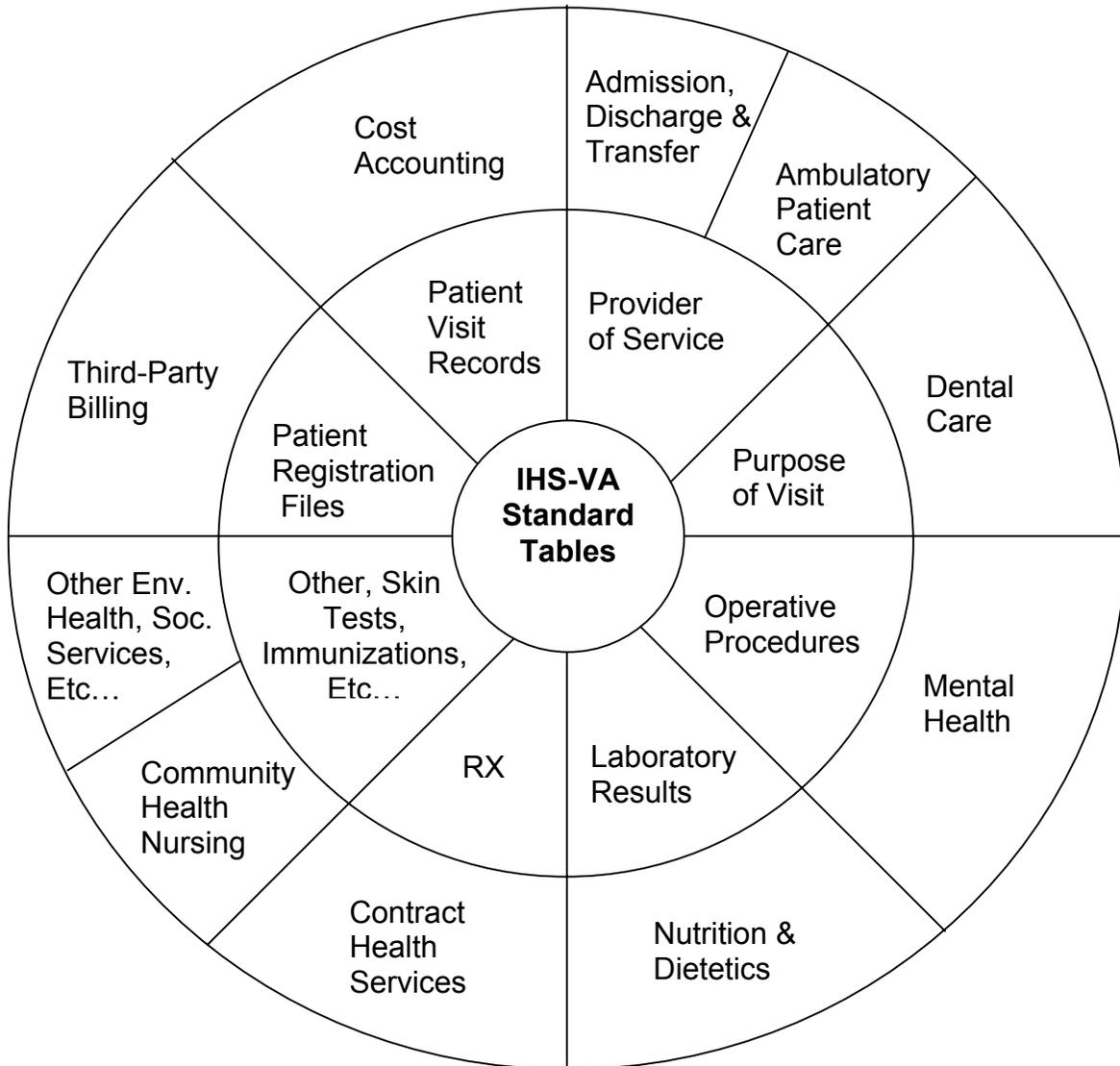
The RPMS software is developed in the programming language M, also known as MUMPS. M is a general purpose programming language that can process large data files. This ability allows the RPMS to store pertinent patient data in a core set of centralized files. This way, core patient data is not scattered in a number of discipline-specific or program-specific files. This allows core data, such as patient visit data, to flow to the necessary software applications without having the system access multiple files. Based on this single database structure, RPMS has a core set of IHS/VA tables that are shared by all applications. Sets of data files are shared by related groups of applications as

appropriate. Each health care facility will feed information from its patient encounters into this core set of data.

Finally, there are discipline-specific program and management data, which are not in common with the data of most other disciplines and so have their own files. Data flow from these files to the necessary software applications. Exhibit 4-5 presents the RPMS file relationships.

**Exhibit 4-5: RPMS File Relationships**

Within the IHS M environment, FileMan serves the end users as the underlying data management structure. FileMan, an original VA application, provides end users quick ad hoc queries of files and records in an M database, with access



Inner Circle- Standard IHS/VA  
 Middle Circle- RPMS Patient Care Files  
 Outer Circle – Discipline and Program Specific Files

of M applications for both data entry collection and reporting.

## **NPIRS SOFTWARE ARCHITECTURE**

---

NPIRS, the IHS centralized database, is updated with data received from the IHS Area Offices and from the Tribes. The Areas use the RPMS application to collect and export patient data. The Tribes use RPMS or COTS programs to collect and export patient data. NPIRS is then updated with this data. Each I/T/U specific site currently is responsible for submitting Medicare and Medicaid claims for outpatient visits, such as third-party billing, for approximately one quarter of the IHS regions. The source of the claims data is the NPIRS database. Claims are submitted electronically on a monthly basis. The recipient for Medicare claims is Texas and South Carolina BC/BS. The recipient for Medicaid claims is the Arizona Health Care Cost Containment System (AHCCCS).

## **RPMS PROCESSING PLATFORM ENVIRONMENT**

---

This section describes RPMS' hardware architecture and operating system environment and provides an overview of the various hardware environments currently supporting RPMS users within I/T/U. The IHS NP currently supports two hardware/Operating System (OS) platforms: UNIX on RS/6000s and NT on NT boxes.

A number of legacy host and small facility operating environments that support RPMS exist within I/T/U. The standard RPMS platform IHS is currently procuring is the IBM RS/6000 running AIX. Other environments that host RPMS include various implementations of UNIX, DOS, and Windows NT. At most sites, RPMS is hosted on one of the three UNIX platforms (UNIX, SCO UNIX, and AIX).

## **IHS RS/6000 CONFIGURATION OVERVIEW**

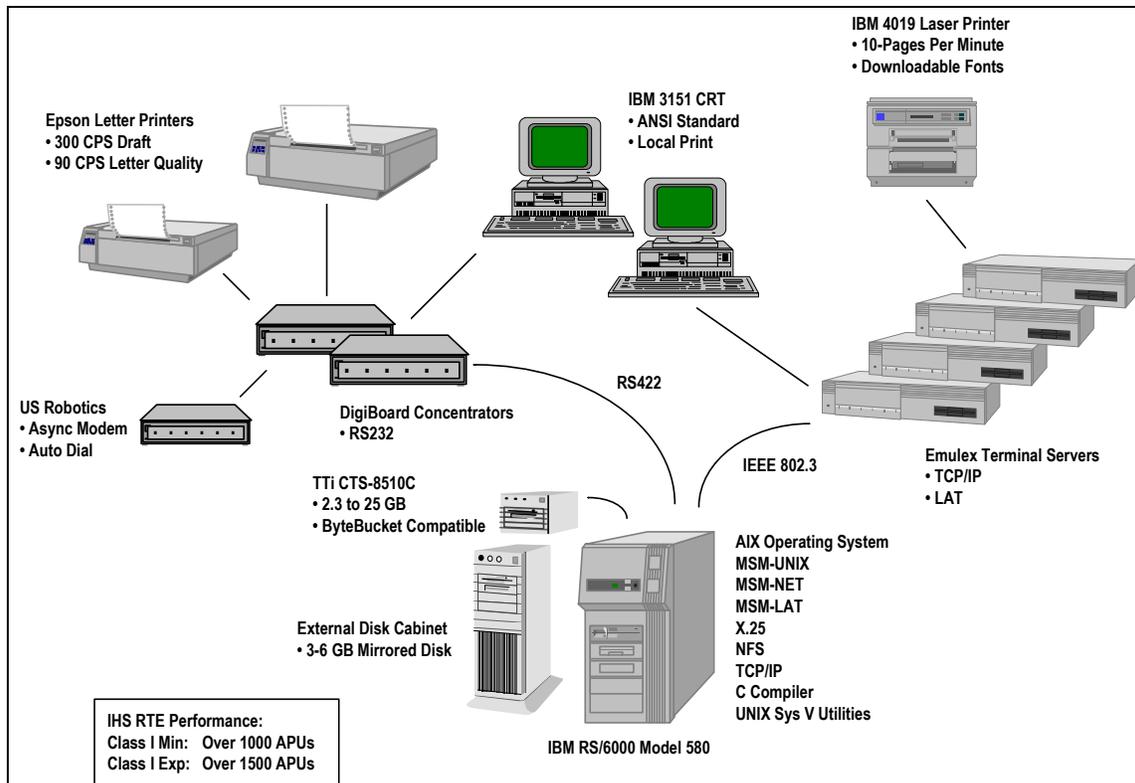
---

The IHS configuration of the IBM RS/6000 runs the AIX operating system, which is IBM's cross platform implementation of UNIX. AIX is fully compliant with all published Federal Portable Operating System Interface for Computer Environments (POSIX) standards. The standard configuration also includes the following software components:

- TCP/IP, NFS
- M
- M Distributed Database Protocol (DDP)
- M Network
- M Local Area Transport (LAT)

IHS deploys two standard configurations of the IBM RS/6000 model 580, which are the Class I System Minimum Configuration and the Class I System Expanded Configuration. IHS has classified HCFs as either low or high volume facilities and uses this classification to determine which of the two RS/6000 configurations is deployed at each site. Low volume facilities are configured with the Class I System Minimum Configuration, which can support 64 or fewer concurrent users. High volume facilities have the Class I System Expanded Configuration, which can support up to 128 concurrent users. Exhibit 4-6 shows the major components of the IHS Class I System configurations. Both configurations are comprised of identical system components, with each RS/6000 connected to a LAN, which is then connected to the IHS WAN.

**Exhibit 4-6: Class I System Major Components**



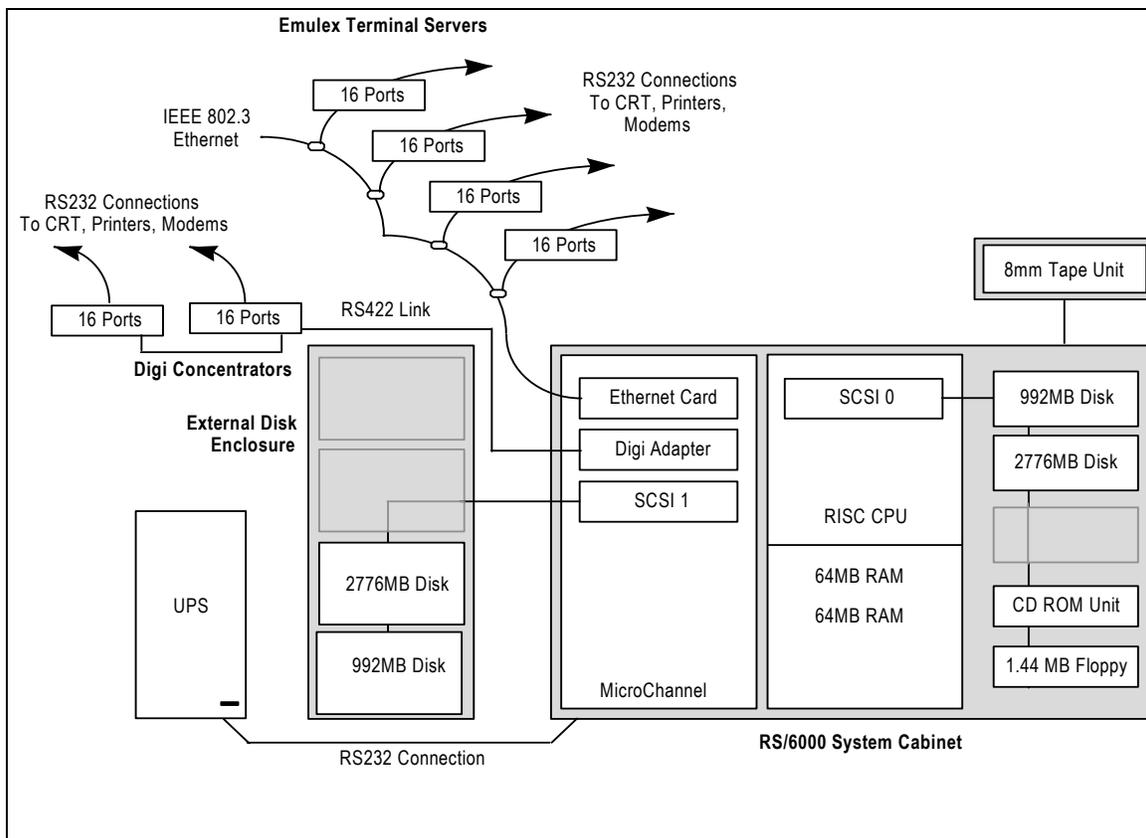
RPMS users access the system via modem, CRT terminals, or personal computers (PCs) located on the LAN. Remote users (typically at small IHS facilities) can access the RPMS via modems that connects to the RS/6000 terminal controllers or by emulating LAN access through LAT, SLIP, or PPP connections. Users accessing the RS/6000 remotely use Cathode-ray tubes

(CRTs) terminals with modems attached or PCs with modems running terminal emulation software.

### Class I System Minimum Configuration

The Class I System Minimum Configuration, shown in Exhibit 4-7, has 128 Megabytes (Mbytes) of memory, two 1.0 Gigabyte(s) (GB) IBM disk drives (3.5 inch), an additional IBM Micro Channel, Small Computer System Interface (SCSI) controller, and an IBM high performance Micro Channel Ethernet controller. Components that have been integrated into the system include two 3.0 GB disk drives (5.25 inch), a 128-port asynchronous (async) Input/Output adapter card, an 8 millimeter (mm) external tape drive, two CRTs, one narrow-carriage dot matrix printer, one wide-carriage dot matrix printer, one laser printer, one 9600 async modem, two RS-232C standard 16-port concentrators, and four Ethernet terminal servers.

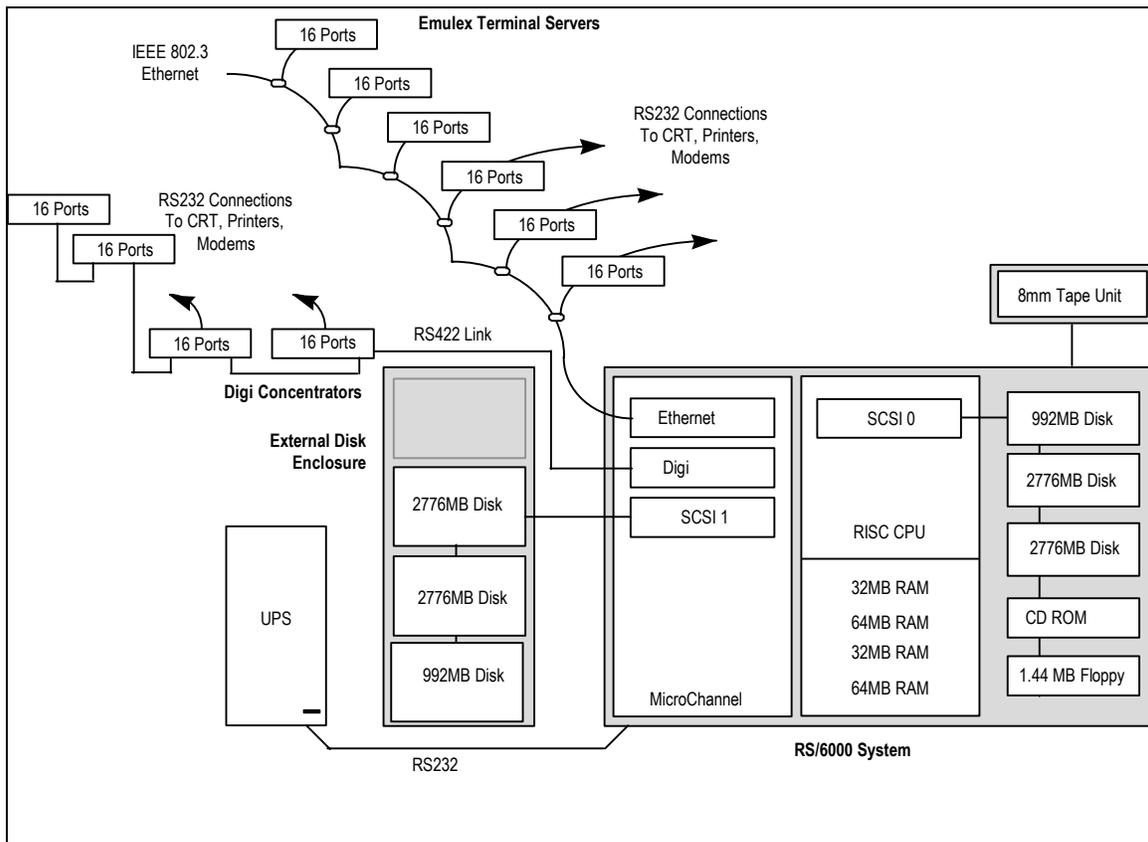
**Exhibit 4-7: Class I System Minimum Configuration**



### Class I System Expanded Configuration

The Class I System Expanded Configuration consists of all minimum configuration components and includes an additional 64 MB of memory (two 32 MB Random Access Memory [RAM] cards), two additional 3.0 GB Small Computer System Interface (SCSI) disk drives, two additional RS-232C standard 16-port concentrators, and two additional Ethernet terminal servers. This configuration is illustrated in Exhibit 4-8.

**Exhibit 4-8: Class I System Expanded Configuration**



### Major RS/6000 Model 158 Components

The Class I configurations contain all components for the system to support the RPMS application. The sections that follow describe the major components for both Class I configurations and those instances where the Expanded and Minimum configurations have different components.

### **Class I System Disk Storage Subsystem**

The Class I Systems are configured with a magnetic disk storage subsystem. Each RS/6000 Model 580 has more than 3 GB of formatted mirrored disks. Systems upgraded to the Expanded Configuration contain 6 GB of formatted mirrored disks.

### **Class I System Network and Direct Ports**

The Class I System configuration provides a number of Network Ports and Direct Ports to support terminals, printers, and modems at respective IHS facilities. The Network Ports use the Emulex Performance 2516 Ethernet/LAT terminal servers in 16 port configurations. These terminal servers reside on the LAN at each facility and support all terminals, printers, and modems. Direct Ports use DigiBoard's DigiCHANNEL Host Adapter and 16 port concentrators. The concentrators operate on an RS-422 standard high-speed channel and service terminals throughout an IHS facility. The DigiCHANNEL concentrators support CRT terminals, printers, and modems.

### **Class I System Operator CRT Console**

The Operators CRT console includes two IBM 3151 American National Standards Institute (ANSI) standard terminals and keyboards with each Class I system. Each console is connected to a Direct Port concentrator or to the Network Port terminal server. The terminal also provides a port to connect a printer, which can be dedicated to local screen-printing or to the host system.

### **8mm Cartridge Tape Unit**

An 8-mm tape backup subsystem is part of the Class I System configuration and can store up to 25 GB of data on any single 8-mm cartridge.

### **Class I System Printers**

The RS/6000 system employs both heavy-duty, dot-matrix printers and laser printers. The dot-matrix printers are configured with both a parallel interface and a serial interface, allowing the printer units to connect to either the Network Port terminal servers or the Direct Port concentrators. Each laser printer unit contains a serial interface and cables for operation from either the Network Port terminal servers or the Direct Port concentrators.

### **Class I System Asynchronous Modems**

To meet the smaller IHS facilities' communications requirements, the IHS Class I System configuration includes US Robotics Courier V.32bis—standard asynchronous modems. These modems support the following:

1. Auto-dial capabilities
2. Asynchronous transmission speeds up to 14.4 KBPS
3. Error-free transmission at the highest possible speed

#### 4. Data compression

Modems are configured to operate on the Network Port terminal servers or the Direct Port concentrators.

#### **Optional Hardware Components**

The following list identifies optional hardware items that can be added to the Class I System configuration. None of the optional hardware items are specified for a particular configuration, such as Minimum or Expanded.

- 9 Track Tape Drive
- Line Printer (+ cable)
- Synchronous Modem (+ cable)
- Uninterruptible Power Supply x 2
- Compact Disc, Read-Only Memory (CD-ROM)

#### **Legacy and Small Facility Operating Environments**

IHS has deployed a variety of platforms to support RPMS application software. These legacy and small facility RPMS operating environments include SCO UNIX and DOS on Intel platforms, and a growing number of sites running Windows NT. The most widely deployed RPMS environments are the following:

- AIX UNIX—The most common platform for IHS running RPMS. The most common models of RPMS UNIX hosts are all varieties of IBM/RISC servers.
- NT/4—The most common NT/4 manufacturers/models are all varieties of Intel-based servers.

Implementing a particular platform reflects area or regional preferences. For example, NT platforms are found in the Bemidji, California, and Tucson Areas. UNIX platforms are common throughout the Agency.

IHS is actively replacing some older platforms with newer Intel based Pentium platforms.

## **NEW & EMERGING TECHNOLOGIES**

Various technologies are crucial to developing the IHS EA. This chapter discusses the building blocks needed to support a distributed open health care architecture within the IHS Enterprise. It does not attempt to cobble together these technologies into an integrated, consistent perspective. Instead, it serves as a compendium. Where appropriate, references have been made to publicly available sources (either Web-based or print) for subsequent research.

## **PROCESS IMPROVEMENT**

---

### **Achieving IHS Goals By Improving the Software Engineering and Acquisition Processes**

The EA guiding principles described in chapter 1 provided the basis for setting the EA's broad architectural goals. For IHS to achieve these goals, EA guiding principles must be instantiated in enterprise-wide processes, structures, and metrics comprising an IHS EA process infrastructure of effective software engineering and management practices. In an era of budget reductions and rapid technological change, continuous quality improvement can be attained only by a focused and sustained effort towards building this process infrastructure.

**Software Engineering Institute's Capability Maturity Model.** The Software Engineering Institute (SEI) has constructed a software process maturity framework, called the Capability Maturity Model (CMM) for Software (SW-CMM), to provide organizations with guidance to establish effective, software process improvement programs. The SW-CMM integrates the following five key concepts<sup>33</sup>:

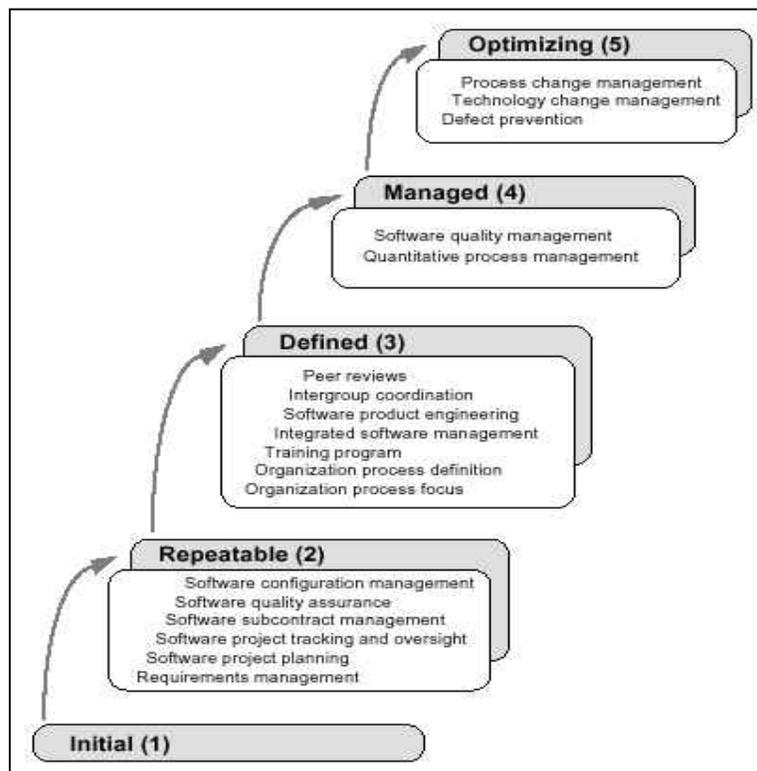
- **Software Process:** A set of activities, methods, practices, and transformations to develop and maintain software and associated products, such as project plans, design documents, source code, test cases, and user manuals
- **Software Process Capability:** The range of expected results achieved by following a software process
- **Software Process Performance:** The results achieved by following a software process
- **Software Process Maturity:** The extent to which a specific process is explicitly defined, managed, measured, controlled, and effective

---

<sup>33</sup> As described in the SEI's *Capability Maturity Model for Software, Version 1.1*, 1993.

- **Institutionalization:** The codification of the software process, through policies, standards, and structure, into a process infrastructure and organizational culture that supports the methods, practices, and procedures of the business so that they endure after those who originally defined them have left the organization

The SW-CMM, which has been refined based on extensive feedback and usage by industry and government in the 1990's, describes an evolutionary path for increasing an organization's process maturity in incremental stages from ad hoc, chaotic processes to mature, disciplined software processes. The stages are ordered, as shown in Exhibit 5-1, so that improvements at each stage establish the foundation on which to improve at the next stage.



**Exhibit 5-1: SW-CMM Maturity Levels & Key Process Areas**

As Exhibit 5-1, SW-CMM Maturity Levels & Key Process Areas, shows, the SW-CMM defines key process areas (KPAs) for each maturity level, except the first level (the initial, "ad hoc" level). The KPAs indicate areas of focus for improving the software process. For each KPA, the SW-CMM identifies a cluster of related

activities, called key practices that collectively achieve a set of goals considered important for enhancing process capability.

***CMM-Based Appraisal for Internal Process Improvement.*** The SW-CMM includes guidance on how organizations can conduct assessments of their software processes to identify risks and areas of potential improvement that relate to long-term organizational goals. An appraisal is the first step toward gaining control of the processes for developing and maintaining software, and evolving into culture of software engineering and management excellence. As shown in the findings of the 1997 Software Process Assessment <sup>34</sup> conducted for IHS by Mitretek, the SW-CMM, on which the assessment approach was based, is designed to help software organizations select process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, IHS can steadily improve its enterprise-wide software process to enable continuous and lasting gains in software process capability.

***The Software Acquisition Capability Maturity Model.*** Over the last decade, as the SW-CMM gained greater acceptance by industry and government because of its effectiveness in assisting organizations to improve their software processes, the need for a model addressing the requirements of the software acquisition process emerged. The resulting CMM for Software Acquisition (SA-CMM) is designed to be

- 1) Generic enough for any organization to use, regardless of size, to acquire software
- 2) Applicable to acquiring all types of embedded and stand-alone software, including in-house developed software, out-sourced (contracted) software, COTS and GOTS products, and other non-developmental item software being acquired as part of a system or separately
- 3) Appropriate for use throughout the software life cycle. The SA-CMM maturity levels and key process areas are shown in Exhibit 5-2.

As IHS evaluates using or acquiring other-agency-developed software, the need for a mature, enterprise-wide software acquisition process tailored to IHS requirements and contexts becomes critical. Every acquisition begins with a requirement, and as the acquisition develops, more requirements are identified and refined. To ensure a common understanding about what is being acquired and when, between IHS, as the acquirer, and other agencies' developers (or

---

Adapted from SEI CMM as depicted on the SEI Web Site.

<sup>34</sup> Mitretek (1997). Annotated briefing "IHS IRM Software Process Assessment, Task Overview and Results."

even in-house developers), the software requirements and organizational roles and responsibilities must be specified, baselined, managed and controlled. Management these requirements is the responsibility of IHS, as the buyer, even when the other agency or a contractor is responsible for performing project management activities.

**Exhibit 5-2: CMM Maturity Levels and Key Process Areas**

Level	Focus	Key Process Areas
5 Optimizing	<i>Continuous process improvement</i>	Acquisition Innovation Management Continuous Process Improvement
4 Quantitative	<i>Quantitative management</i>	Quantitative Acquisition Management Quantitative Process Management
3 Defined	<i>Process standardization</i>	Training Program Acquisition Risk Management Contract Performance Management Project Performance Management Process Definition and Maintenance
2 Repeatable	<i>Basic project management</i>	Transition to Support Evaluation Contract Tracking and Oversight Project Management Requirements Development and Management Solicitation Software Acquisition Planning
1 Initial	<i>Competent people and heroics</i>	

## **ACHIEVING IHS GOALS BY IMPLEMENTING DATA MANAGEMENT PRACTICES**

---

One of the most difficult goals to achieve in any organization is to ensure the quality of the information it uses. The basis for all information is data, whether they are maintained in file cabinets or in the latest electronic storage devices. To discover useful information and explore it in meaningful ways requires developing significant relationships between the data and the discrete levels of Information that are vital to the organization. It has become a truism that information is one of the organization's primary resources. In the private sector, the quality and timely use of information frequently spells the difference between a firm's success and becoming a market leader and its failure. In the Federal Government sector, the quality and availability of data frequently dictate the levels of trust that the public has in the agency and how well the agency accomplishes its mission. IHS has additional responsibility for ensuring the timeliness and accuracy of data because much of the data has to do with the health and welfare of its constituents. In addition to meeting its primary responsibilities, IHS uses data to manage its own resources and to support its long-term planning.

With the widespread use of computer technology, data management is often confused with the tools that support data manipulation—hardware and telecommunications architectures, database management systems, query tools, storage devices—rather than focusing on actual data management. As defined here, data management is the function of organizing, cataloging, locating, storing, retrieving, and maintaining data. In effect, data management optimizes the organization's use of the data assets. At a basic level, data management focuses on the organization and data maintenance. At higher levels, data management includes vigilance against corruption, loss, and misuse. One of the paradoxes of computers is that they support the manipulation of very large data sets at very high speeds, and yet, because of these capabilities, electronic data are uniquely susceptible to accumulating errors resulting from careless handling, systemic problems, and undetected intrusion. When data can no longer be certified to be accurate and representative, it loses its value and the users' trust.

Effective data management is a key attribute of effective organizations. The importance of timely and reliable data permeates the key process areas comprising Level 2 of the SEI CMM. To achieve IHS EA architectural goals, it is necessary to develop an effective data management program that is part of the process infrastructure of effective software engineering and management practices. Sound data management provides the following:

- Data management planning

- Inventory of data resources
- Metadata management
- Configuration management of data items
- Data standards management
- Chain of custody of information
- Business rules documentation
- System interface specifications

A sound data management program will maintain an inventory of the data items that constitute the organization's data resources. Data have two components: metadata and domains. The metadata describe and define the data items. The data domains indicate the sets of valid values that apply to data items. In many organizations, metadata and data domains are usually placed under configuration management.

Sound data management programs also contain processes to manage the chains of custody of data items. Chain-of-custody documentation identifies the data steward organizations of data items, the organizations that access, modify, or delete data item instances, and general disposition and archival of data item instances when their importance becomes historical rather than current.

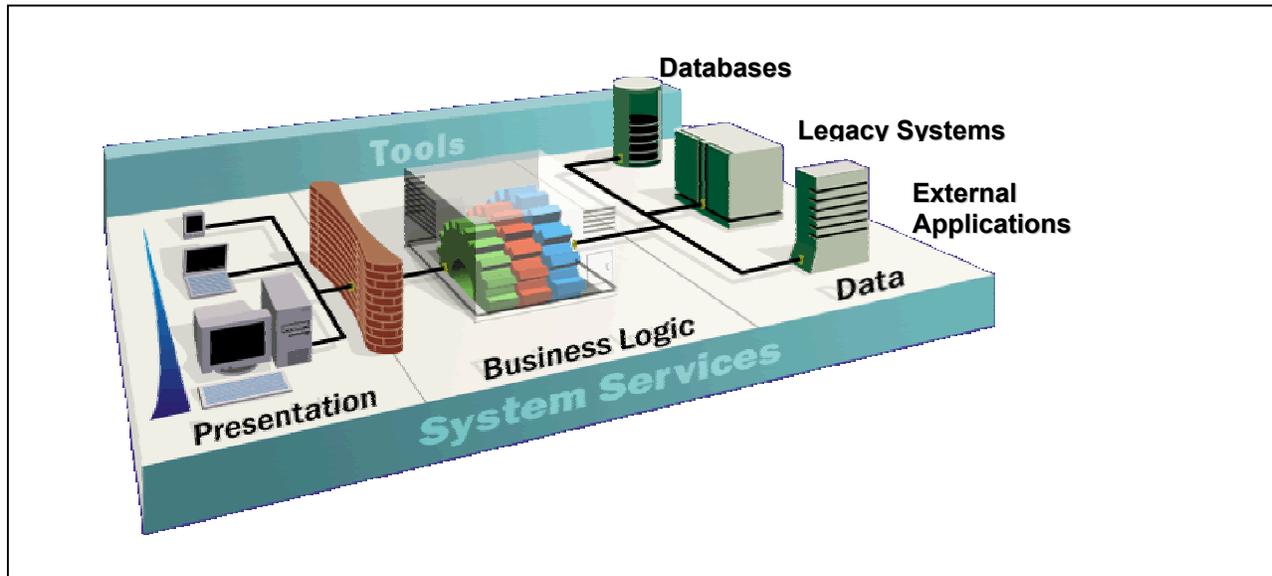
All good data management programs start with a plan that outlines the goals and objectives of data management, the roles and responsibilities of all parties involved in the data management program, the tasks that comprise the data management program, the metrics necessary to determine how well the program is performing, and the schedules necessary to implement the plan.

## **DISTRIBUTED ARCHITECTURE**

---

A health care, distributed architecture is based on distributed technologies designed around three-tier or n-tier architectures, as depicted in Exhibit 5-3.

**Exhibit 5-3: Tiered Architecture**



The second tier (middle tier server) is between the user interface (client) and the data management (server) components. This middle tier provides process management where business logic and rules are executed and provides functions such as queuing, application execution, and database staging. The middle tier server (also referred to as the application server) improves performance flexibility, maintainability, reusability, and scalability by centralizing process logic. Centralized process logic makes administration and change management easier by localizing system functionality so that changes must only be written once and placed on the middle tier server to be available throughout the systems. Two prominent technologies that are used to implement the middle tier are the Microsoft Component Object Model (COM/COM+) component-based technology and CORBA, an object-based technology.

## **MICROSOFT TIER ARCHITECTURE**

---

Microsoft is building its tier architecture around term Distributed Internet Applications, which includes Microsoft's Distributed Component Architecture (MDCA )<sup>35</sup>, but as yet doesn't have a term to specifically describe their middle tier technologies. However, the term MDCA is cropping up more and more in Microsoft literature, and may eventually acquire official status. In any case, because of the widespread distribution of session book and newsletters within Microsoft, the term is at least generally understood within the company.

MDCA consists of the following six closely related products:<sup>36</sup>

1. COM defines the basic component/object model.
2. Distributed COM (DCOM) allows components to be moved around a network.
3. Microsoft Transaction Server (MTS) provides a component runtime environment for the middle tier.
4. Distributed Transaction Coordinator coordinates distributed transactions.
5. Microsoft Message Queuing (MSMQ) provides asynchronous communications.
6. Microsoft Cluster Server (MSCS) allows multiple servers to work as one.

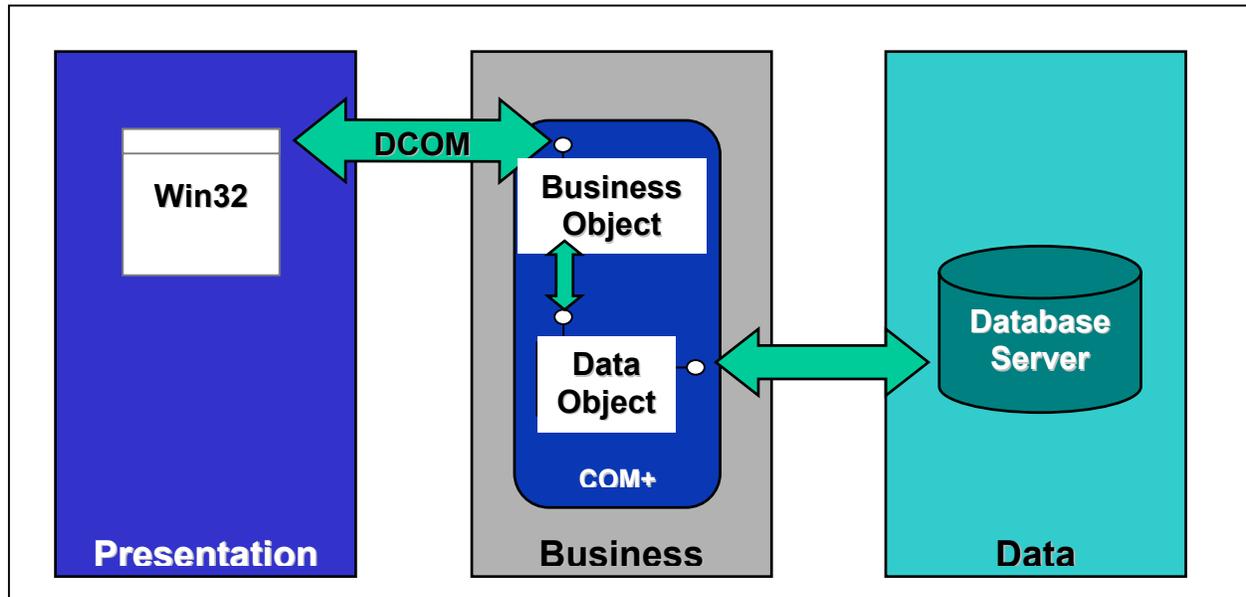
The MDCA is a COM+ application, as depicted in Exhibit 5-4, which rolls together the functionality of COM, DCOM, and MTS, and add functionality found in MSMQ (asynchronous communications). Systems being developed today that are designed to take advantage of COM, DCOM, and MTS are well positioned for the latest generation of Microsoft's middle tier architecture.

---

<sup>35</sup> COM+ and the Battle for the Middle Tier, by Roger Sessions, 2000

<sup>36</sup> COM+ and the Battle for the Middle Tier, by Roger Sessions, 2000

**Exhibit 5-4: Simple COM+ Application**



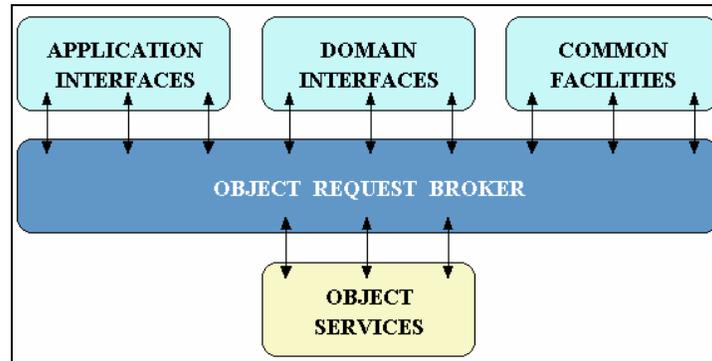
COM+ is language neutral and any language may be used to implement COM+ components, but it is up to a particular language vendor to make it easy to do so. Microsoft Visual Basic may be the easiest of all COM+ component implementation languages.

## OMG TIER ARCHITECTURE

The CORBA is the OMG answer to the need for interoperability among the rapidly proliferating number of hardware and software products available today. Simply stated, CORBA allows applications to communicate with one another no matter where they are located or who has designed them.

The Object Request Broker (ORB), illustrated in Exhibit 5-5, is the Middleware that establishes the client-server relationships between objects. A client can use an ORB to transparently invoke a method on a server object, which can be on the same machine or across a network. The ORB intercepts the call and is responsible for finding an object that can implement the request, pass it to the parameters, invoke its method, and return the results. The client does not have to be aware of where the object is located, its programming language, its operating system, or any other system aspects that are not part of an object's interface. In so doing, the ORB provides interoperability between applications on different machines in heterogeneous distributed environments and seamlessly interconnects multiple object systems.

**Exhibit 5-5: Object Request Broker**



The OMG has recently developed a new specification called the CORBA Component Model (CCM). The CCM is a server side component model for building applications that support the construction and assembly of components written in multiple programming languages. The CCM builds on the Enterprise Java Beans (EJB) model to bring its benefits to components written in multiple languages and defines an architecture for building CORBA containers for EJB. The CCM also introduces an architecture to package and deploy component implementations using an XML vocabulary and defines a Meta Object Facility (MOF)-based meta-model for both components and component packages.

## **COMPONENT-BASED SOFTWARE ENGINEERING (CBSE)**

---

The term component refers to a reusable, self-contained piece of software that has a published interface and can be used to construct an application. Components usually have a well-defined functionality and behavior. In CBSE, many different components are used to construct the final application. The process of building applications from components is sometimes referred to as Component Scripting. Other terms that appear in this context are COTS and ComponentWare. Components ideally are self-describing and are best used in an environment and language that supports reflection or introspection. For some languages, such as Java, graphical development tools allow the visual editing of component attributes. Because components are intended to be re-used, users should not be required to understand all of the component's internal workings.

Component technology consists of object-oriented aspects, components, frameworks, and reuse, which are all closely related and have common goals. All of the approaches aim to reduce the amount of unnecessary work that is performed and aim to spread expertise and knowledge across a broader base.

All of the approaches can and should be combined to achieve maximum results. Components are best used in conjunction with frameworks. Popular Component Models include Microsoft's COM, and Sun Microsystems' JavaBeans.

## **INTERNET INTER-ORB PROTOCOL (IIOP)**

---

IIOP is the OMG CORBA internet-protocol created to facilitate communication and interaction between ORB. IIOP's ability to connect applications utilizing commercially available ORBs allows architects to choose best-of-breed implementations and to integrate with existing CORBA applications. IIOP is an instance of the General Inter-ORB Protocol (GIOP), using TCP/IP as its transport. All CORBA 2.x ORBs must support IIOP either directly or through a mechanism called a half-bridge, providing a means for converting the ORB's proprietary protocol to IIOP. IIOP is important for enterprise Java deployment because it provides the communication link that allows Java components (e.g. EJBs) to interact with any CORBA-compliant component. Over the last few years, CORBA has become popular for the development of distributed applications and for interfacing new development with legacy applications; note currently, IIOP support in Java2 Enterprise Edition provides this capability. In addition, IIOP allows EJB components to communicate with Microsoft DCOM components through a DCOM to IIOP bridging product.

## **STORAGE SERVICES**

---

The OMB has recommended that the IHS provide cost accounting data for the products and services it delivers. A cost accounting process will require the ability to assign costs for supplies and services delivered to patients. Additionally, legislation directs the IHS to collect from third party payers where and when possible. Medicare and Medicaid are the dominant third party payers in the health care industry. The administration arm for these programs, HCFA, requires completion of the hospital and hospital Complex Cost Report by each participating facility every year.

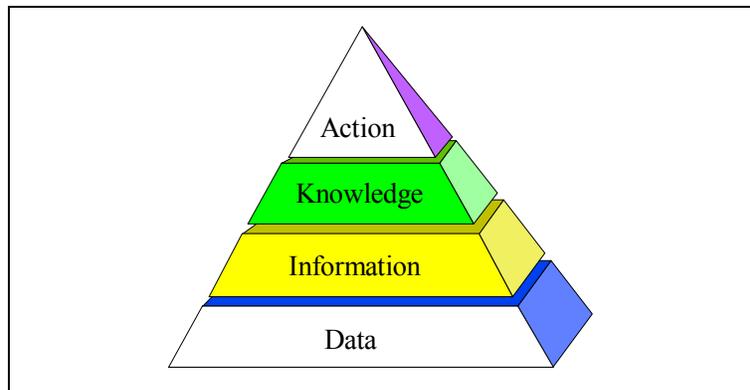
To address this requirement the IHS will look at the concept of a data-warehousing framework that will enable decision support information to be gathered across the enterprise. The methodology to develop these types of client server systems must be a comprehensive data warehouse framework specifically designed for client server. The major components of a logical data warehouse framework are the following:

- Data assembly with concurrency and integrity
- Data transformation constrained by business rules

- Data distribution controlled by data migration rules
- Optimized data design and access

The challenge for the IHS is to develop a decision support system based on the framework shown in the Exhibit 5–6, Layered Decision Support Framework. A decision framework has four components, including data, information, knowledge, and action. Within the framework, the data component is made up of clinical data, financial data, external data, surveys, and ambulatory data. This data may then be aggregated to provide information to support case studies, population use, and encounter studies. The knowledge component of the framework allows IHS to become equipped to begin to leverage patient information for determining clinical pathways, profiling providers, improving business processes, and for developing cost cutting strategies. The action component provides the basis for improving wellness care, providing better contract negotiation, improving clinical practices, and reducing overall operating costs.

**Exhibit 5-6: Layered Decision Support Framework**



As data traverses the framework its value increases at each framework component level. Exhibit 5–7, Enterprise Data Warehouse (EDW) Process, indicates the activities between components. Data warehousing is required to gain information from any raw data accumulated. Data warehousing activities involve storing massive amounts of detailed data gathered from multiple sources that have been cleansed. Warehousing allows the Agency to perform analysis and studies that result in providing services that impact business.

### **Data Warehouse Architectures**

The corporate data warehouse represents the design, development, and implementation of various decision support technologies that provide information to the user community that is accurate, timely, and aligns IT with

corporate business goals and objectives. Exhibit 5-7 describes an EDW process.

**Exhibit 5-7: Enterprise Data Warehouse (EDW) Process**

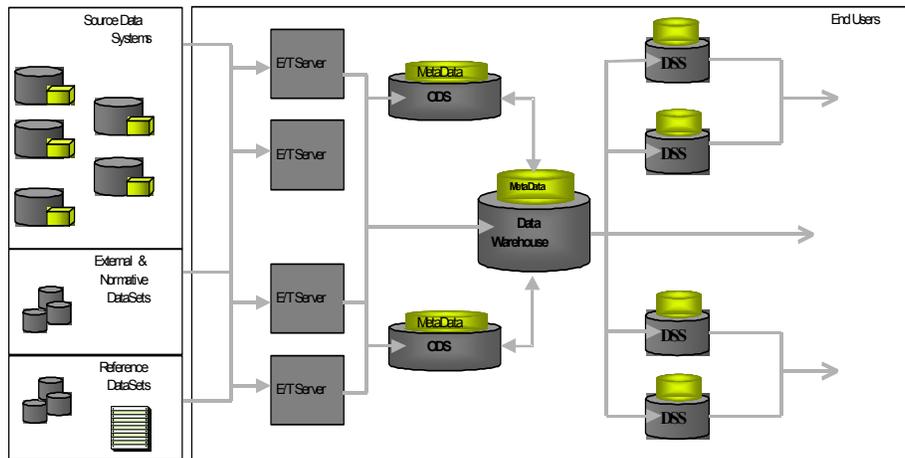
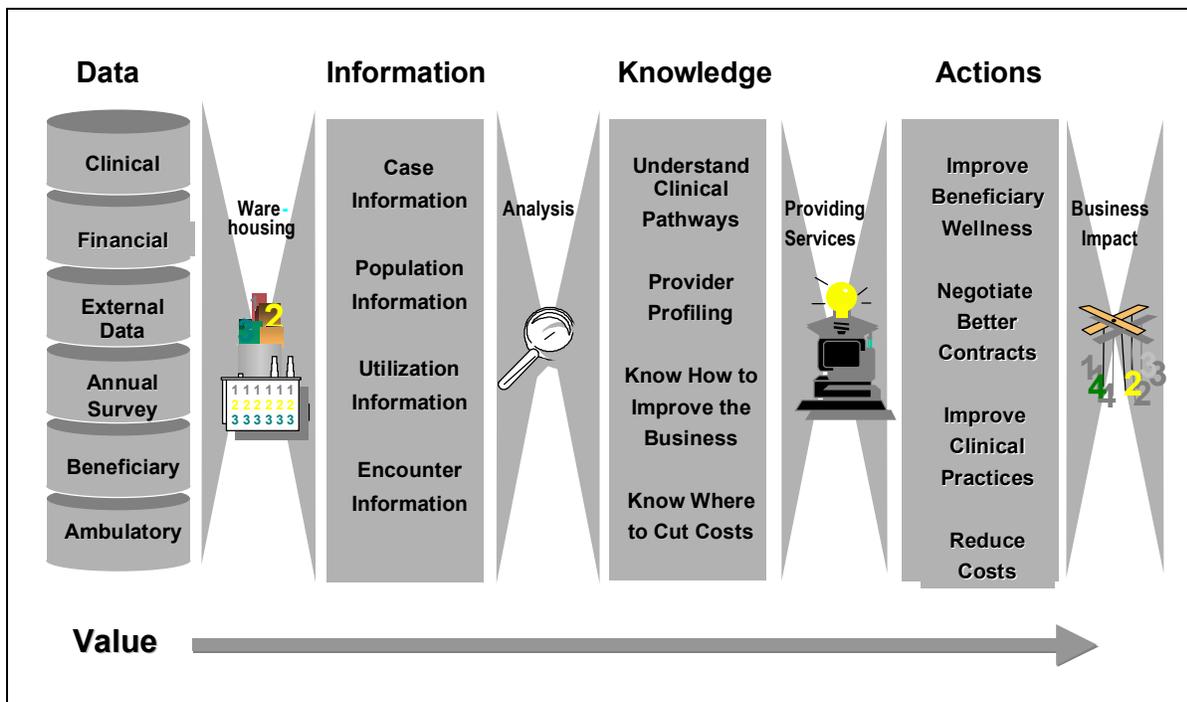


Exhibit 5-8 provides a logical view of an EDW. Local hospitals collect and process treatment data on patients, including demographics, providers, geographics, time, encounter types, diagnosis, and procedure.

**Exhibit 5-8: EDW Logical View**



This data moves along a data continuum to regional data marts where the data goes through an extraction, transformation, and cleansing process before being uploaded to the corporate data warehouse. The continuum is shown as data is moved through the enterprise to the data warehouse. Data warehousing is the key to attaining success within a decision support system (DSS) framework. A data warehouse and its services enable the collection and organization of the data sources within the IHS providing managers and executives with an integrated business-oriented view of their corporate and external data. Four important aspects of data contained within the warehouse are the following:<sup>37</sup>

- Data is oriented to major subject areas.
- Data from multiple data sources are integrated into a single logical model.
- Data is time variant; it is accurate as of a specific moment in time.
- Data is non-volatile; updates occur in scheduled and coordinated periods.

### **Clinical Data Repository**

A CDR can be considered a specific use of an Operational Data Store (ODS). A CDR is a dynamic tool used to manage clinical data, including patient-related information, such as care provided, ancillary services, and the outcome of a course of care. Using standards-based formats, the CDR brings together disparate clinical data from various points of care into an integrated view. Many technology strategists today consider a CDR to be a core component of a complete CPR. A CDR may be implemented in a variety of configurations including a central repository for the whole enterprise or as regional repositories based upon patient population density.

### **Data Marts**

A data mart is a subject-specific data warehouse that provides information specific to an individual department or business area, such as radiology. Each data mart has its own data, infrastructure, and format, and may be populated from data in the corporate data warehouse.

### **On-line Analytical Processing**

On-line Analytical Processing (OLAP) is a style of decision support processing that enables analysts, managers, and executives to gain insight into data through interactive access. Measures such as cost per patient, are analyzed via primary business variables referred to as dimensions, such as time,

---

<sup>37</sup> "Data Warehousing", Bill Inmon

provider, medical center, and line of care, and attributes of the dimensions, such as attributes of time are month, fiscal quarter, and fiscal year.

OLAP is a rapid, iterative process in which the user slices the data across any dimension. Data navigation capabilities, including drill down to lower levels of detail data, drilling up to the most summarized data, and drill across to different data views, are typically provided via a client or web browser GUI. OLAP capabilities can include trend analysis over time, what-if analysis, modeling, and forecasting.

### **Archival Persistence**

Particularly for health information, with the increasing interest in full longitudinal patient records, on-line or near-line storage of information is essential. With a cradle-to-grave record, the requirement exists for essentially all medical information ever captured on a patient to be available in electronic form for eventual consumption by an authorized party.

This requirement places a huge burden on technical infrastructures to make available vast amounts of information. The need for “information triage” to keep critical, real-time information available but make less-frequently-requested information available on an as-needed basis, highlights the importance of near-line storage.

Also essential to this requirement, and complicating the issues, is the capability of technology doubles every 18 months (as described in Moore’s Law<sup>38</sup>), and the storage formats of this information must be long lived. Storing application information in proprietary or binary formats without also storing the full access information, or an explanation of the underlying binaries, renders this information useless, particularly as applications evolve without backwards compatibility.

The role of XML in addressing this issue is significant. Because XML is both machine and human readable, the ability of its markup capabilities to identify and store content without proprietary binary encoding makes it an attractive mechanism. Because XML is human readable, it is better positioned to withstand the test of time without depending on supporting software products. The embedded markup language makes XML documents parsable, allowing their content to be leveraged and used by multiple applications.

---

<sup>38</sup> About thirty years ago, Intel’s co-founder, Mr. Gordon Moore, predicted that the computer processing power could be doubled every 18-24 months. Measured by doubling the transistor counts in the microprocessor; this has become known as Moore’s Law.

## **SEMANTICS AND TERMINOLOGIES**

---

### **Metadata Registries**

Metadata registries contain the characteristics of data (that is, data about data) necessary to name, identify, define, classify, and register data elements. A metadata registry is usually implemented as an electronic repository that systems or users use to locate, retrieve, and exchange data. Metadata registries provide the capability to map disparate concept representations into a common ground, allowing for mediation and reconciliation across care facilities or organizations. Functional experts and/or data stewards (registration authorities) who have the domain knowledge, expertise, and localized control over their particular functional area maintain the registry. The ISO Standard 11179<sup>39</sup> provides registry conventions for consistent representation of identified content and for organizing registries into federations to facilitate data interchange among many enterprises. Building upon this work, efforts such as the U.S. Health Information Knowledge base (USHIK)<sup>40</sup> effort led by HCFA are providing the infrastructure into which “local” versions of these concepts are identified and related across organizations thus enabling interchange and interoperability.

The USHIK work has been influenced by similar efforts from the Australian community with their National Health Information Knowledge base,<sup>41</sup> which has been using metadata registries to interoperate across regional boundaries. A data registry can also serve as a tool and guide for data planning, maximizing data quality and reuse, and minimizing data redundancy.

### **Controlled Vocabularies<sup>42</sup>**

Non-technical issues pertaining to implementing controlled vocabularies are becoming more important as information systems are integrated and as encoded data those information systems provide play an increasing role in enterprise management.

Although desired technical characteristics of terminology systems have been a significant focus of analysis and publication, non-technical characteristics of terminology systems are playing an increasingly important role in determining appropriateness of terminology systems for particular enterprises.

---

<sup>39</sup> 11179 information can be found at <http://sdct.itl.nist.gov/~ftp/18/11179>

<sup>40</sup> The U.S. Health Information Knowledgebase can be found at <http://hmrha.hirs.osd.mil/registry/>

<sup>41</sup> See the NHIK website at [http://www.aihw.gov.au/nhik/owa/hik\\_mainmenu.entire\\_page](http://www.aihw.gov.au/nhik/owa/hik_mainmenu.entire_page)

<sup>42</sup> This section was distilled from “Enterprise Issues Pertaining to Implementing Controlled Terminologies,” Campbell, K. et. al., Kaiser Permanente, undated.

Controlled vocabularies provide the foundation for Informatics applications that require encoded data. The following terminology systems must satisfy certain desired characteristics to meet requirements of application developers and data consumers:

- Comprehensive content
- Concept Orientation
- Concept Permanence
- Non-semantic concept identifier
- Polyhierarchy
- Formal definitions
- Reject Not Elsewhere Classified
- Multiple granularities
- Multiple consistent views
- Representation of context
- Evolve gracefully
- Recognize redundancy

Based upon the above characteristics, the following recommendations pertaining to terminologies and controlled vocabularies were identified in the Campbell [37] paper:

- Terminologies should be licensed with an agreement that prevents local modifications in ways that might result in semantic drift and incompatible dialects. Without copyright and licensure, data may become incomparable across enterprises.
- Terminology systems should be vendor neutral and readily available to all vendors without providing a competitive advantage to any particular vendor.
- Terminology content should be scientifically valid, understandable, reproducible, and useful, containing defining relationships that reflect current understanding of the science and valid for all the participants in the health-care process.
- Terminologies should be well maintained so that new terms can be requested from a central authority capable of rapid response (so as to minimize or eliminate local enhancements). Proper maintenance will increase operational quality and decrease operational costs.
- Terminology efforts should be self-sustaining. In the absence of secure public or endowment funding, terminologies should be

licensed with fees proportional to the value the system provides to the enterprise and the end user, yet not out of proportion with the development and support costs of the terminology itself.

## **INTERFACE TECHNOLOGIES**

---

### **Clinical Context Object Working group (CCOW)**

HL7's Visual Integration Special Interest Group (formerly the Clinical Context Object Workgroup) creates standards that enable the visual integration health care applications. It included the User Link specification that enables a user to sign on to any application on a clinical desktop as the means for securely signing-on to all applications. The applications need not be limited to the desktop; they may be client server. However, integration is via information, which is presented and/or entered at the client side, and all such applications must run in windows on the same desktop environment. For example, CCOW may be used to capture a new patient entry into a registration program and use this to trigger a managed care program to retrieve patient eligibility and payment information (as if the patient had been manually selected on the latter).

### **Health Level 7 (HL7)**

Through the use of HL7 software, individual RPMS sites can use commercial products, such as pharmacy or immunization systems, while retaining all of the functionality of their current RPMS (including Patient Care Component [PCC], health summaries, etc.). An HL7 link between RPMS and a commercial system allows each system to update the other, so that both remain current without requiring users to enter the same data into both systems.

One example currently in use is a commercial pharmacy system. Whenever a change is made to a patient's information in RPMS, such as during patient registration, an HL7 message is sent to the pharmacy system to its patient database automatically. Similarly, whenever a prescription is issued by the pharmacy system, it sends HL7 message to the RPMS, which then files the information in its database, including PCC.

### **XML Technology**

XML is subset of the Standard Generalized Markup Language (SGML) defined in ISO standard 8879:1986 that is designed to make it easy to interchange structured documents over the Internet. XML files always clearly mark where the start and end of each of the logical parts (called elements) of an interchanged document occurs. XML restricts the use of SGML constructs to ensure that fallback options are available when access to certain components of the document is not currently possible over the Internet. It also defines how

Internet Uniform Resource Locators can be used to identify component parts of XML data streams.

By defining the role of each element of text in a formal model, known as a Document Type Definition (DTD), users of XML can check that each component of document occurs in a valid place within the interchanged data stream. An XML DTD allows computers to check, for example, that users do not accidentally enter a third-level heading without first having entered a second-level heading, something that cannot be checked using the HTML extensively used to code Web documents.

However, unlike SGML, XML does not require the presence of a DTD. If no DTD is available, either because all or part of it is not accessible over the Internet or because the user failed to create it, an XML system can assign a default definition for undeclared components of the markup. XML allows users to do the following:

- Bring multiple files together to form compound documents
- Identify where illustrations are to be incorporated into text files, and the format used to encode each illustration
- Provide processing control information to supporting programs, such as document validators and browsers
- Add editorial comments to a file

It is important to note, however, that XML is not the following:

- A predefined set of tags, of the type defined for HTML, that can be used to markup documents
- A standardized template to produce particular document types

XML was not designed to be a standardized way of coding text. In fact, it is impossible to devise a single coding scheme that would suit all languages and all applications. Instead, XML is a formal language that can be used to pass information about the component parts of a document to another computer system. XML is flexible enough to be able to describe any logical text structure, whether it is a form, memo, letter, report, book, encyclopedia, dictionary, or database. XML technology provides the following:

- A universal data format
- Data objects can be serialized into text streams
- Is fast to parse, so that it can be used to pass data between processes
- Produces documents that can be passed easily over a variety of network protocols

- Has companion standards to support browser presentation, hyperlinks, and querying

A number of application categories are currently being built using XML. The following is a brief list of the more common ones.

**Document repository:** Similar to traditional SGML usage, an XML document repository can store docs in XML and deliver in a variety of presentation formats, including HTML, searchable catalogs, and print catalogs.

**Business-to-business exchanges:** As more business object formats are standardized in XML, businesses can share information and/or transactions across the Web more easily. Buy-side procurement systems have taken the lead in adopting this type of Business-to-Business (B2B) exchange. Web sites providing shared product catalogs from multiple suppliers to multiple buyers are already in existence. By sending XML data to a browser, more processing can be applied in the browser rather than relying on the server.

**Information interchange:** Metadata and content exchange between software tools. This approach is being actively explored in the data warehouse and OLAP markets. Wireless Application Protocol (WAP): The WAP Consortium (which is made up of more than 90 firms, including Microsoft) is building a unified XML standard for wireless mobile devices and services utilizing microbrowser technology.

Enterprise sharing is improved when systems loosely coupled by messages can use a common message format that is independent of any one vendor or domain. In fact, such sharing of XML business objects may be the key to implementing business processes and transactions across enterprise domains using workflow technology. Application architectures may change in even more dramatic ways.

First, the ability to push XML data to a browser along with presentation instructions in the form of XSL commands may reduce and simplify the information that a Web site has to send to a browser. It may also increase the amount of processing done by client browsers. An HTML page can be displayed in only one way, but when the data driving the page is available, the data can be displayed in many ways. For example, downloading a set of products to a client as XML data is feasible if the client's browser can sort and present the data in different ways, as requested by the client, without having to return to the HTTP server for more information.

Next, it may be possible to rethink how IHS uses the client tier in an N-tier architecture. As mentioned above, the traditional approach is to push HTML

pages and XML data to the client in response to an explicit request. With the ability to move XML data between the client and a Web server, there is now a two-way channel for exchanging data. This ability would make it possible to reverse the normal flow of data by having the client initiate a transfer of data to the Web server. In fact, by adding an onboard, personal Web server, clients could have a mechanism for handling incoming requests made by Web servers, an approach that would make Web clients and Web servers approximate peer-to-peer. The protocol for the communication would be HTTP and the data and requests exchanged would be in XML.

Following this line of thinking clients could also send XML data and requests out to more than one Web server to drive multiple business processes. The client browser could easily become the integration point between multiple Web sites, just as the application server for a Web site may be the integration point for many company-side systems. In any case, the main point is that XML data, requests, and messages running over HTTP may be the best way to avoid problems with firewalls and make the Web clients a full-functioning member of an N-tier architecture.

The most exciting new architectural approach maybe the ability to use XML-based Middleware and the exchange of XML business objects to integrate business processes across corporate firewalls. Communication between Web applications is far easier to build when a WAN protocol, such as HTTP, is available for the transport layer, and one is not restricted to LAN-based protocols/Middleware like IIOP/CORBA.

Integrating Web applications across the Internet will not be easy, even when all the technical transport problems have been solved. Our experience with Electronic Data Interchange (EDI) has shown that integrating business processes and coordinating documents is hardly trivial. Security and legally binding document exchanges are issues with which the XML community has far less experience than the EDI vendors have. Nonetheless, at a time when corporations are trying to integrate their business processes with those of key suppliers and customers and trying to outsource many parts of their supply chain, the rewards for successful inter-corporate implementations may be great.

New B2B applications are already beginning to appear. Some Web sites are already offering to host consolidated up-to-date product catalog services where suppliers can provide XML-based product specifications and catalog pages for display to buyers. Even an online auction site has begun providing a similar service to host specialty auctions. The items to be auctioned are loaded as XML documents with individual look and feel style sheets provided to each

specialty auction client to maintain a separate look and feel. XML promises to bring architecture to a new level, and we, as IT architects, have the opportunity to exploit this technology in our future environments.

### **XML-BASED WEB SERVICES PLATFORM: MICROSOFT'S NET<sup>43</sup>**

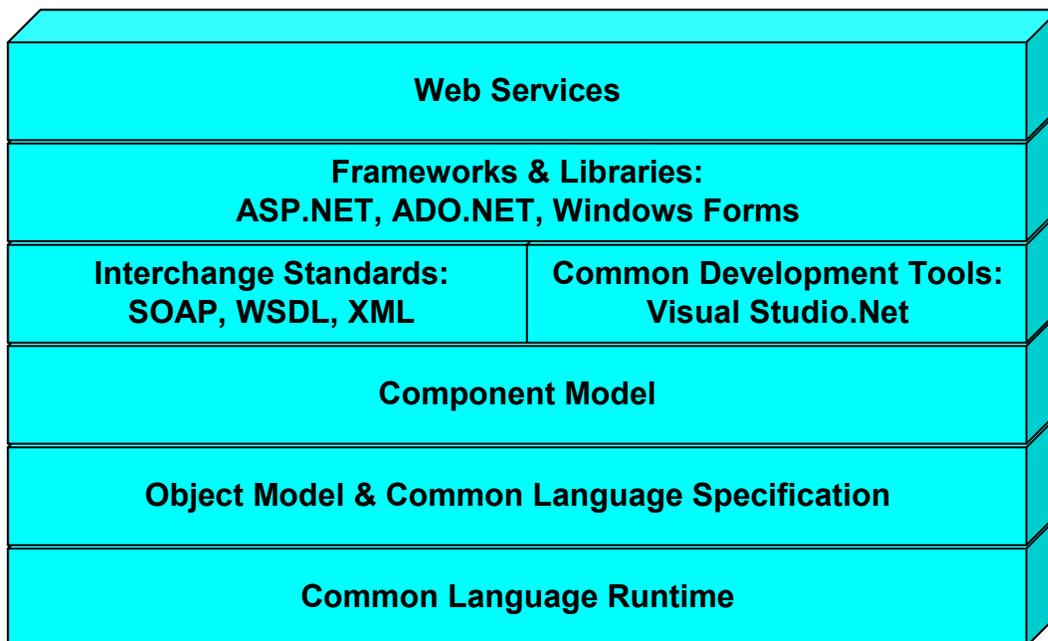
---

.NET is Microsoft's open language platform for enterprise application software and Web application development and deployment. It is a key component in Microsoft's strategy to integrate the Internet, Web services, building block services, development tools, and many other features. The projected release of the first version of .NET is late 2001 or early 2002.

#### **.NET Architecture**

Microsoft .NET provides software developers with a common environment that supports both "traditional" IT (client-server, n-tier) development *and* Web development. As shown in Exhibit 5-9, the .NET architecture comprises six layers, which are described below.

**Exhibit 5-9 Microsoft .NET Architecture.**



---

<sup>43</sup> Sources: Microsoft Developer Network (MSDN) Web site; the Developer Network Journal (DNJ) Online; and Meyer, Bertrand. ".NET is Coming." IEEE Computer, Volume 34, No. 8. August 2001.

**Web Services**, the top layer, which provides .NET users with Web services for e-commerce and business-to-business applications.

**Frameworks and Libraries**, a set of reusable components for developers, such as ASP.NET, active server pages for developing Web sites and services; ADO.NET, an XML-based that extends ActiveX Data Objects for databases and object-relational processing; and Windows Forms, a framework for graphics.

**XML-based Interchange Standards**, such as Simple Object Access Protocol (SOAP) and Web Services Description Language (WSDL), which provide a platform-independent means to encode and exchange information and objects.

**Common Development Environment**, called Visual Studio.Net, which provides facilities for developing, compiling, and debugging applications using tools and programming languages developed by other vendors, such as Cobol, Eiffel, Fortran, Perl, Python, Smalltalk, as well as Microsoft-implemented languages, such as Visual Basic, Visual C++, and the new C# (C-sharp).

**Component Model**, a new model based on object-oriented concepts, which allows developers to build “assemblies”, collections of selected classes with well-defined interfaces that do not rely on an Interface Definition Language (IDL).

**Object Model and Common Language Specification (CLS)**, which provide the conceptual basis .NET’s object-oriented type system and for language interoperability.

**Common Language Runtime**, the schema and set of compiling, translation, loading, security, memory management, version control, and non-.Net program interface mechanisms for executing .NET programs, regardless of the programming language used by the developer, on a broad spectrum of target hardware and software platforms, ranging from high-end servers and server farms, to PCs, phones, PDAs and other wireless devices, and Internet appliances.

### **Potential Role of .NET in Achieving IHS EA Goals and Objectives.**

**Integrated Software Development & Maintenance Environment.** By providing a common platform for all software development activities, .NET

removes the distinction between IT and Web development. The ASP.NET framework (more than an update of Active Server Pages) supplies tools and objects for Web-enabling existing enterprise software applications, and for incorporating the advanced processing normally associated with enterprise software development into Web applications. Under .NET, a Web page is a program, and a program can easily become a Web page.

As a result, the .NET platform provides IHS with an opportunity to establish consistent approaches for both IT and Web application development. For example, ASP.NET's Web controls enable development of Web pages that look and behave more like a modern non-Web GUI. In addition, the Web controls automatically tailor output to the client's browser, based on capabilities supported by the browser version. ASP.NET maintains session state without storing client information on the server, thereby eliminating the time-consuming, cumbersome manual coding performed now by developers to "workaround" HTML's stateless protocol to retain the client's state (i.e., retain information from one page to the next). Because .NET frameworks and libraries are tied directly to the .NET object model, compilers, and runtime facilities, the code associated with a Web page can be part of an application.

**Web Services: Delivering the Right Information to Users at the Right Time.** Under .NET, Web pages can be used as human interfaces and as application program interfaces (APIs). Each ASP.NET page is tied to a set of program elements called .NET assemblies; as a result, each ASP.NET page is already an API, which can be bundled with other components to provide Web services for information delivery. In addition, Microsoft's "Passport" technology (through Microsoft's "Hailstorm" initiative) enables a user to define a personal profile, make it available as a set of Web services, and specify who can use what parts of it. .NET, by coupling profiling technology with XML-based interchange standards as the platform-independent means of exchanging objects, provides IHS with methods for achieving the EA objective of delivering the right information, to the right users, at the right time, while assuring individual privacy and system integrity.

**Improved Security.** .NET's security policy – integrated with its component model and object model layers – combines four techniques for enforcing software development and access constraints:

- Type verification, which checks compliance with the object model's type system rules to detect and prevent "Trojan Horse" objects (i.e. objects pretending to be something other than what they are), and other security violations.

- Origin verification, using 128-bit public key encryption to prevent a .NET assembly from impersonating another software source (a Trojan Horse variant)
- A fine-grained permission facility, which enables each .NET assembly to specify the permissions it requires callers to have, and to enforce each permission on direct and indirect callers.
- The notion of “Principal”, which grants access to security levels based on the role assumed by each software element.

The .NET security mechanisms, support the IHS objectives of maintaining patient privacy, delivering information to authorized users, and of mitigating the risk of inadvertent, unauthorized, or malicious penetration of IHS IT assets.

**Improved Version Control.** As IHS web-enables its applications and extends its information exchange capabilities using XML-based web services, effective version control will become a necessity. The .NET versioning model defines a standard version numbering policy and enables developers to specify what version of each software element is required for each assembly being constructed, such as a specific version number, a range of version numbers, or the last one that worked.

**New OO-based Component Model: Simplified Component Reuse.** Under .NET, developers can build an application using multiple programming languages, selecting the programming language most suitable for each task performed by the application. The new component model removes the distinction between a program element and a software component, instead using the concept of an assembly. Each assembly has a well-defined set of interfaces. As a result, a .NET assembly can be directly used by other assemblies, without having to write a special interface definition language (IDL), as is the case with CORBA and COM technology.

**Improved Component Documentation: Metadata.** Under .NET, compilers of for .NET-supported languages retain information in the source code – the list of classes, each class’s characteristics, numbers and types of arguments, whether it’s a function or procedure, etc. –as metadata. The metadata are accessible using a .NET graphical application, and in XML format, thereby enabling applications outside of the .NET environment to access information about the component.

**Improved Language Interoperability.** IHS and its partners, such as VHS, have a significant investment in applications developed using a variety of programming languages. .NET affords IHS the opportunity to retain that

investment as IHS migrates to its target EA environment. Under .NET, modules written in different languages can call each other and, in the case of classes, inherit from each other, across languages. .NET's language interoperability offers developers the opportunity to select the programming language most suitable for a task, with the expectation that it will interface and operate smoothly with other parts of the application.

### **Current Practices & Tools to be replaced by .NET.**

.NET currently runs on the Windows operating system. However, in late 2000, Microsoft submitted key parts of the .NET technology for standardization by the European Computer Manufacturers Association (ECMA), and the recently announced MONO effort<sup>44</sup> is intended to develop an open-source implementation of .NET, based on the ECMA specifications. These efforts, coupled with Sun's endorsement of SOAP and WSDL, suggest that .NET may within the next few years become a multi-platform development environment.

The Visual Studio.NET development environment includes .NET development tools, such as Visual Studio.NET and ASP.NET, and support for Microsoft and third-party languages and tools. Only a few .NET facilities are Windows-specific. The Windows Forms framework replaces the Windows graphical API and the graphical part of the Microsoft foundation classes for C++, ASP.NET runs on Microsoft's Internet Information Services (IIS) Web server. Theoretically, most of the rest of .NET could be implemented in Linux, Solaris, and other operating environments.

Microsoft also provides COM Interop, a mechanism to ease the transition from COM to the new OO-based component model. In addition, to ease the transition of C++ applications – and C++ developers – to the .NET environment, with its strong restrictions on type mixes, .NET handles two types of code for execution: managed code, which benefits from .NET's runtime facilities, such as garbage collection, exception handling, and security, and unmanaged code, which does not comply with .NET's OO-based type restrictions.

### **Implementation of .NET in IHS Architecture**

.NET has the potential to transform software development and delivery by integrating enterprise application software development and Web development. The first step in integrating .NET into the IHS IT environment is to undertake a pilot project to determine requirements and develop a technical approach.

---

<sup>44</sup> Information about the Ximian MONO effort is available at <http://www.go-mono.net>.

Based on the results of the pilot project, and management approval, the next step is to develop a detailed plan that provides the approach, schedule, and resource allocations for migrating a predetermined set of applications to .NET. The results of this step provide the baseline for transitioning the other IHS applications to .NET.

## **SERVICE-BASED ARCHITECTURE**

---

In contrast to the software architecture of a single application, a service-based architecture provides the underpinning to bring multiple components into a cohesive whole within an enterprise. Formalizing inter-system interfaces is key to a service-based architecture.

Through formal interface definition, the supported operations and signatures are articulated so that other components can reference and depend upon them. New services can be integrated into this architecture as long as they implement interfaces corresponding to the defined signatures and behaviors. Similarly, this interface definition approach provides a means to integrate existing applications and capabilities into the architecture.

By creating interfaces supporting the defined requirements, existing and legacy applications can communicate with new service capabilities. If the interface definition steps are robust, mechanisms are provided to identify limited-subset implementations addressing only those capabilities that are required. This approach offers the enterprise significant flexibility, since services can be added into the infrastructure as needs are identified. Furthermore, through the use of standardized, formal interfaces, vendors produce competing products based upon underlying capability and not integration strategy. Therefore, the underlying service-based architecture is not impacted as a result of replacement of one (or multiple) component product(s).

Analogies can be drawn between this service-based architecture and Microsoft Windows™. Windows is a commercial framework that offers services such as video display, printer control, device driver support, operating system support, and so forth. Within this framework, applications are developed by leveraging the common components to their advantage. Windows applications are an integration of lower-level components within a business context, such as the application's purpose, to add business value.

### **COTS/GOTS**

For the service-based architecture model to be successful, production-quality components must be purchased and integrated into the software infrastructure to enable this enterprise. Just as it would be unreasonable to create a

relational database engine from scratch, the same philosophy holds true of health care components and the building blocks of tomorrow's systems.

Within current market conditions, it is of much greater value to integrate COTS application capabilities that have been customized to address project-specific requirements. As health care software products and standards mature, they bring increasing value to health care organizations. Explosive growth has already occurred in many of these areas, with core technologies available as commercial products, such as MPI support, which only a few years ago would have been custom development efforts.

Similarly, the government has invested resources across several venues, particularly CDC, DOD, VHA, and HCFA, to develop and mature health care capabilities that have previously been unavailable in the marketplace. These investments are available as COTS capabilities to other government organizations.

## **NETWORKING**

---

### **TCP/IP6**

Probably one of the most significant events to occur over the next several years will be the industry acceptance of IPv6 as the preferred telecommunications protocol. IPv6, also known as the "Next Generation Internet Protocol," IPng, the successor to IP version 4 (IPv4) was designed to provide a natural evolution from IPv4, retaining only the existing functionality consistent with the new protocol. Key changes between the protocols are the following:

- Expanded routing and addressing capabilities through using a 128-bit address size. As a result, more levels of addressing hierarchy and a significant increase in addressable nodes are attained.
- Simplified auto-configuration of addresses, with improved scalability of multicast via the addition of a "scope" field.
- Addition of "anycast addresses" to identify sets of nodes to which a packet may be delivered. As a result, anycast enables nodes to control the path over which their traffic flows.
- Header format simplification to reduce the processing and bandwidth costs of packet handling IPv6 headers.
- Encoding and improved support for IP header options to allow for efficient forwarding, less stringent length limitations, and greater flexibility in the future.

- Quality-of-service support allowing for special handling of so-labeled packets, such as real-time service.
- Authentication and privacy capabilities that support authentication, data integrity and confidentiality, and allow for defining extensions.

As part of the evolution of networking with the IHS, consideration must be paid to the transition from IPv4 to IPv6. The protocol has been engineered to allow for concurrent operation without downtime, supporting interoperability across the protocols.

During the transition, network devices will be able to maintain their existing addresses after being upgraded to IPv6. Apart from the critical-path dependency of Domain Name Service upgrades to support the new protocol, IPv6 provides the needed infrastructure to allow for concurrent operations and minimal deployment interdependency, allowing for the maximum leveraging of existing network infrastructure.

### **Broadband**

Broadband telecommunications (such as DSL and cable modems) have already made significant inroads to providing inexpensive, high-bandwidth communications to smaller locations and individuals. This connectivity has become widely available and is becoming widely used. As a result, increasing bandwidth availability at decreasing costs offers several opportunities to the health care provider.

First, this technology-enabler has direct benefits pertaining to distributed care, such as supporting home-based care, remote consultation, and telemedicine. Secondly, the cost-effective nature of this communication allows for connectivity of locations previously considered outside the scope of the networked enterprise, for instance, small clinics and remote offices.

These technologies are serving to allow previously unconnected locations to be embraced within the scope of the care enterprise.

### **Wireless**

Just as wireless technology has had profound impacts on the voice communications industry with cellular and digital services, similar impacts can be expected within data connectivity capabilities as well. Already available are “cell-modems” and wireless networking providing connectivity to mobile machines.

This infrastructure is beginning to receive large-scale visibility with Personal Digital Assistants (PDA) initiatives such as the Palm VII, enabling its users to

send and receive email and Web-based data via wireless connection within most metropolitan areas. Though not yet pervasive, this technology has significant potential, particularly within the health care industry. This technology has enjoyed early adoption within the medical community, as evidenced by the number of medical applications already available for PDA platforms.

Its integration into the health care enterprise, such as integration with workflow packages, opens several opportunities to target information directly at the individual consumers who need it – both providers and patients.

Within the technology industry, too, are efforts to address this requirements spectrum. The “Bluetooth” initiative is a consortium of vendors, led by 3COM, Ericsson, Intel, IBM, Lucent, Microsoft, Motorola, Nokia, and Toshiba, who are developing wireless protocols to allow for intercommunication of devices.

Another advancement in Wireless Technologies is the WAP. WAP is a vendor-neutral and network independent open specification for providing Internet and advanced telephony services on digital mobile phones, pagers, PDAs, and other wireless devices. The WAP Specification as recommended by the WAP Forum provides two key capabilities: a communication stack to transport data via the air, and an XML compliant markup language called Wireless Markup Language (WML) for publishing information on small screens using WAP-enabled mini-browsers. Mobile users have the capability to access Internet, obtain emails, news headlines, map directions, personalized information, and even conduct e-business transactions.

The WAP Forum ([www.wapforum.org](http://www.wapforum.org)) has wide support from more than 200 vendors and includes members such as Nokia, Ericsson, Motorola, IBM, and Microsoft.

## **SOFTWARE DEVELOPMENT LIFE CYCLE SUPPORT**

---

### **Tools Selection Methodology**

Given the increasing interdependence of products in the software development and engineering environments, it is no longer sufficient to choose tools based solely on their capabilities. Instead, tools must be considered in concert with the remainder of the development and deployment environments, choosing products which best fit into the fabric of the development environment.

As such, a tool selection methodology must be determined to ensure that product selections satisfy these increasingly complex requirements. Though a

specific tool selection methodology is not being prescribed, the key aspects of consideration are the following:

- 1) Ensure that the development suite provides for integration across the full development life cycle, such as requirement elicitation and capture through implementation.
- 2) Interfaces between products, particularly products supporting different life-cycle phases, should be standards-based to provide for vendor independence.
- 3) Identify a minimum-subset of key “critical success factors” for each product (for this step, “critical success” means that the project would fail if the product did not deliver this capability adequately). These factors will depend upon project specific needs, complementing development tools, and the maturity of the market sector of the product. Identifying the key differentiators between products in this market space eases the product selection process.
- 4) Using the critical success factors above, determine a short-list of products. Ideally, the project will be successful if it chooses *any* product from this list.
- 5) Determine the best-fit product using additional criteria. These criteria can be based on multiple sources, but tend to be more subjective than the critical success factors.

This selection approach differs slightly from traditional approaches as it invokes a two-tiered process. Singling-out products satisfying critical success factors can establish a more objective short-list. From this short list a final selection is determined. This allows teams to make product selections minimizing the risk of biased results due to favoritism (or criticism) of a product based upon past experience.

### **Tool Integration**

For development tools to support the software life cycle processes, integration across the tool suite must occur. In particular, the following steps should be considered as part of the tool selection process:

- 1) Ensure that the product being selected fits appropriately within the tool suite. It should address those functional capabilities expected of it within the context of the other tools.
- 2) For those work products to be migrated across tools as part of the development process (for example, forward engineering of models into application “stubs”), ensure that the integration mechanism is standards-based (either de-facto or industry). For example, XMI allows for models and meta-models to be interchanged across software tools.

Similarly, the Microsoft Repository provides a shared back-end supporting multiple development environments.

- 3) Whenever possible, choose a tool integration approach that allows for multiple products to be used in tandem, which helps to resist the temptation of a single-vendor solution from requirements through implementation, unless that vendor provides integration through open, public interface standards.

Application development tools and environments are particularly dynamic, as are the demands on the development community. To the extent possible, an open integration approach for the development environment affords the greatest opportunity to substitute or replace products that are not meeting expectations.

### **Software Life-Cycle Tools**

To support the increasing demands placed on IHS' IT infrastructure, several support tool categories are required. Many of these tools support the key process areas identified within the SEI/CMM.

**Requirements Elicitation and Capture:** Using formal contractual documents with outlined “shall statements” identifying system capabilities do not satisfy user community requirements. Emerging as tools to address this shortcoming are tools for joint application design (JAD) and requirements capture. These tools allow analysts to work with user communities, “mocking-up” functionality to elicitation requirements. Once discovered, these requirements can be formally managed in requirements management software.

**Simulation:** To gain a better understanding of information systems and their impacts on the enterprise, an increased demand for simulation tools is likely to occur. Software such as order entry and workflow packages has significant impacts on health care business practices and how they are performed. These impacts will need to be examined and analyzed before implementation-time to determine their optimal use. Simulation tools fill this void, allowing the analyst team to identify potential impacts of systems implementations within the care Enterprise.

**Modeling Environments:** Current trends in modeling will continue as this phase of software life cycle development increases in importance. Particularly as applications become more component-based and systems are integrated with off-the-shelf products and commercial services, the use of modeling to depict these interactions will be essential to successful delivery.

Just as it is commonplace today to employ entity-relationship modeling to support sound database engineering, the use of object models and component models to describe and formalize software architectures will grow to bring the same benefits to systems integration. Similarly, domain reference models (such as the HL7 Reference Information Model [RIM]) will allow for lessons learned to be documented and reused to the maximum advantage of their consumers. This will facilitate interoperability across like enterprises at the content level, ensuring that the supporting systems address sufficient breadth in their domain implementations.

**Configuration Management (CM):** Formal CM (both of code and platforms) will be increasingly important. As systems become more heterogeneous, encompassing multiple care organizations through contracted care and outsourcing, the need to manage and control the IT infrastructure is tantamount. CM will extend beyond “source code control” as it is often viewed today, and will also need to address requirements prioritization, release management, and platform management. The enterprise will extend beyond the desktop into the wireless world, including CM to the personal device space.

**Testing and Implementation Validation:** Receiving increasing attention in the development life cycle are automated testing tools integrated with the requirements environment. Through the use of these tools, scripted test scenarios can be “played” against implemented systems to ensure that desired capabilities have been implemented correctly.

## **OPERATIONS AND MAINTENANCE**

---

As the I/T/U enterprise moves into the future, the role of Operations and Maintenance (O&M) will become increasingly important. Particularly given the impacts of service-based capabilities and outsourcing, pressure to keep disparate integrated systems online and available will increase. Further, the high costs of on-site technical resources will drive O&M towards a virtual model with more contracted personnel responding to diagnosed problems and fewer “standby” technical resources within the enterprise.

Operations and maintenance will become more remote-oriented, with systems management capabilities managed through the network. Remote systems management centers will be capable of handling all but the most significant operational issues such as hardware repair and upgrade. Even system failures will, for the most part, be handled remotely through clustering environments. Distributed processing capabilities will allow for dynamic re-hosting at the direction of the operations center.

This operations center will be capable of performing systems administration tasks such as load balancing, session-management, and user management. User account services, such as account creation, deletion, and permissions, will be handled remotely. Transaction management and event management will be monitored and managed virtually.

The "Telecommunications Management Team," and the "Computer Systems Management Team" Albuquerque currently perform similar services that could be expanded with various operational tools.

### **Simple Network Management Protocol**

Technologies, such as Simple Network Management Protocol (SNMP), in conjunction with distributed enterprise management tools, such as Tivoli and Unicenter, provide the infrastructure to allow remote operations and maintenance across the I/T/U enterprise. Furthermore, as health care applications move from machine-centric to distributed capabilities, such as Middleware-based and n-tier solutions, load balancing and performance-based issues can be more easily addressed remotely. This minimizes dependence on site personnel to perform these tasks.

### **Configuration Management**

Beyond source code control and version management, CM plays a significant role in operations and systems deployment. By identifying formal configuration items down to the desktop or beyond, CM provides the means to support, troubleshoot, and rectify problems as they occur within deployed systems. More details on CM follow in the Seat Management section.

### **Remote Administration and Seat Management**

Beyond management of the technical infrastructure supporting the enterprise, such as server and network platforms, the future enterprise will see increased demands on outsourced seat management strategies. In this approach, a per-seat cost is incurred to maintain hardware at the user workstation. Outsourcing this activity accrues several benefits, particularly related to technology refresh at the desktop. Management is performed both remotely and on site, as the maintenance agreement dictates. Similarly, it is customary for response-time requirements to be built into the agreement, ensuring that devices are not out of service for longer than a predetermined time.

Seat management allows formal configuration control down to the desktop, providing for hardware, operating system, and workstation support. This control addresses software CM, new user/hardware installation, and technology-refresh of existing infrastructure at what is generally a per-seat cost. The technology refresh frequency is inherent in the seat management

contract and can be performed at intervals as frequent as budget and strategy suggest. Eighteen to 24 months is generally considered desirable.

### **Storage Area Networks**

Storage Area Network (SAN) is a dedicated network that connects all of the enterprise servers and clients to a shared pool of storage assets. Consequently, any server connected to the SAN can access any storage asset also connected to the SAN. Because storage is externalized and decoupled from the servers, the architecture ensures storage on demand. Although standards are currently still evolving and vendor alliance driven, SANs are beneficial because they do the following:

- Enhance scalability by speeding up the movement of large quantities of data using bandwidth provided by storage channels
- Eliminate load on enterprise network backbones
- Increase information availability and server performance
- Manage operations effectively (be able to seamlessly perform such functions as hot swapping, mirroring, clustering, load balancing, replication, disaster recovery, fail-over, and incremental upgrades/reconfigurations)
- Centralize storage asset management—reducing total ownership costs
- Support superior data speeds, for example, upwards of 100 megabytes per second

## **SECURE TECHNOLOGIES**

---

### **Introduction**

In recent years, the scope and depth of information security issues have expanded tremendously. In the past, computer security was an IT responsibility and entailed user IDs, passwords, and access permissions. With the explosion of networking and the Internet, security is now a pervasive requirement that must be considered in each component of the EA.

Information exchanged inside or outside of I/T/U facilities, as well as with other government agencies and external third parties, should be protected against eavesdropping, information alteration, and falsely represented sending or receiving parties. Information can be protected with hardware, hardware/software combinations, or by software-only solutions. Industry standards are being developed to implement authentication, verification, and information exchange data encryption seamlessly. This section discusses the different techniques to secure communication and data exchange.

## **Secure Socket Layer**

Netscape Corporation developed Secure Socket Layer (SSL) to secure electronic transmissions across the Internet. Since Netscape released this protocol to the public domain, it has been incorporated into all major Web server and desktop browser products. Various versions of the protocol are in use today with SSL version 3.0 being the latest release. SSL protocols use both public and secret key cryptography techniques to encode data. Of the two encoding techniques, the more modern and applicable method is public-key usage.

SSL also provides a method of authentication of a client/server connection. When a secure connection between client and a server is requested, the process of authentication takes place, whereby keys are exchanged and messages are encrypted and decrypted using the keys from each entity. If the exchanged messages match, the secure channel is opened between the devices.

## **Public-key Infrastructure (PKI)**

Much has been written about the benefits of deploying a PKI within an environment that uses the Internet for information exchange. PKI can be thought as a set of standards and services that facilitate using public-key cryptography and X.509 digital certificates in a networked environment. PKI offers many benefits because of its potential to solve many problems with a single set of technical standards and methods.

PKI is a set of mechanisms that supports enhanced security services within a wide range of applications. It provides encryption, privacy and digital signature services to support commerce, balancing the legitimate needs of commerce, governments, and the privacy of citizens. More specifically, PKI is a system of digital certificates, certificate authorities, registration authorities, and directory services programs that verify the identity and authority of each party involved in transmitting information.

Until now, many enterprises have been reluctant to invest in PKI technology because some of the important standards are still under development, many questions remain about its implementation, and available solutions have been incomplete and difficult to deploy.

Most of the issues, however, have become clearer or have been resolved. Vendors have begun to deliver products with PKI implementations or have a firm statement of direction concerning their solutions to secure transmissions using PKI technology.

## **Digital Certificates (DC)**

DCs are also called digital IDs and are a structured set of information that a Certificate Authority (CA) has issued. These certificates are electronic equivalents of driver licenses, passports, and security cards.

DCs contain the owner's public key and name, an expiration date, the name of the certificate issuer, and digital signature of the CA that issued the DC, a serial number, and perhaps some other information. Once this information is placed within a certificate, it cannot be modified without re-registration of the certificate because the key values are generated based on the information within the certificate that makes the certificate virtually tamper proof.

Once issued, the DCs can be used for the following applications:

- **Privacy and confidentiality:** for message encryption and decryption
- **Integrity, authentication, and non-repudiation (digital signing/verification):** for digital signing of messages to establish the identity of the sender and establish that messages have not been tampered with
- **Access control:** to control access to facilities, Internet sites, Intranets, and other digital networks
- **Proof of document transmission (time stamping):** as an independent time stamping authority to verify dates and times of critical messages for legal and commercial use
- **Document archive and retrieval:** to validate that stored documents have not been altered and to provide controlled access to authorized individuals
- **Identification and privileges:** to establish rights and privileges, such as for licensing

Currently, digital certificates come in two types:

1. Personal certificates for use with applications or customer certification solutions (clients)
2. Server certificates for use with secure Web servers (organizations).

CAs generally offers three classes of assurance (Class 1-3 Digital Certificates) differentiated by the method of verifying a person's identity during the certification request process. Prior to issuing a DC, the CA is must verify an organization's or user's identity. The user information is then stored in the CA server, which generates a unique public key and issues a DC to the user, along with a related private key. With these keys, the user can encrypt information using his or her private key and a recipient's public key. The recipient can

decrypt the information with his or her private key and the sender's public key, thereby verifying the sender's identity.

DCs comes in many formats. The most predominant format currently being implemented is defined in the X.509 version 3 standard. This standard supports SSL 3.0 encryption and other encryption schemes.

### **Digital Signatures**

A digital signature is a piece of data that is sent with an encoded message to identify uniquely the originator and to verify that the message has not been altered since it was sent. A digital signature is an excellent mechanism for messages because it supports non-repudiation. It may legally be used to resolve disputes should one party deny that the message transfer occurred.

### **Public Key Cryptography**

One of the most popular techniques to protect valuable information is via a key system, in which information is coded according to an algorithm and can only be shared among users who hold a key or the decoding algorithm.

The government-sponsored Data Encryption Standard (DES) is an example of such a key system. Using a DES system, encryption keys are shared among parties who wish to exchange information. While this technique is effective in small networks with limited access requirements, it would have drawbacks in enterprise environments.

Other key-based encryption systems derived from the set of standards called Public-key Cryptography Standards use a pair of related keys: a public key, which is freely distributed and all users can see; and a corresponding unique private key, which is kept secret and not shared, thus ensuring privacy and verification of the sender's identity.

The public key and private key perform inverse operations and are used together. For example, if a message is encrypted with the public key, the private key decrypts it. Conversely, a message coded with the private key is validated with the public key.

One of the interesting arguments in the standards committees is the discussion of how long an encryption key should be. The key's size determines how secure the information needs to be and the number of possibilities that an intruder would have to test to break the encryption.

### **Integrated Approach**

Information security and assurance require an integrated implementation of procedures and concepts. Security is not an add on or separate component developed in isolation. Access, integrity and availability are interrelated, and an integrated approach is key to successful a security architecture.

### **Access Control**

Positive identification of system users is a core requirement for information assurance. A corollary requirement is positive authorization of user functions to provide each user all the capabilities he or she requires without allowing unneeded capabilities. This area also encompasses protecting information in transit to or from the intended user, including the concept of non-repudiation, where each transaction is directly linked to the authorized user initiating the transaction.

### **Data Integrity**

Policies and procedures are required to provide an environment where information is entered correctly, accurately manipulated, and protected from corruption, either inadvertently or maliciously. This includes disaster recovery procedures, back ups, and other procedural controls. Data integrity also covers the confidentiality of information at all points within the system.

### **Data Availability**

Information needs to be available when the user requires it. Component reliability, access path redundancy, and data recovery procedures are all components of this requirement.

## **IT PLAN**

The IT Plan discusses IHS architectural goals, an architecture implementation strategy, and the projects currently underway.

A strategic project section ties in the current IHS projects with the target architecture and illustrates the Agency's commitment to achieving the EA. The projects are ranked according to IHS and their alignment with the VA.

## **MAJOR ARCHITECTURAL ATTRIBUTES**

---

The IHS supports an information architecture that encompasses core applications, interfaces, and approaches to care delivery. The EA has the following major characteristics:

- Patient health-centered
- Service-oriented
- Standards-based
- Secure
- Component-based
- Web-enabled
- EIM-based

## **PATIENT HEALTH-CENTERED**

---

Patient-related medical information, whether in or out of the “official” medical record, has historically been facility or location-based. Even within a facility, ancillary information such as laboratory, radiology, and pathology has been kept under the control of individual services. Although these sorts of information have legally been defined as the patient’s medical record, in practice it has been very difficult to consolidate all relevant information. Paper, film, slides, and videotapes have been difficult to keep in temporal sequence or even proper diagnostic association.

In the modern era, patient care occurs across multiple locations and multiple disciplines, but patient and societal expectations are that the services rendered across these divides will, in fact, be integrated. Different providers of care will be—with patient consent—aware of, and have access to, the information that others gather or produce. Only now, with the advent of electronic medical record components, can patient-centered information be made available at whatever location.

The vision is to align the architecture with the organization's primary business of health-centered services to create a fully electronic health record. To do so, we will pursue standards-based, patient-centered Clinical Data Repositories (CDRs), and structure our data in accordance with a formalized Patient Record Architecture (PRA) to ensure that patient-related data from all variety of sources can be integrated into a single structure. In this way, an individual patient's longitudinal medical record will incorporate a true chronology of care, whether delivered completely, or only partly, within the IHS. In addition, the components of the architecture will be structured to allow the analysis of health and patterns of care across individuals and populations.

A genuine Electronic Health Record as specified by such organizations as Computerized Patient Record Institute (CPRI), American Society for Testing and Materials (ASTM), and Health Level Seven (HL7), will exist as a higher-level functional extension to both the CDR and PRA. It will provide functionality to capture, store, process, communicate, secure, and present health information.

## **SERVICE-ORIENTED**

---

The architecture vision includes implementation of a service-based architecture, also known as Common Services Architecture (CSA). In contrast to the monolithic software architecture of a single application, a service-based architecture forms a "services back plane" that will provide the technical underpinning support to open up systems and applications. Instead of viewing applications as stovepipes addressing specific niche needs, a CSA transforms these applications into the integration of granular "Lego" building blocks of common services that can be reused application to application.

The key is to create sharable interfaces capable of supporting identified requirements. Based on these services, these "Legos" can be used to enable existing and legacy applications to intercommunicate with new service capabilities. This approach provides a legitimate glide path to integrate existing applications and capabilities into the architecture. New services can be integrated into this architecture as long as they implement interfaces corresponding to the defined signatures and behaviors. The key to this architecture is marshalling the application's processing flow and promulgating department policy requiring its adoption.

This approach allows the EA to provide the architectural basis for application interoperability, a key requirement that must be addressed in new development and future purchases. Initial services included within this architectural vision include patient identification, lexical mediation, authorization and access control, authentication, and directory services.

## **STANDARDS-BASED**

---

An open systems approach based upon those standards influencing the marketplace is a constant in the vision. Widely accepted industry standards provide the strongest of architectural foundations. The architecture values many characteristics that standards help deliver, including adaptability, portability, interoperability, and maintainability.

A standards-based architecture is a strategic fulcrum when leveraging business innovation in a technology-based market. Investing in standards development and specification of standards in purchasing and design are the best means to reduce the risk of platform and vendor dependence. Reduced complexity and increased efficiency will realize reduced costs for development, support, and maintenance.

A variety of standards organizations will support the structural framework. Working at national and international levels, both within and without the health care domain, Standards Development Organizations such as International Standards Organization (ISO), HL7, Object Management Group (OMG), Accredited Standards Committee (ASC) X12, ASTM, W3C, digital Imaging and Communication in Medicine (DICOM), IHSB, and Internet Engineering Task Force (IETF) will prominently figure into our future success.

## **SECURE**

---

The IHS Security Program seeks to satisfy the two primary imperatives of every health care provider: (1) to honor the privacy and confidentiality of the patient-provider relationship by safeguarding health information from improper disclosure, release, or misuse, and (2) to provide care, which requires ready access to sensitive information. In addition, because IHS is a public organization, the second imperative—to provide health care—includes two major extensions that must also be addressed by the IHS security program: to protect public health, and to maintain law enforcement's ability to audit and investigate health care fraud.

The effectiveness of the IHS Security Program depends on the quality of its Information Technology Security Architecture (SA), which describes the major security services that are needed to safeguard IHS IT assets—the business functions, processes, information, application systems, and infrastructure that enable IHS to perform its duties—while enabling reliable, consistent, readily available access to IHS resources by authorized users and systems.

As IHS migrates health care applications to the Web—using browsers and wireless devices to support the transmission of voice, video, data, and images—

IHS security services will be provided by standards and technologies, such as Secure Socket Layer (SSL), Public Key Infrastructure (PKI), Digital Certificates, Digital Signatures, and Public Key Cryptography.

The goal of the security architecture is consistent, reliable, secure information delivery to any authorized system or user, at any time, to any place, over any path, while assuring patient privacy, data integrity, confidentiality, and availability.

## **COMPONENT-BASED**

---

A component-based architecture allows flexibility in application implementation and adaptation. Through standard interfaces, components will comprise the building-blocks supporting the entire organization as an application infrastructure fabric. Ironically, these smaller discrete components prove to be an enabler of big picture and systems thinking, addressing portability across heterogeneous platforms through a shared technological infrastructure.

Application encapsulation will be achieved both horizontally and vertically. Future applications will be purchased, or even rented, and developed based upon the extent they are able to support component integration.

When applied within systems integration efforts, this approach allows for marketplace competition based upon effectiveness. It will also minimize, or eliminate altogether, the risk of being limited to a particular vendor's product line. Concurrent development activities can occur and interoperate without the need for coordinated specialized interface or heroic delivery measures.

## **WEB-ENABLED**

---

A Web browser will be the primary delivery vehicle for the vast majority of information presentation. An architecture that embraces web-based approaches offers many opportunities for both the stakeholder and developer communities. Given the pervasiveness of the web and the degree of independence between platforms that it provides, it is a natural selection consistent with the standards-based, component-based application infrastructure that has been chosen.

Web-enabled architecture also entails the use of web technologies such as XML, XSL, HyperText Markup Language (HTML), Extensible Metadata Interchange (XMI), and HyperText Transfer Protocol (HTTP) by applications in order to deliver content to the browser. Because these technologies allow for both data and metadata transfer, they separate logic from the underlying

structure. This separation permits the browser-based application to apply information as suited, allowing for more consistency from a data integration and delivery perspective.

IHS health care delivery models will migrate to the web. Web delivery will be extended to pervasive wireless devices such as personal digital assistants, smart phones, monitoring devices, prescription writers, and two-way pagers. The web will support voice, video, data, and images.

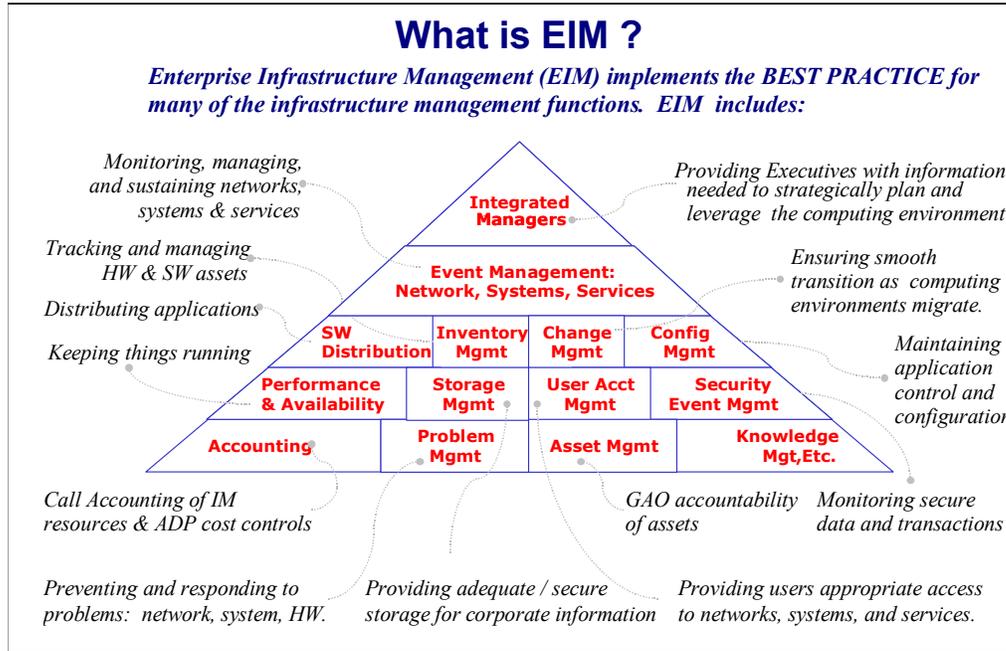
## **EIM-BASED**

---

HHS has undertaken a project to implement Enterprise Infrastructure Management (EIM) across its domain in response to PDD-63, "Critical Infrastructure Protection." EIM is an information infrastructure and systems management approach that is embodied in a set of best practices often referred to as Enterprise Systems Management (ESM). Much of the potential benefit of ESM is a result of centralizing and automating the most important, non-business specific infrastructure management functions. An efficient, high quality computing environment is the result since ESM is better than other infrastructure management approaches at meeting organizational requirements for reliable and available systems, efficient sharing of information, proper access to applications, and secure information and applications.

The HHS EIM initiative focuses on providing a Department-wide, integrated and consistent approach to cross-functional, non-OPDIV specific infrastructure management functions, such as inventory, network, system, application, and help desk management. Supported by EIM tools, each EIM component is tightly integrated and builds upon its underlying services to provide centralized management and information, as shown in Exhibit 6-1.

**Exhibit 6-1: Components of EIM45**



The HHS (and IHS) infrastructure comprises the workplace computing environment and the types of IT services provided to users. The workplace-computing environment includes the wiring of a building; the local area connectivity of hubs, bridges, and routers; the operating systems on the mainframes, servers and personal computers; the wide area network connectivity; and associated communications devices supporting both data and voice needs. The types of IT services that satisfy Department wide needs include electronic messaging, voice messaging, directory service, IS problem management, IT asset management, and software distribution.

The EIM tools selected by HHS are based on the Tivoli Enterprise and Peregrine Systems Infrastructure Management suites. They are available to all OPDIVs and provide common interfaces to a shared EIM solution. Event management will be policy-driven and rule-based to provide status information across the Department. The EIM tools will ensure consistency in corporate network connectivity and high systems availability for customers. Application software and documentation will be deployed from each designated OPDIV site to its remote sites, and configuration management will be automated.

<sup>45</sup> From HHS EIM, Vol.1 – System Architecture Overview, dated 1 Dec 2000, p.20.

## **TARGET BUSINESS ARCHITECTURE**

---

The I/T/U is facing the most profound changes in its history. We are simultaneously faced with the challenges of downsizing and restructuring our administrative infrastructure, providing for local control of resources to tribes wishing to exercise their options of self-determination, and demonstrating results consistent with the GPRA.

With participation from the Indian people, the I/T/U is exploring ways to improve essential health programs and administrative support to Indian communities. The Director convened 29 representatives of the primary stakeholders in Indian health care in January 1995 as the Indian Health Design Team (IHDT). The IHDT, which includes 22 representatives of Indian tribes and communities, submitted a report making 50 recommendations for designing a new IHS. Under their guidance, the recommendations are being implemented in two phases. The IHS system is being re-designed to address an era of rising health care costs, a growing population, and a changing health care industry. The redesign efforts emphasize patient care; strengthening government-to-government relations; streamlining administration and management; quality support services to field-based health care activities; diversification of operations; facilities staffing expansion; and fair treatment of employees.

### **IHS Mission**

The IHS' mission, in partnership with AI/ANs, is to raise their physical, mental, social, and spiritual health to the highest level.

### **IHS Goal**

The IHS' goal is to assure that comprehensive, culturally acceptable personal and public health services are available and accessible to AI/ANs.

### **IHS Foundation**

IHS' foundation is to uphold the Federal Government's obligation to promote healthy AI/ANs, communities, and cultures and to honor and protect the Tribes' inherent, sovereign rights. These three IHS fundamentals were integrated into the IHS strategic plan for the GPRA to yield the following four broad IHS Strategic Objectives to guide the Agency:

*Strategic Objective 1:* Improve Health Status to reduce mortality and morbidity rates and enhance the quality of life for the eligible AI/AN population.

*Strategic Objective 2:* Provide Health Services to assure access to high quality, comprehensive public health services, such as clinical, preventive, community-based, and educational services, provided by qualified, culturally-sensitive

health professionals with adequate support infrastructures, such as facilities, support staff, equipment, supplies, and training

*Strategic Objective 3:* Assure Partnerships and Consultation to assure that I/T/U and IHS Area and HQ achieve a mutually acceptable partnership in addressing health problems, in addition to the following:

Providing adequate opportunities for I/T/U and AI/AN organizations to participate in critical functions such as policy development and budget formulation

Assuring that I/T/U has adequate information to make informed decisions regarding options for receiving health services

*Strategic Objective 4:* Perform Core Functions and Advocacy that are consistent with the IHS' Mission, Goal, and Foundation, to advocate for the AI/AN people's health care needs and execute the core public health and inherent Federal functions

## **IHS TECHNICAL ARCHITECTURE STRATEGY**

---

To paint the vision of a target-architecture to support the IHS, the capabilities spectrum must be considered. As this view is integrated, each technology solution component cannot be considered independently but must be assessed in tandem to find a solution that offers the maximum flexibility to support the both the organization's current and evolving mission. Given these requirements, it is important to consider the following underlying principles that define the context in which the architecture must be supported:

***Support Leverage of Existing Investments***—Given the significant investments that have been made in IHS IT systems, it is important that architecture can integrate and support those systems, even as technological evolution broadens beyond their capability. As a result, the ability to support disparate timelines and heterogeneous technologies is essential, particularly as multiple automation efforts will continue. It is important to recognize that it is unrealistic and inappropriate to expect consensus within the IHS on implementation platform, language, and approach. Instead, the key to enabling the enterprise and maximizing value of these multiple investments is to ensure that they can interoperate. Architecture is the key to this interoperability.

***Support Evolving Technology and Health Care Needs***—For the target EA to carry the IHS into the future, scalability and evolution to support functional and technological growth are essential. To support these needs, there are scheduled steps in the technical process, including an ongoing re-assessment of available technologies and infrastructure, ensuring that best-fit

opportunities are being recognized and capitalized upon as heritage systems, environments, and technologies evolve. Furthermore, the target architecture must support changes to business processes, particularly those driven by technological influences and evolving care and care practice standards. A plug-and-play capability allowing for iterative refinement of component services and flexible, open interface technologies should be incorporated to allow for growth and evolution as the IHS and health care evolve.

Using standards, de-facto standards, and open systems practices, an independence between interdependent systems can be maintained, allowing the IHS to not be wholly-reliant on any vendor's hardware or software products and allows a best-fit approach to support new or replacement capabilities.

**Support Service-Based Health care Components**— Identifying the core needs of the IHS health care enterprise, and then describing those needs as services that the health care components must provide, will enable IHS to evaluate product features, determine integration requirements, and compare the feasibility of acquiring the capabilities through COTS or GOTS procurement and integration, or through in-house development.

The building-block approach shifts the emphasis of IHS IT initiatives from systems development and custom coding towards capability integration. Through efforts already expended within the global health care community, the IHS architecture comprises functional capabilities that have been identified and standardized within the global health care community. These services will be based primarily on standards coming out of the OMGs Health care Special Interest Group (SIG), CORBAMED, and COM+.

By identifying and using services based on a natural separation of functionality and concerns, the enterprise is positioned to leverage best-of-breed offerings from commercial vendors and to extend and enhance capabilities to meet organization-specific requirements.

The following sections describe the strategies to implement the IHS target architecture. The strategies cover enterprise infrastructure management (EIM), information presentation, security, integration, and network architecture. The section also includes strategic projects that are active and those that are being planned.

## **ENTERPRISE INFRASTRUCTURE MANAGEMENT**

---

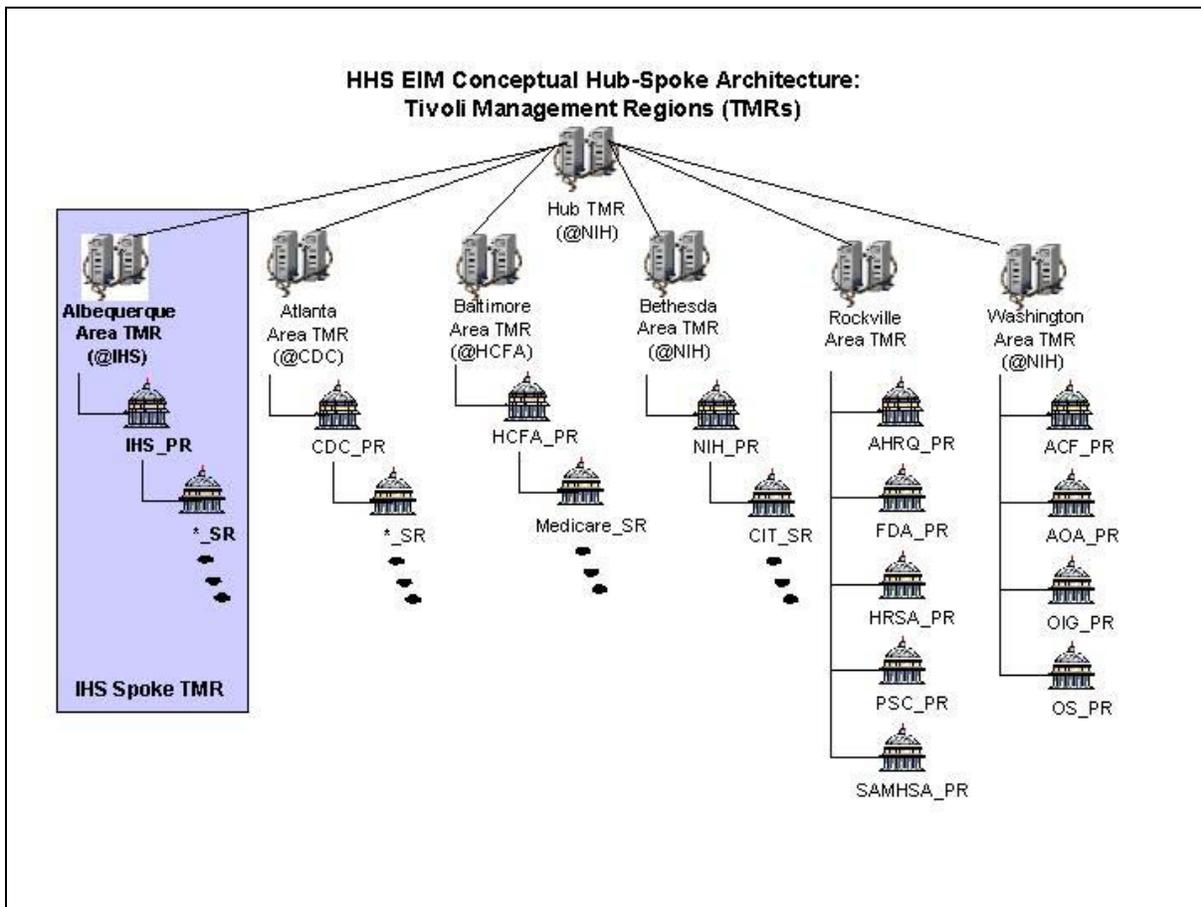
As noted earlier in this chapter, HHS is implementing an Enterprise Infrastructure Management (EIM) solution to improve the reliability, performance, and administration of its underlying IT infrastructure and

business applications. HHS is undertaking this initiative in response to Presidential Decision Directive 63 (PDD-63), “Critical Infrastructure Protection,” which requires each Federal agency to develop a vulnerability plan, implement an infrastructure framework solution, monitor the enterprise infrastructure for vulnerabilities, and respond to threats as appropriate.

HHS has acquired, and begun to deploy, a Department-wide EIM solution that is based on the Tivoli Enterprise and the Peregrine Systems Infrastructure Management product suites. These COTS tools automate common infrastructure management functions, such as asset management, security management, network and systems management, configuration management (including software distribution), user account management, and problem management.

The HHS EIM conceptual architecture divides HHS into multiple, connected Tivoli Management Regions (TMRs), based on the Hub-Spoke model. As depicted in Exhibit 6-2, IHS is one of the regional spokes.

**Exhibit 6-2: HHS EIM Conceptual Architecture**



The Hub and Spoke TMRs, deployed by geographical regions, will each have a dedicated TMR Server to manage the resources within the respective TMRs. This will optimize network utilization and system performance, and allow an OPDIV to manage its own servers and workstations via gateways attached to a regional Spoke TMR. In the physical architecture, each TMR will have a Tivoli Enterprise Console (TEC) for managing events, as well as a logical design that describes the layout and use of Profile Managers and Policy Regions in that TMR. To support the Peregrine environment, the Hub TMR will have Peregrine ServiceCenter and AssetCenter servers, and a Peregrine Inventory Network Discovery (IND) device. The IND device will be configured to populate data discovered into the EIM AssetCenter system. The ServiceCenter system will be integrated with the Tivoli Hub TMR for automatic problem notification and management. ServiceCenter will also be capable of accessing the AssetCenter system to allow for complete problem history for IT assets.

The HHS EIM initiative and its objectives provide the context in which IHS integration, security, and network initiatives will be evaluated. The major objectives of the HHS EIM initiative are to:

- Provide department wide IT security
- Manage change efficiently and effectively
- Improve Department-wide communication
- Improve operating productivity
- Lower costs and avoid costs
- Implement consistent & repeatable processes
- Manage resource utilization; release capital back into the organization
- Improve organizational learning
- Provide common, simple web interface to enable users to get what they need immediately.

## **INFORMATION PRESENTATION**

---

**Use GUI-based Interfaces.** Develop GUI-based interfaces to RPMS to take advantage of RPMS and minimize training costs.

**Adopt Visual Integration Special Interest Group standards.** Adopt Visual Integration Special Interest Group (formally CCOW) standards for implementing seamless GUI across the I/T/U enterprise. The VISIG publishes standards for the visual integration of cooperative interaction among independently authored health care applications at the point of use. The term visual integration emphasizes the specific scope the workgroup chose for addressing applications with GUIs that operate together on a personal computer or workstation.

**Expand the use of markup languages.** Explore using XML to deliver content to the workstation. XML allows both data and meta-data transfer.

## **SECURITY**

---

The IHS Security Architecture is documented in the IHS Security Architecture Plan, which is provided as Appendix A of this EA. The SA Plan identifies the information access, privacy, and security policies that IHS must address, such as the Health Insurance Portability and Accountability Act (HIPPA) and the Privacy Act of 1974. The Plan stipulates organizational roles and responsibilities for establishing and maintaining a secure operating environment; describes the basic set of security services that must be provided, as part of the IHS EIM, to satisfy policy requirements; evaluates the extent to

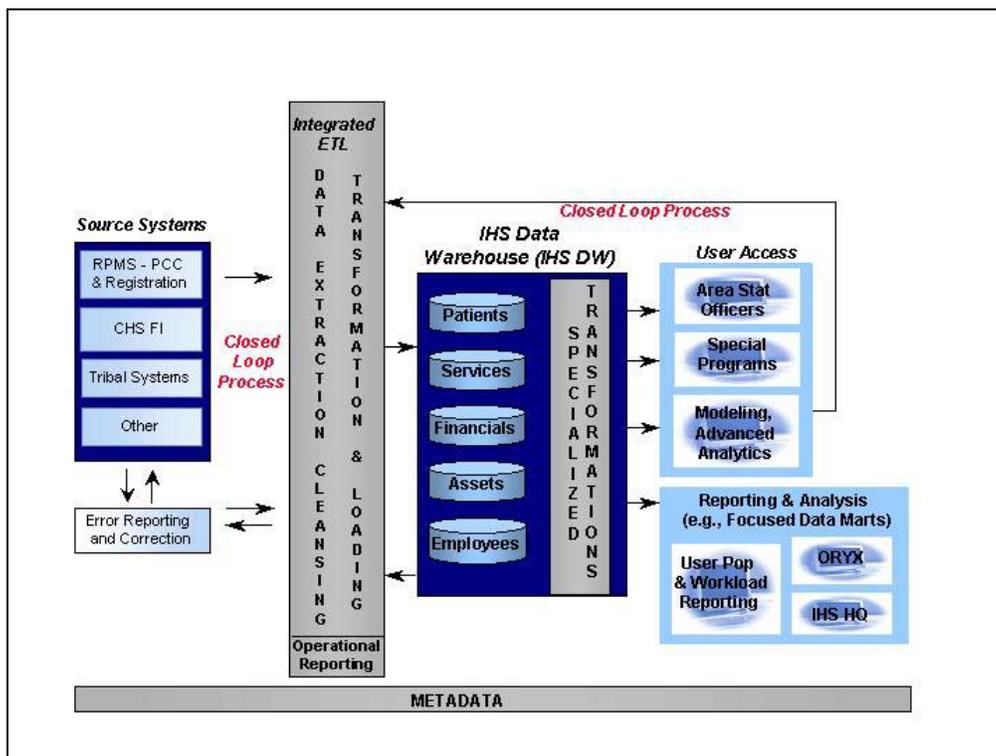


(PIDS), the Health Care Information Locator Service, and the Clinical Observation Access Service (COAS).

The notional architecture also depicts a care facility that allows a user at an MS window workstation to access the GCPR through a CORBA/COM. This operation will be transparent to the user. I/T/U care facilities will be able to communicate with each other through HL7 or COM interfaces. Exhibit 6-4 illustrates that HL7 interfaces provide access to patient data stored in the legacy MUMPS as well as a state-of-the-art DBMS backend. For example, having deployed HL7 in the enterprise provides the flexibility for data interchange for CPRs and MPIs. Another notional consideration is the use of Integration Engines to manage data access and integration, query processing and transaction within the I/T/U.

***Implement IHS National Data Warehouse.*** The Enterprise Data Warehouse (EDW), as shown in Exhibit 5-7, has an HL7 3.x interface allowing decision support data to be collected and distributed by using XML. This scenario allows the agency to take advantage of HL7 data interchange services and capability to distribute data effectively using XML. Exhibit 6-4 provides a conceptual model of the IHS National Data Warehouse.

**Exhibit 6-4: Conceptual Model of IHS National Data Warehouse**



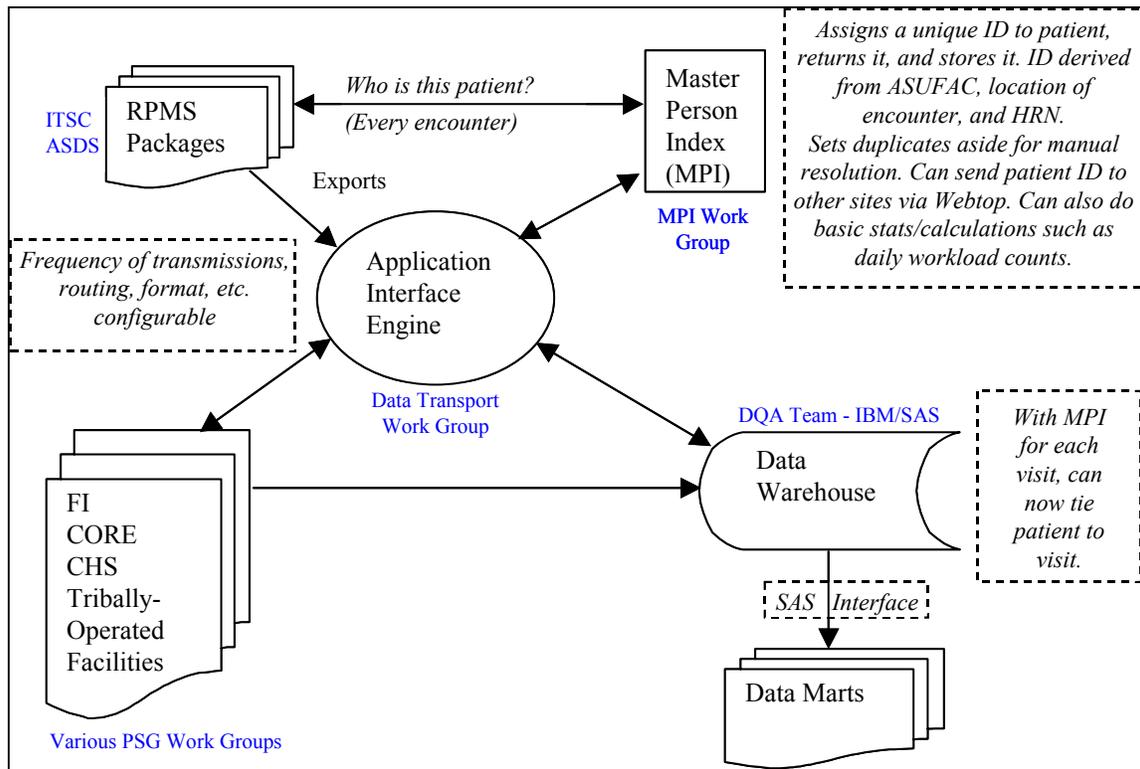
A data warehouse will provide IHS an essential means to meet its business challenges pro-actively. The added value of a data warehouse is that it adds time as a dimension of business data. This additional dimension makes possible the application of trend and cohort analysis over IHS historical data store. The results of these kinds of analysis provide a basis for future improvements in existing services and the possibly creation of new services in the future. In addition to the software tools with which the data warehouse will be implemented, the efficacy of the data warehouse will depend on the quality and the completeness of the metadata that will drive the ETL processes and the end-ser analytical processes. Although it is not elaborated in figure 6-4, the metadata used to support the data warehouse include at least the following (in addition to the normal types of metadata associated with DBMS environments):

- Maps and correlations of input and output formats of data sources and targets
- Business rules that define data transactions and transformations
- Business rules that address conflict resolutions for the same data drawn from different sources or at different times

- Business rule to address missing data—within records as well as across files
- Error correction rules
- Maps of value domains (semantic mappings) so that meanings of data domains will not be lost over time

Exhibit 6-5 provides an overview of the future movement of data within IHS.

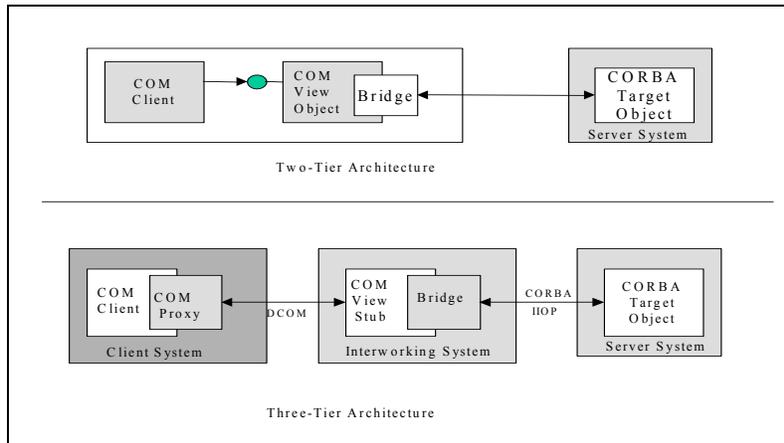
**Exhibit 6-5: Future Movement of Data Within IHS**



The key to the proper movement of data depends on the rules that affect the data and the robustness of the middleware—the application interface engine.

**Implement COM+/CORBA Bridges.** Bridging allows programmers to use a local “bridged proxy” to access a CORBA object. Bridging gives the object the capabilities and characteristics of a COM object, even though the programmer is accessing a remote CORBA object. Consider using bridging to interface with external partners and applications. Exhibit 6-6 illustrates how bridging is accomplished and shows a COM object communicating bi-directionally with a CORBA object and a bridge between a COM+ server and a CORBA server.

**Exhibit 6-6: COM/CORBA Bridging**



The health care technical architecture framework described a health care environment in which patient information is readily accessible, regardless of the system on which the data are stored and managed. Within the I/T/U health care enterprise, patient data is stored at the health care facility from which the care is provided. In order to share data across the enterprise, I/T/U will depend on distributed object technologies from Microsoft and from the OMG. These technologies fall under COM+ from Microsoft and CORBA from the OMG. The I/T/U relies on CORBA to interface with the GCPR and COM+ services to interface with the MUMPS-based legacy system.

**Use XML mapping.** XML is rapidly becoming the transport mechanism for several interchange formats including HL7. HL7 version 3.x messages will be based on XML messages derived from the HL7 RIM. Major software giants, including Microsoft, are currently adopting XML.

**Use XML as the data transport mechanism for EDW.** The NPIRS database's purpose is to provide IHS management with decision support information. This information includes patient registrations, patient clinical encounters, patient dental encounters, and financial data. Given this wealth of information, IHS can meet HCFA requirements for justifying expenditures and can show return on investment for health care operations.

IHS data are both data-centric and document-form. Data-centric data include patient registration data, such as name, address, phone number, and date of birth, while document-form data include the doctor's diagnosis and detailed description of the patient's health issues and procedures.

The challenge is to decide how to store and retrieve the data. Some possible approaches are the following:

- Using a relational, object-oriented, or hierarchical database and either built-in or third-party Middleware
- Using an XML server (a platform for building distributed applications, such as e-commerce, that use XML for data transfer)
- Using an XML-enabled web server that can build XML documents from data in a database.

Currently, the transformation process is labor intensive and involves I/T/U personnel at the AOs manually going through the local data to make sure all business rules have been met.

## **INFORMATION REPRESENTATION**

---

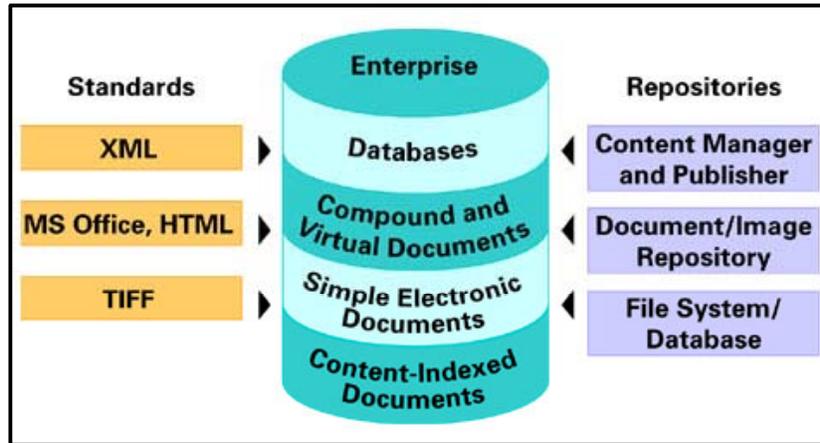
***Implement a Data Modeling Strategy.*** Data modeling represents an enterprise's or application's data. Data models include enterprise, entity-relationship models, and object models. Enterprise models represent the functions as well as the organization's data and information. As new technologies are developed, data and enterprise modeling tools are being improved, such as the applying object technology. The current trend is to integrate data modeling and process modeling into a unified effort. A data model is a valuable tool to develop business applications quickly and accurately. The iterative process of data modeling helps to do the following:

- Understand the nature of the business data and activities
- Organize and document relevant data and activities
- Identify and eliminate data, activities, and interactions that are either redundant or missing
- Ensure communication based on agreed-upon terminology
- Develop a basis to understand future change implications

***Apply Document Management Strategy.*** These strategies are document manager's solutions to integrate processes, people, and technology to optimize and automate what were, historically, paper-based business processes.

Exhibit 6-7 describes an architecture that supports the management process.

**Exhibit 6-7: Document Management Architecture**



**Adopt Patient Record Architecture (PRA).** A PRA provides a formal set of relationships between clinical content with respect to the subject and circumstances of care. The PRA provides the structure for the formal electronic health record, and can serve as the evidential record, presuming that sufficient context and security are included.

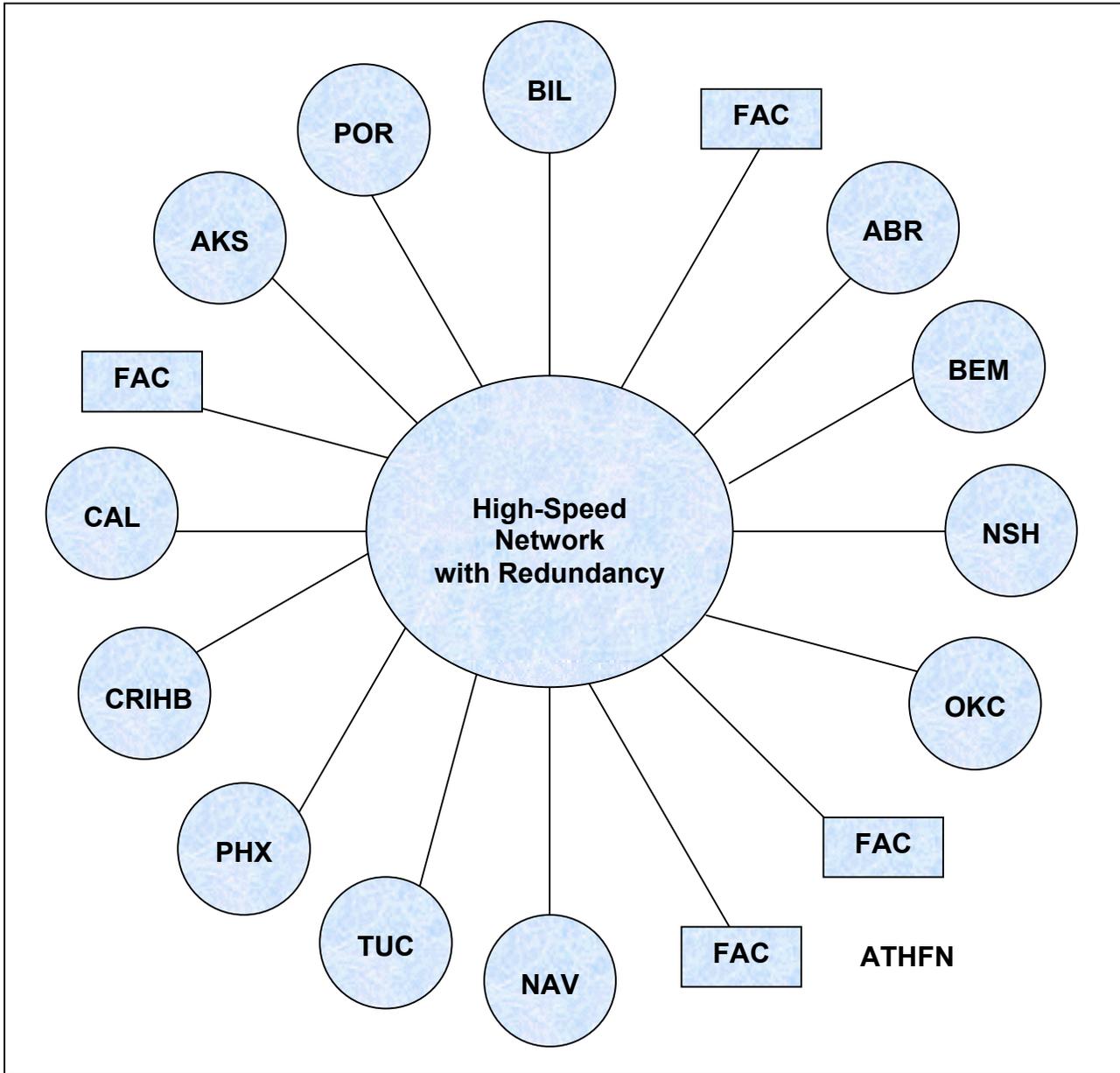
A PRA brings to the formal health record a consistent means and structure to represent content. The architecture acts as a “record template” structure to which patient records must comply. This structure offers a significant advantage in that it enables interchange of health records across systems and care organizations. HL7 has developed the PRA, an XML-based clinical document architecture that provides an exchange model for documents of varying complexity levels. Using the PRA, Version 3, enables systems to create XML documents that incorporate HL7 message content, to generate messages from document content, and exchange and process messages and documents between disparate systems.

When addressing areas of intersystem interoperability of clinical records, or maintaining and storing clinical records, a patient record architecture can address all identified requirements.

## NETWORK ARCHITECTURE

In any flexible, robust enterprise network, such as the high-speed network depicted in Exhibit 6-8, design must reflect several core principles.

**Exhibit 6-8: IHS Network Architecture**



The I/T/U health care network should perform the following:

- Be standards-based and vendor-independent
- Reduce costs by enabling maintenance and management

- Support changing patient care and business needs by allowing for substantial growth in traffic volume and the number of interconnected devices
- Accommodate fast-changing technology with clear transition strategies and migration paths
- Protect existing investments by integrating legacy systems well
- Support unprecedented mobility of both people and facilities
- Be realistic about existing capital outlays and network infrastructures

The I/T/U target network architecture must do the following:

- Support a mixed-media infrastructure based on fiber or category five station cabling
- Support multiple WAN technologies, such as frame relay, Integrated Services Digital Network [ISDN], Switched Multi-megabit Data Service (SMDS), Asynchronous Transfer Mode [ATM]
- Permit migration to high-speed protocols and infrastructures, such as fast Ethernet and ATM, as required
- Support both switching and routing
- Support comprehensive server and network management
- Support multiple networks for file, print, communications, applications, and database servers, such as Windows NT/BackOffice and UNIX
- Use TCP/IP as a primary transport protocol, while encapsulating or segmenting and managing non-standard protocols, such as SNA and IPX/SPX
- Support business continuity needs, using redundant or fault-tolerant components
- Support both centralized and decentralized server configurations
- Support voice, video, image, and data traffic
- Support "any-to-any" connectivity for system-to-system and user-to-user communications
- Be centrally manageable and supportable by the enterprise-wide information systems organization, enabling easier support, improved licensing coordination, maintenance and implementation, and improved economies of scale

## STRATEGIC PROJECTS

---

This section discusses the strategic projects identified within each architectural vision component that will help IHS achieve its desired EA and increase compatibility with the VHA.

## PROJECT AREAS

---

The strategic projects described in the paragraphs that follow are organized into four development areas:

- Data Representation
- Data Exchange
- Systems and Applications
- Enterprise Infrastructure Management (EIM)

Those projects that the VHA is undertaking and that IHS will be able to leverage and incorporate are indicated below. The other projects represent those that either IHS or both agencies will or have undertaken. Over the next 5 years, RPMS and VHA's VistA will undergo changes in the following areas.

**Data Representation.** Projects related to data representation include the following initiatives that develop standard data formats across information systems:

- Clinical Repository (VHA)
- Lexical Services (VHA)
- Corporate Data Registry (VHA)
- Patient Record Architecture Analysis (VHA)
- Information Modeling
- National Provider Identification
- Person Name Standardization

**Data Exchange.** Projects related to data exchange include the following initiatives that develop standard methods for accessing, transferring and using information:

- Application Use of Messaging
- Web-accessible Patient Record (VHA)
- Interface Engine
- Federated Master Patient Index
- GCPR/MPI Implementation
- Data Movement

- Common Tool Set (VHA)
- Electronic Data Interchange

**Systems and Applications.** Projects related to systems and applications include the following initiatives that require modifying or developing systems and applications to support information capture, storage, transfer, and analysis.

- Application Encapsulation (VHA)
- Enterprise (Corporate) Data Warehouses and Data Marts
- Consistent Operating Environment
- VHA VistA Infrastructure Compatibility and Reuse
- VHA VistA Application Compatibility and Reuse
- CPRS
- RPMS GUI Patient Chart/RCIS/ARMS Deployment
- IHS Implementation of CACHE'

**Enterprise Infrastructure Management.** Projects related to EIM include:

- The HHS EIM initiative to deploy a Department-wide EIM solution, based on the Tivoli and Peregrine tool suites
- Security initiatives to improve and maintain the integrity of the HHS infrastructure, systems, applications, and information by strengthening authentication measures and access controls, such as the Security Services project and Electronic Signature Study (VHA).
- Connectivity initiatives to provide the telecommunications technology and bandwidth to support IHS' informational needs, such as the WAN Backbone project.

Lower level details of the individual project plans for each project are available but not included in this document. These areas lay the foundation or the infrastructure to deploy top priority systems or applications, such as integrated billing, achieving a CPR, integration with COTS/GOTS solutions, decision support, interoperability, and increased functionality in departmental applications. In Exhibit 6-9, each project is ranked according to its importance to IHS and the VA.

## **PROJECT EVALUATIONS AND RANKINGS<sup>46</sup>**

---

To manage resources and project profiles development, it is critical to rank them in order of importance and codependence. To determine order of

---

<sup>46</sup> *RPMS Growth Path Plan*, May 2000, Vn. 1.0

importance, each initiative was analyzed with respect to its overall benefits to the I/T/U. These benefits were based on the ability of the project profiles to meet and align with organizational strategic objectives. The initiatives were then ranked based on those benefits and their dependence on one another. These are ranked according to the IHS Notional Architecture and importance to achieve compatibility with the VA. Exhibit 6-9 summarizes the ranking of the project profiles and includes VHA's ranking of their projects:

**Exhibit 6-9: Project Evaluations and Rankings**

Project Name EA-Related Projects	IHS Rank	VA 2000 Rank
<b>VHA VISTA INFRASTRUCTURE COMPATIBILITY AND REUSE</b>	1	
<b>SECURITY SERVICES</b>	2	3
WAN Backbone	3	
HHS EIM Deployment	Unknown	
Application Use of Messaging	4	8
Interface Engine	5	2
Data Movement	6	
Electronic Data Interchange	7	
RPMS GUI Patient Chart Deployment	8	
IHS Implementation of CACHE'	9	
VHA VistA Application Compatibility and Reuse	10	
Corporate Data Warehouse and Data Marts	11	10
Computerized Patient Record System (CPR)	12	
Lexical Services	13	4
Information Modeling	14	
National Provider Identification	15	
GCPR/MPI Implementation	16	13
Person Name Standardization	17	
Application Encapsulation	18	12
Clinical Repository (VHA)		1
Patient Record Architecture Analysis (VHA)		5
Web-accessible Patient Record Pilot (VHA)		6
Corporate Data Registry (VHA)		7
Consistent Operating Environment (VHA)		9
Electronic Signature Study (VHA)		11
Common Tool Set (VHA)		14

**DATA REPRESENTATION PROJECT PROFILES**

Exhibit 6-10 lists the strategic projects in the left column and describes their purpose, describes the associated problems and the solutions.

**Exhibit 6-10: Strategic Projects**

<b>Data Representation Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Clinical Repository</b>	<p>To create a clinical repository that represents a patient's electronic longitudinal health record.</p> <p>*VHA only project, IHS will monitor this project for potential applicability.</p>	<p>Providers have difficulty accessing complete patient information from heterogeneous systems in a standard format. In many cases, the information is text-based and cannot be used to support computational needs, such as alerts, reminders, drug and interactions. The current approach of presenting patient information from departmental applications is resource intensive (both personnel and systems) and difficult to modify to meet changing needs.</p>	<p>This project will consist of multiple phases. The first phase will consist of a contracted study of how best to institute a clinical repository in VHA followed by a cost benefit analysis. Subsequent phases will depend on the outcome of the initial phases. The ultimate goal is to implement a clinical repository based on a patient record architecture and supported by a lexicon and lexical services. IHS will leverage VHA studies and activities in this area.</p>
<b>Corporate Data Registry</b>	<p>To create a data registry that identified detailed information about the data in its systems.</p> <p>*VHA only project, IHS will monitor this project for potential applicability.</p>	<p>Individuals and systems that access VHA data are often unclear as to what the data is and how it was developed. The current information environment of VHA consists of multiple systems with minimal information regarding metadata ("the information and documentation which makes data sets understandable and shareable for users" - ISO Standard 11179). There are currently no standards that identify the classification, attribution, definition, naming, and registration of data elements within VHA systems. Even worse, it is often not know if VHA collects a certain element or what system(s) it resides on.</p>	<p>The VHA will create a corporate data registry that identifies detailed information about the data in its systems, (a data encyclopedia of sorts). This data registry will provide standards for the development of data elements and will help users in assimilating information. A corporate data registry will provide VHA with a consistent, sharable set of data across systems and will increase the quality of information captured. Creation of a corporate data registry will further ensure that data is stored in an accurate, compact way that improves data quality and limits data redundancy.</p>

Data Representation Project Profiles			
	Purpose	Description of Problems	Description of Solutions
<b>Information Modeling</b>	<p>Since information modeling is an ongoing activity for the GCPR Program, it consequently also is for the participating agencies. IHS is required to describe the content of information in its health information systems, primarily RPMS, via information models. Information modeling of RPMS will enable application developers and process engineers to visualize what systems and information are available throughout an enterprise and facilitates new application development along with process reengineering.</p>	<p>Individuals and systems that access IHS data are often unclear as to what the data is and how it was developed.</p>	<p>Combinations of ER and UML diagrams will be utilized to model the information and show what the data is and how it is utilized.</p>
<b>Lexical Services</b>	<p>To create a set of lexical services that supports the exchange of health care information.</p> <p>*VHA only project, IHS will monitor this project for potential applicability.</p>	<p>The lack of a standardized reference for clinical terminology across VHA, as well as between VHA and other health care organizations, inhibits the recording, transmission, retrieval, and analysis of clinical information in a precise manner and independent of clinic or hospital. As a result, sharing of information within and between health care organizations is also inhibited.</p>	<p>A robust lexicon and a set of lexical services are needed to support the meaningful exchange of health care information. Complete lexical services not only serve to translate different terms of like conceptual meaning, but more importantly, include conceptual maps that support expressing and transmitting complex and modified concepts while retaining their expressive details.</p>

<b>Data Representation Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>National Provider Identification</b>	<p>To assign a unique provider identification number to health care providers in order to meet legislative requirements.</p>	<p>The Health Information Portability and Accountability Act of 1996 (HIPAA, Public Law 104-191) requires that the Secretary of Health and Human Services (HHS) adopt standards for electronic health care transactions, unique health identifiers, code sets, security, and privacy. Within the scope of HIPAA, the Health Care Financing Administration (HCFA) is to establish and maintain a program for identification and enumeration of all health care providers.</p>	<p>This process will require that each IHS facility submit its list of active clinical users (e.g., physicians, nurses, social workers) and organizational providers (e.g., medical centers, outpatient clinics) to a IHS National Provider Index (IHSNPI). The IHSNPI will, use a set of identifying attributes (e.g., name, SSN, DEA number, etc.) to determine if the provider is a new provider and, if so, will assign a provider ID number. Organizational providers will be enumerated using appropriate identifying attributes. Where it has been determined that the provider is enumerated already, the IHSNPI will return that ID. IHS will, in turn, provide the full list of enumerated providers to HCFA for inclusion in their National Provider System (NPS). IHS software used to submit Medicare and other third party billings will include the provider ID. IHS will also use the provider IDs for coordination and tracking of health care across IHS facilities.</p>
<b>Patient Record Architecture Analysis</b>	<p>To analyze multiple patient record architectures that can be used to build a structure that supports patient information exchange.</p> <p>*VHA-only project; IHS will monitor this project for potential applicability.</p>	<p>Providers have difficulty accessing complete patient information from heterogeneous systems in a standard format. In many cases, the information is text-based and cannot be used to support computational needs (e.g., alerts, reminders, drug interactions, etc.). Providers also have difficulty exchanging health information electronically with other providers.</p>	<p>This project proposes to adopt a patient record architecture (PRA) that can be used as the basis for implementing a clinical repository and that supports the exchange of patient information. This architecture will provide a unified structure to support an electronic health record and help define such a record. There are several patient record architectures to choose from. This analysis will determine the patient record architecture that VHA should adopt to meet its needs.</p>

<b>Data Representation Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Person Name Standardization</b>	To establish a standard way to specify and store a person's name.	IHS does not enforce a uniform procedure for recording names of persons in RPMS/VistA. This has led to duplicate entries for individual patients within systems, health data being associated with wrong patient records, and problems in matching records across systems. Name suffixes (Jr., III, etc.) have caused the most problems; IHS has issued conflicting instructions and RPMS/VistA applications are based on conflicting requirements on how name suffixes are recorded.	<p>In the short term IHS should re-issue a clear policy on how to use the existing person name fields. Either the PIMS or HL7 RPMS/VistA application (depending on which format is chosen) must be patched. Facilities must bring all recorded person names into compliance with the policy.</p> <p>The medium term solution is for all IHS database person name fields to be recorded and stored as five components: Family Name, Given Name, Middle Name, Name Prefix, and Name Suffix. RPMS/VistA applications should be revised to use a common set of APIs for entering, editing and retrieving person names.</p>

**DATA EXCHANGE PROJECT PROFILES**

Data Exchange Project Profiles			
	Purpose	Description of Problems	Description of Solutions
Application Use of Messaging	<p>To make IHS and Vista applications message aware. HL7 and X12 are internationally supported messaging standards. Although HL7 has been part of IHS DIR's technology architecture since 1997 and some initial steps have been undertaken by the Agency, further work is needed. IHS must plan for the migration from HL7 Version 2.X to 3.X messages and message specifications and the utilization of X12 messages to meet HIPAA requirements.</p>	<p>The IHS' network-based organization requires the integration of its information systems to provide optimal service to patients and the best use of resources at multiple facilities. IHS must be able to share information within its facilities and with external organizations at low cost and with ease. The current IHS messaging capability has improved to provide reasonable support, flexibility, efficiency and ease of implementation to meet the information sharing objectives of IHS. Further work on the use of COTS products and migration towards open systems is ongoing. Use of this messaging capability by RPMS applications, however, is very limited.</p>	<p>The solution is to increase the use of the IHS messaging capability by RPMS applications by making them "messaging aware." Work should also continue on development of a robust messaging system utilizing a variety of inter-application/site communications and applications protocols that will enable standardized sharing of IHS information. A messaging infrastructure using these components will facilitate information sharing between local applications, VISN level systems, and corporate level systems. In addition, this messaging infrastructure will support the interfacing of existing applications with COTS products.</p>

<b>Data Exchange Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Common Tool Set</b>	<p>To analyze and select different developmental tools to use in to create applications and databases.</p> <p>*VHA-only project; IHS will monitor this project for potential applicability.</p>	<p>VHA currently uses an M-based suite of software products augmented by use of Delphi for GUI front ends. While this suite has served VHA's needs in the past, the need for additional development capabilities and the need to incorporate COTS and GOTS products into VistA necessitates the expansion of this tool set. Expansion of the VistA tool set will ensure that VHA users have state-of-the-art tools for delivering VHA IT solutions.</p>	<p>VHA will employ a suite of software development and database management tools both for the development of in-house software and the management of COTS/GOTS software. A standard set of requirements for all products will be developed so that the highest level of interoperability can be achieved. Standards for data access, query and interchange will be defined with the objective that users perceive VistA as a seamless system. Selection of COTS/GOTS solutions will be weighed against criteria for database features. New in-house products will be developed using the newly identified technologies. Technical Services will ensure that evaluation of all developer and user tools meet required criteria with minimal resource impact on VHA medical facilities. A migration strategy to evolve VistA from its current environment to one that employs new tools will also need to be developed. As this environment evolves, VHA must also ensure that the complexity of the VistA does not exceed the ability to effectively manage the overall system and that the necessary skills needed for success – both for product development and system operations – are invested in VHA IT staff.</p>
<b>Data Movement</b>	<p>To simplify and accurately move data between I/T/U facilities and NPIRS. Modify update programs to conform to new database design created during the database enhancement project.</p>	<p>The current extract and transmission of data creates several challenges and integrity problems.</p>	<p>Information common to multiple extracts will be combined.</p>

<b>Data Exchange Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Federated MPI</b>	Create new programs to comply with new GCPR/Master Person Identifier requirements.	An increased need exists to exchange information with other enterprises. Each enterprise has its own unique patient identifiers that need to be exchanged and aligned to ensure proper identification and sharing of patient information.	The IHS MPI system will be enhanced to interface with other MPI systems to exchange patient identifier information and align identifiers between enterprises. The solution will be based upon the federated MPI capabilities developed for GCPR. Federated meaning that multiple MPIs can share and correlate unique patients between each other without having to keep creating a single global MPI.
<b>Interface Engine</b>	To implement a commercial interface engine to manage multiple interfaces between systems thus reducing the total number of interfaces that have to be supported.	No standard methods currently exist for accessing and transferring information from the RPMS. This lack of standardization causes massive variations in the way information is accessed and transferred throughout the organization. In addition, with no standards for interfacing with the RPMS, the ability to use and deploy COTS products is difficult due to various access and messaging methodologies.	IHS will procure and implement an interface engine that supports multiple industry standard messaging (e.g., HL7, X12, DICOM) and communication (e.g., TCP/IP) interfaces. This implementation will provide a consistent format and method for accessing and transferring information from the RPMS. The interface engine will facilitate future development initiatives that require interaction with RPMS. The interface engine will also streamline the interaction with outside systems without the need to change the behavior of existing operational systems.

Data Exchange Project Profiles			
	Purpose	Description of Problems	Description of Solutions
Web-accessible Patient Record (Pilot)	<p>To pilot test the use of web technologies to share health care information.</p> <p>*VHA-only project; IHS will monitor this project for potential applicability.</p>	<p>VHA has always had a significant need to share health care information between health care facilities. The reorganization of VHA health care facilities into networks has made this need critical. The need to share health care information extends beyond VHA and includes contract and other non-VHA providers. Health care information must be shared in a secure, reliable and efficient manner.</p>	<p>Major advances are being made in Web-based technologies to support information sharing. These technologies have the potential to support the secure, reliable and efficient sharing of health care information. A pilot test of a Web-accessible patient record will be conducted to determine whether current Web-based technologies can support the sharing of health care information required by VHA. The goals of the pilot test will be to:</p> <ul style="list-style-type: none"> <li>• Determine the impact of a Web-accessible patient record on the wide area network</li> <li>• Determine if security needs such as single sign-on, access control, authentication and authorization can be met</li> <li>• Determine if the Web-based technologies can support efficient access to health care information stored on heterogeneous hardware and software platforms and in heterogeneous databases</li> <li>• Determine if the implementation of Web-based object technology can provide an adaptable and efficient interface between heterogeneous applications</li> <li>• Determine if the VHA MPI can be efficiently integrated into a Web-accessible patient record</li> </ul>

**SYSTEMS AND APPLICATIONS PROJECT PROFILES**

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Application Encapsulation</b>	To provide standard methods for applications to use to access and store information.	IHS's M-based applications currently do not employ a standard method to access information. As systems/individuals within IHS require information from the M-based applications, interfaces must be developed each time. This lack of a consistent methodology for accessing application information has led to a variety of access methods and inconsistencies in the information received. Without a consistent method to access information in RPMS, the implementation of COTS products (an OI focus for future development initiatives) becomes much more complex.	The solution is to completely encapsulate M-based applications by creating a common interface for accessing information. This solution will eliminate the discrepancies of information access by providing a computing environment in which systems that need to access RPMS must use an application programming interface (API) to access the data. APIs are interfaces that allow systems to access information in a standardized manner. The APIs will be developed so that they define business rules, standardize access to the data and are based on standard messaging protocols. The result will be elimination of discrepancies in information access and support of data consistency throughout the organization.

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Computer-based Patient Record (CPR)</b>	<p>To establish a Computer-based Patient Record through the testing and deployment of a Computer-based Patient Record System.</p> <p>The Institute of Medicine (IOM) in 1991 defined the computer-based patient record as an: "electronic patient record that resides in a system designed to support users through availability of complete and accurate data, practitioner reminders and alerts, clinical decision support systems, links to bodies of medical knowledge, and other aids."</p> <p>The IOM report also defined the computer-based patient record system as: "the set of components that form the mechanism by which patient records are created, used, stored, and retrieved...It includes people, data, rules and procedures, processing and storage devices, and communication and support facilities."</p>	<p>At the current time, the IHS IT solution lacks an integrated CPR that meets the recommendations from the IOM report. While RPMS is able to meet the majority of our individual and population based clinical needs, there are many components that are currently lacking within the system. At the current time, there is also a lack of available fiscal resources to develop adequate functionality of RPMS. In addition, the recent IOM report on Mistakes highlights the need to have an integrated CPR. It is clear that a CPR that allows for point of entry care in certain clinical areas can result in decreased clinical mistakes, as well as improved health status for individuals and populations.</p>	<p>An integrated, interactive, GUI based CPR, such as the VHA's CPRS, would allow IHS to meet the individual as well as population health care needs in a fiscally responsive manner. In addition, IHS currently recognizes the need for fiscal/billing issues to be integrated with CPRS. CPRS is a solution to the IT needs of the I/T/U clinical settings. In addition, close collaboration with the VHA and DOD through the GCPR project has recently illustrated the value of diverse clinical input in designing an information framework. This current work has helped set the stage for ongoing relationships and sharing of IT solutions to medical issues.</p>

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Consistent Operating Environment</b>	To establish a common desktop operating system across VHA.	VHA's current operating platform varies across the organization and does not fully support the VHA's information management and information sharing needs. Employees cannot universally use email, imaging, file management software, or web browser-based applications. To meet VHA's strategic goals, all employees must be able to access the tools to perform their job functions and must be able to share information. Also, VHA cannot easily use current technology and COTS products universally across the organization because of the use of multiple operating platforms.	This project converts all VHA system users to either a Microsoft Windows NT operating system with workstations utilizing Intel processors (Wintel platform) or Thin Clients using Terminal Server technology provided by Microsoft or other third party vendors. The NT and Thin Client environments enable access to information management components such as e-mail, imaging, file management software, web-based Internet and Intranet applications, and GUI components of Vista. All NT client desktop computers can be managed via the Systems Management Server (SMS) software to standardize and facilitate software installation and inventory. The Terminal Server environment is centrally managed, eliminating the need for SMS as a management tool. In both environments, the system administrator will be able to easily "lock down" the NT environment to maintain controlled, consistent, and secure configurations across sets of users without changing hardware or software.

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Enterprise Data Warehouse and Data Marts</b>	<p>Establish data warehouse systems that use an open standard compliant RDMS with tools available for on-line analysis. The data warehouses will be scalable from a facility level up to an enterprise level. It will contain information aggregated from the I/T/U's administrative systems, health care systems, and other external data sources such as Medicare, Medicaid, and Private Insurance entities. Create Common data sets for area data to be accessed via the Intranet and also provided to the areas via compact disc.</p>	<p>None currently exists other than at the National level.</p>	<p>Incorporate a streamline process that involves the use of XML and other tool sets available in the workplace.</p> <p>The EDW Project has been ongoing over the past year.</p>

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>IHS Implementation of CACHE</b>	To evaluate the use of CACHE in place of MSM as the M database application supporting the RPMS platform.	IHS has been using MSM as the underlying M database platform since 1986. CACHE, while still M based, is significantly different than MSM both in features and in use. Porting the RPMS programs and database to CACHE will involve significant time, effort and resources. In particular, there are approximately 200 developers and system managers that have no experience with the CACHE product and would require extensive training. Also a revamping of the development environment that currently focuses on MSM would have to take place. To facilitate IHS application reuse and compatibility, I/T/U will need to convert to CACHE as the underlying DBMS since much of the ongoing IHS technologies in the future will rely on it components.	<p>First a test bed environment should be set up with the porting of one of the test sites to occur under "lab" conditions. Then after ample testing it could be moved to the actual field site for live use. A review of this site along with one or more others would establish the mechanisms for use throughout IHS. Software and test systems will need to be obtained for starters.</p> <p>As of June 2001, the project is now developing procedures for converting from MSM to Cache, and is conducting conversion process tests. The project goal is to complete the conversion of the majority of RPMS sites from MSM to Cache.</p>
<b>RPMS GUI Patient Chart/RCIS/ARMS</b>	To deploy the GUI based RPMS Patient Chart Application to use as a benchmark for the full use of GUI based applications in RPMS and to allow non-RPMS traditional users to assist with the order entry process.	RPMS currently has no officially released applications that utilize a GUI. This lack of a GUI for providers and other selected users has led to the underuse of RPMS and increased training costs. It is also unknown what impact the introduction of a RPMS GUI application will have on computing resources and capacity management.	The RPMS Patient Chart will be tested and deployed to those facilities wishing to deploy it. Valuable experience regarding the appropriateness of the screens and the data entry process will be gained. In addition capacity management metrics will be obtained for determining the impact of a GUI application on current hardware platforms.

<b>Systems and Applications Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>VHA/Vista Application Compatibility and Reuse</b>	To bring the RPMS versions of VHA VistA applications to the same release and patch level and to establish an ongoing effort for staying at the current release.	The deployed IHS versions of VHA VistA applications are not current with the latest VistA release. When IHS is not current, the end users are prohibited from taking advantage of the latest functionality that is provided. While there are core packages such as Laboratory, Radiology, ADT, Scheduling, Outpatient and Inpatient Pharmacy that need to be updated there are other applications that IHS would like to deploy such as the VistA CPRS that have dependencies on the deployment of these latest versions.	A renewed effort to bring those VistA applications that IHS has deployed, including PIMS, Laboratory, Outpatient and Inpatient Pharmacy, Scheduling, National Drug File, and Adverse Reaction Tracking to current release and patch level will be made. In addition to those applications that IHS currently has deployed an effort to deploy the latest version of VistA's CPRS dependant packages of Health Summary, OE/RR, Lexicon, Problem List, Scheduling, Text Integration Utility, Visit Tracking, Pharmacy Data Management, Radiology, Consult/Request Tracking, Central Mail-Out Pharmacy, Dietetics, Vitals, PCE, and Imaging will be made.
<b>VHA/Vista Infrastructure Compatibility and Reuse</b>	To bring the RPMS and VHA's VistA infrastructure to the same release and patch level and to establish an ongoing effort for staying at the current release.	VistA and RPMS applications utilize core infrastructure packages to manage device handling, database management, mail, and middle ware issues. These core packages include VHA's Kernel, FileManager, RPC Broker, MailMan, Toolkit and HL7. Without the latest release and patches deployed, IHS is unable to utilize the new functionality added to VistA's infrastructure. IHS is also unable to test and deploy any VistA applications that have dependencies on the last version and patches of the VistA infrastructure.	All patches to the VistA infrastructure will be examined and tested for compatibility and then incorporated into the current IHS infrastructure. Resources will be identified to make this an ongoing effort.

## ENTERPRISE INFRASTRUCTURE MANAGEMENT PROJECT PROFILES

<b>Enterprise Infrastructure Management Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>Electronic Signature Study</b>	<p>To establish an electronic signature capability that meets HIPAA standards.</p> <p>*VHA-only project; IHS will monitor this project for potential applicability.</p>	<p>As VHA moves to a mixed application environment (COTS and in-house), the current M-based methods of supporting electronic signatures are no longer sufficient. Federal regulations that the HHS is issuing based on HIPAA legislation will require a much more stringent electronic signature implementation than currently exists in RPMS. IHS must adopt new standard methods to support electronic signatures that meet HIPAA requirements.</p>	<p>This project is a study to determine how to establish an electronic signature capability that meets HIPAA standards. The study will evaluate the technology choices/options and the costs related to the technology choices.</p>
<b>Security Services</b>	<p>To establish a security infrastructure that supports PKIs and VPNs.</p>	<p>As VHA and IHS moves to a mixed application environment (COTS and in-house), the current M-based methods of supporting user authentication, access control, privileges and authorizations are no longer sufficient. VHA and IHS must adopt new standard methods to support these security services.</p>	<p>Authenticating users, controlling access and determining user privileges and authorizations in a mixed application environment can be accomplished by implementing standards-based technologies such as PKI and an enterprise-wide directory service. These technologies will enable VHA and IHS to implement a single, consistent, scalable set of security services.</p>

<b>Enterprise Infrastructure Management Project Profiles</b>			
	<b>Purpose</b>	<b>Description of Problems</b>	<b>Description of Solutions</b>
<b>WAN Backbone</b>	To provide the necessary telecommunications technology and bandwidth necessary for current and future requirements.	As IHS moves toward an application environment based on distributed objects, the need for Area/Tribes to flexibly access a robust, reliable, bandwidth-on-demand network backbone becomes critical.	The IHS WAN needs to support the integration of voice, data and video through installation of a robust, reliable, ubiquitous, bandwidth-on-demand WAN based on SONET/ATM technologies. All WAN hardware must be fully redundant and support automatic failsafe capabilities. There must be at least two connections between the WAN and each local area network. This high quality network will be able to support distributed applications such as CPR, video teleconferencing and telemedicine, access to knowledge bases for clinical decision support and security mechanisms such as PKI and directory services. There have been ongoing discussions about the best way to implement such a network.
<b>HHS EIM Initiative</b>	To establish an HHS Department-wide EIM solution to address PDD-63.	HHS is concerned about the reliability, performance, vulnerability, and cost of its underlying infrastructure and infrastructure management functions.	HHS is deploying throughout the Department a common EIM solution, based on the Tivoli and Peregrine product suites.  EIM implementation at IHS sites is scheduled to begin 3Q2001, with completion in 2Q2002, per the HHS EIM, Volume #1, System Architecture Overview, dated 1 Dec 2000.

**APPENDIX A - IT SECURITY ARCHITECTURE PLAN**

**Indian Health Service (IHS) Information Technology (IT) Security  
Architecture**

## **EXECUTIVE SUMMARY**

The IHS Security Architecture presented herein is derived from several different sources of information. The overall structure of the document is based upon the Chief Information Officers' Council Federal Enterprise Architecture Framework. Details on the current architecture and policies of IHS are derived from the IHS policies and the System Security Plans for the major applications within IHS. The IRM plan and the IHS Data Transportation Concept of Operations drive the future architecture. Additional comparisons and structures were derived from the Information Technology Architectures of other government agencies; namely, HHS, HCFA, and VHA.

**TABLE OF CONTENTS**

**EXECUTIVE SUMMARY ..... I**  
**TABLE OF CONTENTS ..... II**  
**INDEX OF EXHIBITS ..... VI**  
**INTRODUCTION ..... 1**  
EA Definition, Purpose, and Benefits..... 3  
Scope ..... 3  
Document Organization and Summary..... 5  
Overview..... 6  
Guiding Principles..... 7  
**DIRECTION ..... 18**  
Future Business Views ..... 18  
DIR Vision, Goals, and Strategies ..... 21  
Business Drivers..... 26  
Technology Drivers..... 28  
Legislative Drivers ..... 29  
RPMS Growth Plan..... 32  
Phase 1 ..... 35  
Phase 2 ..... 38  
Phase 3 ..... 39  
Phase 4 ..... 39  
**FRAMEWORK..... 40**  
Critical EA Attributes..... 40  
Health Care Information Principles ..... 42  
Health Care Information Infrastructure..... 43  
IHS Technical Reference Model ..... 48  
Definition of Standards and Products ..... 50  
Purpose of Standards and Products ..... 51  
Benefits of Standards and Products ..... 51  
Overview of Standards ..... 57  
System Services ..... 57  
Communications Services ..... 58  
Information Services ..... 62  
Security Services ..... 72  
**CURRENT ENVIRONMENT ..... 76**  
Current Business Architecture ..... 76  
IHS Network Architecture ..... 76  
Details of the Network Architecture..... 79  
Application Software Environment..... 82  
RPMS Software Architecture & Environment..... 83  
Operational Environment..... 87  
NPIRS Software Architecture ..... 90  
RPMS Processing Platform Environment ..... 90

IHS RS/6000 Configuration Overview.....	90
<b>NEW &amp; EMERGING TECHNOLOGIES.....</b>	<b>96</b>
process improvement .....	96
Achieving IHS Goals by Implementing Data Management Practices.....	100
Distributed Architecture .....	101
Microsoft Tier Architecture.....	103
OMG Tier Architecture.....	104
Component-Based Software Engineering (CBSE).....	105
Internet Inter-ORB Protocol (IIOP).....	106
Storage Services .....	106
Semantics and Terminologies .....	112
Interface Technologies .....	114
XML-based Web Services Platform: Microsoft's NET.....	118
Service-based Architecture.....	123
Networking.....	124
Software Development Life Cycle Support .....	126
Operations and Maintenance.....	129
Secure Technologies.....	131
<b>IT PLAN .....</b>	<b>136</b>
Major Architectural Attributes.....	136
Patient Health-centered .....	136
Service-oriented.....	137
Standards-based .....	138
Secure .....	138
Component-based .....	139
Web-enabled .....	139
EIM-based .....	140
Target Business Architecture.....	142
IHS Technical Architecture Strategy .....	143
Enterprise Infrastructure Management .....	144
Information Presentation.....	147
Security.....	147
Integration Strategy .....	148
Information Representation .....	153
Network Architecture .....	154
Strategic Projects.....	157
Project Areas .....	157
Project Evaluations and Rankings .....	158
Data Representation Project Profiles.....	161
Data Exchange Project Profiles .....	165
Systems and Applications Project Profiles.....	169
Enterprise Infrastructure Management Project Profiles .....	175

**APPENDIX A - IT SECURITY ARCHITECTURE PLAN ..... 177**  
**EXECUTIVE SUMMARY ..... 178**  
**TABLE OF CONTENTS ..... 179**  
**TABLE OF EXHIBITS ..... 183**  
**INTRODUCTION ..... 184**  
    Scope ..... 184  
    Model..... 184  
    Document Use and Content ..... 184  
**POLICIES, PRINCIPLES, AND RESPONSIBILITIES ..... 186**  
    IHS Security Principles ..... 186  
    Security Architecture Policies ..... 187  
    Privacy and Security ..... 189  
        Agency Responsibility ..... 191  
    Security Responsibilities ..... 191  
        IHS Chief Information Officer (CIO)..... 191  
        IHS and Area Information System Security Officers (ISSO) ..... 192  
        Area Director ..... 192  
        Area Information Systems Coordinator (ISC) ..... 193  
        Subordinate ISSO ..... 193  
        System Owner/Custodian..... 193  
        Records Management Officer ..... 194  
        Privacy Act Officer/Coordinator ..... 194  
**ENVIRONMENT AND CURRENT ARCHITECTURE ..... 195**  
    Information Users ..... 195  
    Information Resources..... 196  
    Risks and Threats..... 196  
    Summary of Current Security Architecture and Business Requirements..... 198  
**TARGET ARCHITECTURE ..... 199**  
    Technical Protection Measures ..... 199  
        Public Key Infrastructure (PKI) ..... 199  
        Virtual Private Networks (VPN) ..... 200  
        Confidentiality, Integrity, and Availability Services ..... 200  
        Standards ..... 204  
    Physical Protection, Contingency Planning, and Disaster Recovery ..... 204  
        Physical Protection..... 205  
        Business Continuity and Contingency Planning (BCCP)..... 205  
    Administrative Security, Personnel Security, and Procedures ..... 205  
    Logging and Auditing ..... 206  
    Training and Awareness ..... 207  
    Incident Detection and Response Capability ..... 208  
**ARCHITECTURE MAINTENANCE AND COMPLIANCE ..... 210**  
    Architecture Management..... 210  
    Architecture Compliance..... 211

**SUMMARY .....212**  
**SOURCES .....213**  
**HIPAA SECURITY SERVICES .....214**  
    HIPAA Security Requirements..... 214  
    1. Administrative Procedures..... 214  
    2. Physical Safeguards..... 215  
    3. Technical Security Services..... 216  
    4. Technical Security Mechanisms ..... 217  
    HIPAA Electronic Signature Requirements..... 217  
**APPENDIX B - GLOSSARY OF TERMS .....218**  
**APPENDIX C-ACRONYMS.....265**

<b>TABLE OF EXHIBITS</b>
--------------------------

<i>Ehibit A-1 Data Types and Level of Risk</i>	198
<i>Exhibit A-2 Basic Security Services and Technical Measures</i>	202
<i>Exhibit A-3 Emerging Technologies – Candidates for Inclusion in IHS Security Architecture</i>	211

## **INTRODUCTION**

### **SCOPE**

---

The IT Security Architecture provides guidance for protecting IHS's business assets: systems, software, and information resources. The key goal of the information security architecture is to provide uniform secure information delivery to any authorized system or user, at any time, to any place, over any path, while ensuring patient privacy, data integrity, confidentiality, and availability. Any less comprehensive alternative will allow risks, weaknesses, and vulnerabilities to be overlooked, and, as a result, provide inadequate protection for the architecture as a whole. In this context, it is important to note that the information security architecture must address information in all its forms, not just electronic. Thus, the policies and protections will deal also with information as paper documents, and as verbal and fax transmissions.

### **MODEL**

---

The IHS Security Architecture is based on the Chief Information Officers' Council Federal Enterprise Architecture Framework (version 1.1, September 1999). The architecture begins with Level I, a high-level view, by specifying the architecture drivers in terms of IHS policies and design principles. Level II and III include the current architecture and the target architecture. Finally, the areas that need to be addressed for HIPAA compliance are specified in Appendix A. The result is a concise and compliant statement of the current and target Security Architectures.

### **DOCUMENT USE AND CONTENT**

---

The responsibility for allocating resources and accepting business risks lies with IHS management. The responsibility for carrying out procedures and implementing an effective system and controls lies with every employee and user, both staff and management. This architecture looks at security from the viewpoint of both groups.

This document is organized into the following seven sections to provide an answer to security questions that must be addressed by the architecture:

1. Introduction: A statement of scope and overview of methodology.
2. Policies, Principles, and Responsibilities: An itemization and explanation of the architecture drivers.
3. Environment and Current Architecture: A brief summary of the "as-is" model and business requirements for security. The current architecture

illustrates how the external entities link to the IHS data center and describes the access requirements for the individual domains.

4. Target Architecture: The “to-be” model and business requirements for security. The Target Architecture illustrates the target boundaries and links to the IHS data center and describes the access requirements.
5. Architecture Management and Governance: A process for keeping the target architecture current and meaningful, and guidelines for promoting Security Architecture compliance.
6. Summary: A summary of the document.
7. Sources: A list of documents referenced in the development of the IHS IT Security Architecture.

## **POLICIES, PRINCIPLES, AND RESPONSIBILITIES**

The enterprise-wide integration of IT security is one of the objectives guiding the IHS Enterprise Architecture (EA.) The security principles and policies described in this section form the basis for decisions on formulating the target Security Architecture. Government-wide security themes form the basis for the IHS security principles. The security principles form the basis of IHS security policies. Responsibilities for implementing the policies are also described in this section.

### **IHS SECURITY PRINCIPLES**

---

Several government-wide themes form the basis for the security principles developed for IHS. Government agencies have a responsibility to protect the sensitive data and information they collect against anticipated threats or hazards that could result in harm to any individual on whom the information is maintained. This responsibility must be balanced with need to increase public access for other types of information. Government needs to meet these responsibilities while improving performance, sharing, management, and results in the use of IT, including reducing information collection burdens on the public.

**IHS Information Security Principle 1:** IHS information assets must be protected from loss, corruption, or disclosure, and protection measures must be balanced against the operational cost imposed on the business, and must be appropriate to the threats those assets face and the potential impact of those threats.

**IHS Information Security Principle 2:** As threats evolve and new threats emerge, the security posture must be re-evaluated and protections adjusted appropriately.

**IHS Information Security Principle 3:** The information owner determines the degree of acceptable risk; the level of protection must be appropriate to the risk and the value of the asset being protected. The custodian of the data must adhere to the handling requirements imposed by the information owner.

**IHS Information Security Principle 4:** Protective measures must not prevent necessary business from being carried out.

**IHS Information Security Principle 5:** Protective measures must account for the special needs of each IHS/Tribes/Urban (I/T/U) site.

**IHS Information Security Principle 6:** Security protections must be implemented in a layered, mutually reinforcing way. An appropriate combination of technical controls; physical controls; administrative controls; training and awareness efforts; and auditing, logging, and incident response should be selected to mediate risk and minimize the impact from security threats. Controls can be chosen such that one control's strength supports any weakness in other controls, and that multiple controls protect against any specific threat.

**IHS Information Security Principle 7:** Security controls need to be designed as products or processes integrated from the beginning of the software/systems development or integration, rather than added as an afterthought. Security is but another aspect of quality. A system should do only what it is designed to do – no more, no less. Poor quality is a security risk.

**IHS Information Security Principle 8:** Security mechanisms should balance the level of assurance with ease-of-use. The user should not be overly encumbered by security to the extent that productivity is seriously impacted or a strong motivation to work around security safeguards is generated.

**IHS Information Security Principle 9:** IHS information policies and implementation shall fully comply with all Federal laws and regulations and shall be consistent with the policies and guidelines of the Department of Health and Human Services (DHHS).

## **SECURITY ARCHITECTURE POLICIES**

---

**IHS Security Architecture Policy 1:** Every information asset (i.e., every system process, data set, or document) must have an owner. When information is contained in media which are isolated, such as physical documents or removable electronic media (e.g., floppy disks, removable disks, CDs), the owner is assumed to be the person authorized to hold that media; accountability follows the possession of the asset. For systems, processes, or data that are electronic in nature, in an interconnected environment, a written statement of ownership must document accountability. Such statements must be readily available for inspection.

**IHS Security Architecture Policy 2:** Anyone accessing information using systems or processes must be authorized to do so. When access is limited, such as for accessing private or proprietary information, then the

accessing party must be properly identified and authenticated prior to the access as being duly authorized for the access. Everyone is authorized to see or copy public information, so no authentication is required by policy.

**IHS Security Architecture Policy 3:** Access to sensitive information, systems, or processes will be logged, and the owners (or their designees) will periodically review the logs for anomalous entries. Logs will be subject to audit.

**IHS Security Architecture Policy 4:** All information assets must have explicit boundaries that define the domain of ownership and responsibility. Where information flows across boundaries, the interfaces with other assets must be explicitly understood, defined, and documented. Any trust relationships that grant or imply access authorization across interfaces must be detailed and accounted for in the design and implementation of access roles and rights across the interface(s).

**IHS Security Architecture Policy 5:** All sensitive assets must have a documented security plan that describes the asset and its boundaries. Sensitive assets are those assets that require protection from unauthorized disclosure, modification, or use as defined by Federal legislation or regulations. The security plan documents the current operation of the asset/system; evaluates and enumerates the risks and threats that the asset is vulnerable to; explains the security protections that mediate the risk to acceptable levels; describes the tests that validate the protections work as intended; includes the documented results of those tests; and contains a certification by the asset owner that the protections are adequate and operate correctly. Security plans must follow the IHS **System Security Plan Methodology** [IHS does not have this document] standard. Security plans must be submitted to the IHS Information System Security Officer (ISSO) and accredited by the Chief Information Officer (CIO) prior to the asset being placed into use. IHS business partners must also prepare a Memorandum of Agreement/Memorandum of Understanding (MOA/MOU) that specifies the security of data exchanges. IHS contracts for many services, including a variety of IT services; all contracts that require or allow the contractor access to IHS information must require the contractor to comply fully with IHS Security Policies.

**IHS Security Architecture Policy 6:** Everyone, whether IHS staff or contractor, must receive IHS-approved information security training before being granted access to sensitive information assets.

**IHS Security Architecture Policy 7:** IHS security policies apply equally to IHS staff and contractors.

**IHS Security Architecture Policy 8:** Quality configuration management is essential. Effective configuration management helps ensure that all modifications to a system are properly reviewed, tested, documented, and approved before being implemented. Every change should be reviewed for the security implications to the system. Configuration management also allows for rolling back to a previous baseline configuration if a critical error is discovered in an update after it has been implemented. All mission critical systems must have configuration management in place and adhered to.

**IHS Security Architecture Policy 9:** The IHS security boundary is penetrated only at a very few specifically authorized gateways or control points. Unauthorized paths through the IHS security boundary are not permitted.

**IHS Security Architecture Policy 10:** If IHS out-sources a function, responsibility for security functions or activities will reside with a Federal management official with accountability and responsibility for the security mission.

## **PRIVACY AND SECURITY**

---

The interaction of privacy and security results in a requirement to protect and secure from disclosure and unauthorized access those records that are maintained which are protected by the Privacy Act. The Health Insurance Portability and Accountability Act (HIPAA) provides an additional basis for privacy requirements. Privacy and confidentiality are the driving forces behind security.

The Privacy Act of 1974 can generally be characterized as an omnibus code of fair information practices, which attempts to regulate the collection, maintenance, use, and dissemination of personal information by Federal government agencies.

Broadly stated, the purpose of the Privacy Act is to balance the government's need to maintain information about individuals with the rights of the individuals to be protected from unwarranted invasions of their privacy stemming from the collection, maintenance, use, and disclosure by Federal agencies of personal information about them. The Privacy Act focuses on four basic policy objectives:

1. To restrict disclosure of personally identifiable records maintained by agencies.

2. To grant individuals increased rights of access to agency records maintained on them.
3. To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
4. To establish a code of fair information practices, which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Any item, collection, or grouping of information about an individual that is maintained by an agency including, but not limited to, his education, financial transactions, medical history, and criminal or employment history, and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph, is considered a record under the Privacy Act. A group of any records under the control of any agency from which information is retrieved by the name of the individual, or by some identifying number, symbol or other identifying particular assigned to the individual, is called a System Of Records (SOR).

HIPAA was signed into law on August 21, 1996. Title II, Subtitle F (Administrative Simplification) of the act has the goals of improving the efficiency and effectiveness of the health care system, and protecting the security and privacy of electronically transmitted and maintained health information. The act mandates that HHS establish standards through the formal rule making process for:

- Security and electronic signatures,
- Electronic administrative and financial transaction,
- Code sets,
- Unique health identifiers, and
- Privacy and confidentiality of protected health information.

The proposed security regulation defines a set of requirements with implementation features that covered entities must include in their operations to assure that electronic health information pertaining to an individual remains secure. The security standard is to be comprehensive, be developed through consultation with standards development organizations, be technology-neutral, and be scalable. The law leaves the business decision of how and to what extent the security features would be implemented up to each organization. What this law establishes is a baseline of responsible security measures that will provide adequate protections for individually identifiable health information.

The security requirements proposed under HIPAA are broken down into administrative procedures, physical safeguards, technical security services, technical security mechanisms, and electronic signatures. The requirements are presented in Appendix A -- HIPAA Security Requirements.

### **AGENCY RESPONSIBILITY**

Each agency that maintains a system of records is required by the Privacy Act and by HIPAA to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records, and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Moreover, with the exception of permissible disclosures authorized under the Privacy Act, no agency shall disclose any record contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.

### **SECURITY RESPONSIBILITIES**

---

An effective security program is dependent upon supportive management and assignment of responsibilities to personnel throughout the organization for implementing and enforcing the various aspects of the security policy. This section describes the general responsibilities envisioned for some of the primary IHS employee roles to support an effective information security policy and security program for IHS. Detailed security responsibilities are spelled out in the IHS Security Policy.

#### **IHS CHIEF INFORMATION OFFICER (CIO)**

The Chief Information Officer (CIO) typically is responsible for the security of all information and information resources in their agency. The following responsibilities are envisioned for the CIO:

- Be responsible for the security of all IHS information while the information is being processed and/or transmitted electronically, and for the security of the resources associated with these functions.
- Monitor and report on the status of IT security within the IHS.
- Ensure the adequacy of operating unit IT Security programs.
- Review and approve system security policies.
- Act as the designated accreditation authority of all IHS national programs and national-level systems, and ensure that all certification requirements have been met for each system prior to accreditation.

- Ensure that an Information System Security Officer (ISSO) has been appointed for each area and a senior ISSO appointed for IHS.
- Coordinate with the Privacy Officer and Records Management Officer for interpretation of privacy and records management policies and ensure that these policies are being correctly implemented in IHS systems.

### **IHS AND AREA INFORMATION SYSTEM SECURITY OFFICERS (ISSO)**

Information Systems Security Officers (ISSO) are delegated the authority to perform information security responsibilities within their purview in the IHS. ISSOs typically monitor, evaluate, and report to the CIO on the status of IT security within the IHS and the adequacy of the IT security programs administered by the areas. Area ISSOs would be responsible for ensuring the security of their respective areas, while the IHS ISSO would coordinate between the area ISSOs to ensure a consistent level of security across IHS. The following responsibilities are envisioned for IHS and Area ISSOs:

- Develop policies, procedures, and guidance establishing, implementing, maintaining, and overseeing requirements for the IHS's IT security program to be followed by all IHS organizations.
- Ensure that IHS security plans are developed, reviewed, implemented, and revised.
- Report information resources security breaches in accordance with the security breach reporting procedures developed and implemented by the IHS.
- Provide guidance and technical assistance to operating units.
- Assure IHS IT security oversight.
- Maintain a tracking system and records concerning implementation of the required controls and accreditation status of all IHS IT systems.
- Coordinate with subordinate ISSOs.
- Coordinate the review of controls and evaluate the adequacy of technical controls for accreditation.
- Act as the central point of contact for the Agency for accreditations and for IT security related incidents or violations.

### **AREA DIRECTOR**

Each Area Director will be expected to conduct an IT security program that ensures appropriate and adequate levels of protection for all IT systems within the operating unit.

It is envisioned that the Area Director would:

- Appoint an Information Systems Coordinator (ISC).
- Ensure appropriate and adequate levels of protection based on the security level designations of the Automated Information Systems (AIS).
- Ensure that systems may only be run in a facility that has at least the same or a higher security level designation.

#### **AREA INFORMATION SYSTEMS COORDINATOR (ISC)**

The Area ISC shall:

- Be the designated accreditation authority for all sensitive systems within their area.
- Assure ownership is assigned for all IT resources within the Area (i.e., hardware, software, data, telecommunications, etc.).
- Appoint an Area Information System Security Officer (ISSO) and alternate for the Area. The Area ISSO and alternate should have the staff responsibility for the operating unit ITS security program.

#### **SUBORDINATE ISSO**

Not all operating units within the Areas will require a position at this level. A major subordinate organization is defined as “Any large organizational component that has management responsibility for a number of individual IT systems performing separate functions (i.e., hospital, service unit, Area Office)”. The Area Office ISSO shall serve as the central point of contact for the subordinate organization IT security program with the Area Office. If this level of position is determined to be appropriate for the Area Office, the functions of the ISSO for the subordinate organization generally parallel those specified for the Area ISSO. An ISSO can also be appointed for a single information system.

#### **SYSTEM OWNER/CUSTODIAN**

Responsibility for the protection of IT resources generally falls into two broad categories: custodial and owner. The following responsibilities are envisioned for system owners/custodians:

- All information resources (hardware, software, facilities, data and telecommunications) will be assigned to an owner.
- Each system owner would be expected to:
  - Determine the sensitivity of the resources for which the owner is responsible, based on Federal legislation and regulations.

- Determine the appropriate level of security required which is consistent with laws and the protection requirements of the system for confidentiality, integrity or availability.
- Be the certifying official and complete all required certification actions.
- Monitor compliance and periodically reevaluate previously specified levels of sensitivity and protection.
- Custodial responsibility includes: a) the obligation to comply with applicable security policies and directives. b) To administer application owner specified controls and safeguards for the owner's data and programs.

#### **RECORDS MANAGEMENT OFFICER**

Records Management Officers are responsible for providing consultation to Database Managers to ensure that records retention schedules are adopted in accordance with IHS guidance and that records disposal procedures are undertaken in accordance with the sensitivity of the data.

#### **PRIVACY ACT OFFICER/COORDINATOR**

The Privacy Act Officer is the principal authority on maintenance and release of Privacy Act protected data from the Privacy Act SOR. The Privacy Officer's responsibilities include:

- Interpreting Privacy Act and HIPAA requirements and rules.
  - Coordinating with all System Owners/Managers to ensure that they understand the Privacy Act and HIPAA requirements and their related responsibilities.
  - Reviewing requests and concurring with the need to establish a new Privacy Act SOR or to modify an existing Privacy Act SOR.
  - Assisting System Owners/Managers in preparing Privacy Act SORs in accordance with establish procedures.
  - Ensuring that SORs comply with the Privacy Act and HIPAA.

## **ENVIRONMENT AND CURRENT ARCHITECTURE**

### **INFORMATION USERS**

---

There are many different users of IHS information. A user can be an individual person, an organization, or a system. In general, the users of IHS information are health care providers (hospitals, physicians, and staff); contract organizations, such as Blue Cross Blue Shield organizations and commercial insurance carriers; third-party billers such as Envoy; patients, researchers, state and tribal organizations. Each user has unique access requirements and unique constraints and security requirements.

The users of IHS information have different access paths. Healthcare providers and health facilities access the information directly from the primary computer system at the facility. All other users access information that is extracted from the primary computer systems. The information flow of extracted data is illustrated in Exhibit A-1 of this document.

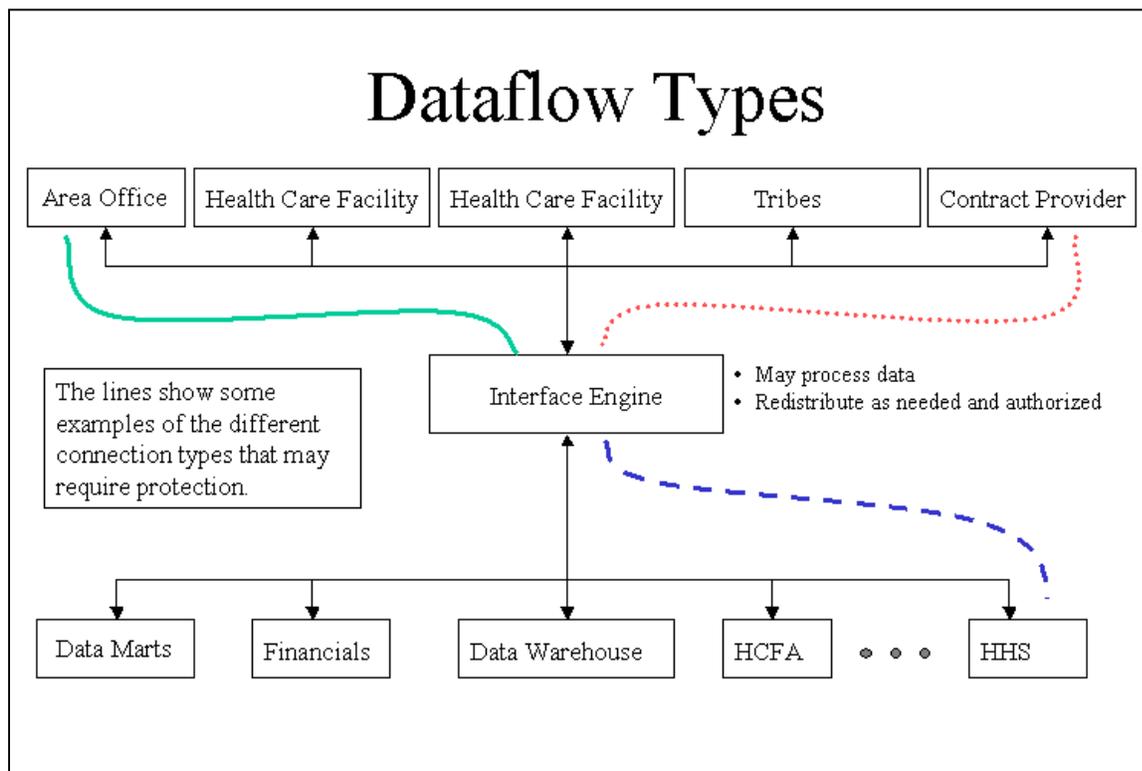
### Exhibit A-1 Data Flow Types

#### INFORMATION RESOURCES

IHS information is stored in many different and diverse locations: IHS data processing center, IHS headquarters, IHS Area Offices, and Healthcare Facilities around the country. The information housed in IHS ranges from very sensitive patient information through less sensitive day-to-day electronic messages. A break down of specific types of information and the associated security risks is presented in the next section.

#### RISKS AND THREATS

The Security Architecture design mitigates specific risks and threats to the IHS enterprise. Threats are identified by examining the limitations in the controls used by IHS that would adversely affect the ability of IHS to conduct business.



Examples of threats include virus attacks, malicious hacker attacks, unauthorized access by former employees or contractors, etc.

The various types of data dealt with by IHS and their associated levels of risk are detailed in Exhibit A-1. These data types are derived from the IHS Data

Transport Workgroup of the Data Management Committee. This group is helping IHS define the future for data movement within IHS.

<b>Data Type</b>	<b>Confidentiality</b> (Protection of data owned by the user)	<b>Integrity</b> (Accuracy)	<b>Availability</b>	<b>Privacy</b> (Protection of data owned by someone else)
Individually identifiable health information	<b>HIGH</b> Breach violates the law	<b>HIGH</b> Fatal consequences if data inaccurate. Faulty reporting violates the law.	<b>MEDIUM</b> Paper files are available. Access to this information impacts IHS critical business functions	<b>HIGH</b> Breach violates the law
Requests for information (Non-life threatening )	<b>MEDIUM</b> Request may not be confidential, but association of request with an individual is confidential.	<b>LOW</b> Lack of integrity results in re-submission of request or longer response time. Non-life threatening requests may be re-submitted without fatal consequences.	<b>LOW</b> Tracking requests for patient information is supports the maintenance of patient history.	<b>HIGH</b> Breach violates the law
Requests for information (Life threatening )	<b>MEDIUM</b> Request may not be confidential, but association of request with an individual is confidential.	<b>HIGH</b> Time to re-submit emergency requests may lead to fatal consequences	<b>HIGH</b> Tracking requests for patient information supports maintenance of patient history.	<b>HIGH</b> Breach violates the law
System status	<b>HIGH</b> Data pertaining to operations is considered sensitive	<b>HIGH</b> Needed to monitor the availability and accuracy of data	<b>MEDIUM</b> Needed to monitor the availability and accuracy of data	<b>LOW</b> Not applicable
Financials	<b>HIGH</b> Data pertaining to operations is considered sensitive	<b>HIGH</b> Accurate financials needed to properly run a business	<b>MEDIUM</b> Financials are not needed immediately to properly run a business	<b>LOW</b> Not applicable

			business	
Personnel Records	<b>MEDIUM</b> Individually identifiable	<b>MEDIUM</b> Can be modified or re-created with some effort.	<b>MEDIUM</b> Availability only on a need to know basis	<b>MEDIUM</b> Need to know only
Statistics	<b>LOW</b> No identification of individuals	<b>MEDIUM</b> May be used to assess operations, plan, and allocate funds.	<b>LOW</b> Not critical to operations	<b>LOW</b> No identification of individuals

**Ehibit A-1 Data Types and Level of Risk**

**SUMMARY OF CURRENT SECURITY ARCHITECTURE AND BUSINESS REQUIREMENTS**

---

The mission of IHS is to provide healthcare to American Indian and Alaska Native people. The IHS currently provides health services to approximately 1.5 million American Indians and Alaska Natives who belong to more than 550 federally recognized tribes in 35 states.

One result of providing healthcare is the production and storage of large amounts of sensitive patient information. Information is received, processed, retrieved, and stored on a large scale. IHS safeguards this information from corruption and misuse. The current security architecture protects data at the primary sources (the Healthcare Providers) and the data centers where data extracts are stored and processed. The target security architecture will layer additional defenses into the transportation and processing of information.

## **TARGET ARCHITECTURE**

This section provides a conceptual description of the target Security Architecture. The target IHS Security Architecture is defined within the context of six areas required by HIPAA. These areas include technical; physical; administrative and procedural protection; event logging and auditing; personnel training and awareness; and intrusion and incident response detection. The basic philosophy behind the IHS Security Architecture is to secure components and secure the data communications. The measures listed in the following section are designed to enhance the security of these components.

## **TECHNICAL PROTECTION MEASURES**

---

Technical protection measures are traditionally grouped into three high level categories: confidentiality, integrity, and availability. They are defined as follows:

- *Confidentiality* measures provide the mechanism to ensure that the privacy of information is maintained.
- *Integrity* measures enhance the reliability of information by guarding against unauthorized alteration.
- *Availability* measures seek to ensure that information assets are accessible to authorized internal and external users when needed.

The keystone of technical protection measures is the use of Public Key Infrastructure (PKI). PKI is a technique that enables users of a basically unsecured public network to exchange data securely and privately through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. This strong authentication mechanism, using certificates provided through the PKI process, is a mandatory prerequisite to both confidentiality and integrity.

### **PUBLIC KEY INFRASTRUCTURE (PKI)**

A PKI provides the ability to disseminate certificates with assurance that those certificates legitimately represent the identity of the private key owner. Encryption and signature are the two basic functions provided by PK technology. But these two basic functions support four security services: authentication, confidentiality, integrity, and non-repudiation. Encryption supports confidentiality, while digital signature provides the basis for the remaining three services. Assuming the private key owner controls the private key and ensures its secrecy, verification of a signed message using the public key contained in the certificate authenticates that the message was sent by the private key owner. The digital signature process has the additional advantage of also providing integrity and non-repudiation services. The comparison of an independently computed digest and the encrypted digest determines whether a

message has been altered. The association of the private key with its owner prevents the owner from denying that he or she was the originator of the message. The existence of a PKI makes all this possible.

The National Institute of Standards and Technology (NIST), on behalf of the Federal Government and working in conjunction with several agencies, is developing a PKI model to promote interoperability across government agencies. The model proposes four classes of PKIs known as Class 1 to Class 4. Each class provides different levels of assurance, with Class 1 providing the least assurance and Class 4 providing the greatest level of assurance. Class 3 is the generally accepted level for sensitive information, to include personal data subject to the Privacy Act. Class 3 imposes requirements on the measures that the Certification Authority (CA) uses to protect its private key, systems and related resources, and its operating environment. Class 3 also includes requirements for a registration process based on face-to-face identification between registration authorities and prospective subscribers.

The Federal Public Key Infrastructure Policy Authority (FPKIPA) sets policy governing operation of the Federal Bridge Certification Authority (FBCA), to provide a mechanism for agencies employing public key technology to interoperate efficiently. The FBCA allows an agency's PKI to trust digital certificates issued by other agency CAs.

It is expected that IHS will adopt policies compatible with the Federal PKI Policy that allow interaction with the Federal Bridge Certification Authority (FBCA) and that comply with the Federal Class 3 criteria to ensure interoperability with other PKIs serving other Government agencies. Initial security services that can be supported by a PKI for IHS include secure electronic mail, strong authentication, and PKI enabled software.

#### **VIRTUAL PRIVATE NETWORKS (VPN)**

A VPN provides an encrypted tunnel over an un-trusted network, such as the Internet. This allows an organization to use the bandwidth available on the Internet without requiring an expensive dedicated link. The VPN will protect communications between secured IHS components that do not communicate over IHSNET.

#### **CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY SERVICES**

Technical protection measures are traditionally grouped into three high level categories: confidentiality, integrity, and availability. *Confidentiality* measures include encryption mechanisms (e.g., VPN, end-to-end and link level encryption) to ensure that the privacy of information is maintained. *Integrity* measures enhance the reliability of information by guarding against unauthorized alteration. A key tool here is digital signature. The architecture will establish the goal of implementing digital signature technology both to

reduce reliance on “wet-signed” paper documents, and to enhance the integrity of IHS information assets. Strong authentication, using certificates provided through the IHS PKI pilot project, is a mandatory prerequisite to both confidentiality and integrity. *Availability* measures seek to ensure that information assets are accessible to internal and external users when needed, and to guard against “denial of service” attacks. Availability protection measures such as planned redundancy will be used to mitigate availability risks created by the potential for system component failures. Protection measures such as firewalls and router filters will be used to mitigate availability risks created by denial of service attacks.

There are ten basic security services:

- 1) Physical Security
- 2) Firewalls
- 3) Intrusion Detection
- 4) Access Control
- 5) Authentication
- 6) Privacy and Integrity (Encryption)
- 7) Electronic Signature/Non-repudiation
- 8) Virus Protection
- 9) Audit Trail Creation and Analysis
- 10) Database Security

These services are addressed from a technical perspective below and are summarized in Exhibit A-2.

<b>Basic Service Areas</b>	<b>As-Is Technical Measures</b>	<b>TO-BE Technical Measures</b>
Physical Security	Major Data Centers have security guards, user badges, and locked equipment rooms	Continued physical security; Integrated smart card access control
Firewalls	Cisco PIX firewalls	Use at Boundary Points
Intrusion Detection	Cisco Intrusion Detection using NetRanger on the main network	Automated monitoring of limited entry/exit points; Pro-active with integrated action plan
Access Control	User Identity based access control	Role Based Access Control
Authentication	Operating System logon Application logon	Private key-based with multi-factor identification
Privacy & Integrity (Encryption)	VPN (Manual key management)	PKI-based key mgmt; FIPS 140-1 approved encryption; SSL, VPN with key management
<b>ELECTRONIC SIGNATURE/NON-REPUDIATION</b>	None	FIPS 140-1 Digital Signature; Escrow for encryption keys (not signing keys)
Virus Prevention	Norton AntiVirus	Workstation and server-based program; signed application
Audit Trail Creation & Analysis	Audit trails are kept on key systems, but procedures for review are lacking	Consistent log content, directive data reduction and analysis
Database Security	RPMS access control NPIRS user access control	Secure communications to interface engine with PKI

**Exhibit A-2 Basic Security Services and Technical Measures**

Physical Security: The Target Architecture envisions physical security that incorporates access control to computer equipment rooms by using smart-cards or other strong authentication mechanisms.

Firewalls: Currently, IHS uses firewalls to establish a secure boundary between IHSNET and the public network. In the target architecture, IHS will use firewalls more extensively to establish internal security boundaries to separate networks operating at different levels of trust. Initially, each Area in IHS will be connected to the IHSNET using a firewall.

Intrusion Detection: Currently, intrusion detection is primarily a reactive function that responds as attacks are identified. Network-based intrusion detection is deployed on the primary server network. In the target architecture, IHS will use intrusion detection software to monitor

network and host-based assets and employ a computer emergency response team to report and respond when incidents occur.

Authentication and Access Control: Authentication and access control is based on the proprietary mechanisms that reside in IHS's distributed computing platforms (e.g., Windows NT and Unix). IHS currently employs user ID and password as the principal authentication technology. The target architecture employs strong authentication using PKI certificate in combination with token or biometric identification. IHS recognizes that a single mechanism will not be appropriate when implementing strong authentication in a diverse business and work environment. Nevertheless, IHS expects to set standards for the type of mechanism that can be used for authentication.

Privacy and Integrity (Encryption): Depending upon the risk of inappropriate disclosure and cost for information protection, IHS system designers, analysts, and managers will base their decision to encrypt and the encryption tactics on an application-by-application basis. In all cases, the exchange of authentication information and HIPAA/Privacy Act protected information will be encrypted when transmitted across untrusted channels. The target architecture requires that all keys used for encryption be managed under the IHS PKI. It also requires that encryption algorithms applied for the purposes of supporting privacy and integrity adhere to FIPS PUB 140-1 or the latest issue.

Virtual Private Networks (VPNs) and Secure Socket Layer (SSL) are two technologies that IHS will use to implement privacy and integrity. The target architecture will employ VPNs to establish secured sub-channels on an otherwise public, unsecured communications medium. The authentication and key exchange necessary to establish the secure sub-channels will be supported by the PKI. SSL is frequently used in electronic commerce to secure the communications path between a consumer and an e-merchant. The target architecture incorporates this well-proven protocol with some provisos. Namely, E-commerce's use of SSL typically does not include authentication of the client, and IHS will only use SSL in this manner when client authentication is not critical to the privacy and integrity of the transaction.

Electronic Signature/non-repudiation: Digital signature is an integrity function. To sign a document or other information resource digitally, the signatory encrypts a representation of the document with his/her private key. A PKI architecture is designed to help guarantee that only the signatory has knowledge of his/her private key. A Lightweight Directory

Access Protocol (LDAP) Directory will store the keys necessary to verify a digital signature, but only the signatory has knowledge of his/her private (signing) key. If the PKI is properly managed and the digital signature algorithm is strong, the signature cannot be repudiated; i.e. the signatory will not be able credibly to deny having digitally signed a document. The goal of the IHS security technology architecture is to ensure non-repudiated digital signatures. All IHS electronic signature algorithms will be FIPS 140-1 compliant.

Virus Protection: IHS has a policy in place to maintain virus detection and removal software on both servers and workstations. The target architecture maintains this program. In addition, the target includes digitally signed applications software executables to further reduce the threat of rogue software, Trojan horses, and viruses. [layered security... files on disk, entry (e.g. web, mail)]

Audit Trail Creation and Analysis: All IHS information systems will create audit logs following the guidance specified in section 4.4 of this document. The analysis should provide sufficient filtering facilities to reduce large volumes of log data to useful information. In addition, the analysis should allow auditing and logging to be varied in intensity in response to ambient security threat conditions and targeted analysis.

Database Security:

The patient care data is protected at each location using logical access controls. Authorized users are provided log on access to specific menus. The data warehouse is protected in the same manner.

#### **STANDARDS**

There is a hierarchy of standards, ranging from most general to most specific, to which all systems under the target Security Architecture must adhere. In general, IHS will base the target Security Architecture technical measures on FIPS PUB 140-1 standards to the greatest practical extent. The keys standards in this area are X.500 directories; X.509 certificates; RSA, DSA, and ECDSA for public key cryptography; and DES and Triple DES (soon to be replaced by AES) for symmetric (i.e., secret key) encryption.

### **PHYSICAL PROTECTION, CONTINGENCY PLANNING, AND DISASTER RECOVERY**

---

Each IHS information asset should have plans for physical protection and a disaster recovery plan. Preparation of these plans is the responsibility of the manager of the asset. This section summarizes some of the issues that should be addressed when dealing with physical access, environmental issues, contingency planning, and disaster recovery. It is not the intent of this document to include a Physical Security Plan. The following section delineates some elements that should be addressed by the Physical Security Plan.

## **PHYSICAL PROTECTION**

IHS will have a documented plan for the physical control of information assets. The plan will include NPIRS, assets located within IHS office space, and removable assets, (e.g., laptops and documents).

The physical protection plan should address such issues as:

- Physical access control including emergency egress.
- Visitor control.
- Temperature and humidity monitoring and control.
- Protection from loss of power, including the availability of an uninterruptible power supply (UPS) and emergency lighting.
- Automatic smoke and heat detectors, and a fire fighting policy.
- Protection from water damage.

## **BUSINESS CONTINUITY AND CONTINGENCY PLANNING (BCCP)**

Every effort must be made to avoid disruption of critical applications processed by automated data files and AIS facilities. IHS must also be able to minimize, and be prepared to recover from, any disruption that does occur. A BCCP must be prepared in writing for all IHS systems and databases, including those provided by contractors that fulfill mission critical business functions, whether they are a facility, network, major application, or stand-alone workstation. BCCP's are documented as part of the organization's overall AIS Security Program.

Managers of IHS's critical information assets must identify the potential consequences of undesirable events and the safeguards needed to counteract their effects. Safeguards included in the BCCP must be selected based on whether they are needed to maintain a minimum level of operation for the affected systems.

Backup and recovery procedures should be prepared for each information system, addressing frequency, testing, and storage of backups.

## **ADMINISTRATIVE SECURITY, PERSONNEL SECURITY, AND PROCEDURES**

---

Administrative processes must support good security practices and integrate with the architecture. IHS will develop and document administrative security procedures to address:

- A virus protection strategy that addresses prevention, detection, containment, elimination, and recovery from virus contaminations.
- Procedures for software development and maintenance, including emergency maintenance, that includes sufficient version control and

authorization of updates to ensure that only management-approved changes are placed into the production environment.

- Role-based access controls and management policy that define individual or group role definitions within domains. Inclusion within the role defines which users are authorized to access which asset and in what capacity.
- Background checks and clearance processes as they apply to Government employees, contractors, and trading partners who would have permission to access sensitive information or physical assets.
- Segregation of duties within the entire security management process.
- A process to ensure that responses to security incidents reported by IHS users are well documented and available for review.

Security plans should be developed for all new and existing applications that are in compliance with the following documents:

- National Institute of Standards & Technology (NIST) Special Publication 800-18 “Guide for Developing Security Plans for Information Technology Systems”.
- OMB Circular A-130, “Management of Federal Information Resources”, Appendix III.
- Public Law 100-235, “Computer Security Act of 1987”.
- Federal Information System Controls Audit Manual.
- HIPAA Security Standards

## **LOGGING AND AUDITING**

---

Security should be proactive. A number of proactive actions should be part of the security plan for each information system. In the areas of logging, auditing, and intrusion protection, security plans should attend to:

- Layered defense. These mechanisms serve to measure security performance, and may serve as indicators that additional protections are needed.
- Auditing of all accesses to sensitive/critical information assets. The ability to monitor for potential security incidents will be limited to a small staff in support of IHS’s separation of duty policy.
- Role-based control of all execution of programs that grant a higher level of access than is normally available to a user, whether directly or indirectly.
- Audit logs that record, in a centralized repository, logon and logoff; instances where a role is authorized access or denied access; the individual acting in that role; the sensitivity level of the data or other asset accessed; what type of access was performed or attempted (e.g.,

whether the nature of the requested action was to create, read, update, execute a program, or delete); and where appropriate what specific fields or finely granular data type name and description the access attempt involved.

- For programs that are not operating directly on behalf of a user, audit logs should record the date and time of each event's occurrence, and a unique program identifier of each program, and either the logical or physical location of the event.
- Computer systems employed in the logging function that safeguard their programming code from unauthorized modification.
- Auditing and monitoring reporting processes should provide useful data for decision makers, not just reams of detailed data that need further processing to be made meaningful.
- Independent reviewers to perform monitoring of the sufficiency of documented controls and the extent of compliance with stated physical access controls and environmental controls, security audit trail logging, and intrusion detection procedures.
- Recording all actions performed by the emergency maintenance accounts in the audit log.
- Retention period of logs.
- Semi-autonomous software agents to detect intrusion attempts regarding networks and systems, and take mitigating action, react and adapt without supervision. The software agents could be empowered to turn off services, close ports, adjust firewalls, replace agents with fresh agents, use alternate means of communication, or send out probes to locate and assess the attacker.

## **TRAINING AND AWARENESS**

---

Many of the classic attacks on information systems start with "social engineering". Social engineering is a euphemism that recognizes those individuals, or more specifically, the poor security practices of individuals, that are frequently the weakest link in the security assurance chain. The IHS security training and awareness program should seek to strengthen this link by both informing users of the proper use of security mechanisms, and by increasing understanding of the threats to business assets and the ways to mitigate the risks.

IHS should develop a comprehensive IT Security Training and Awareness Plan. Because administrative procedures are crucial to all of the other protection measures, training should be tailored to all levels of the user community. The training can be computer-based or tele-learning, to afford the maximum opportunity to participate regardless of geographic location. Participation in

and successful completion of training, and the actual retention of the content, should be measured and monitored to ensure compliance.

IHS security training can have a tiered structure consisting of pre-packaged training programs and customized IHS security training. All personnel should be trained appropriately regarding their roles in IHS security policy. Security awareness training should include both general and role-specific training. New employees and contractors should receive security training as part of their new hire processing. Refresher training should be provided to all IHS and contractor staff annually.

## **INCIDENT DETECTION AND RESPONSE CAPABILITY**

---

It is both theoretically and practically impossible to devise a flawless Security Architecture. Therefore, an incident detection and response capability is a critical part of maintaining a high level of information assurance and asset protection. Computer systems and communication networks are subject to a variety of sophisticated threats, many of which have emerged only during the past decade with the enormous growth in the use of computer workstations, local area networks (LANs), and the Internet. Although prevention must be the main line of defense, when a systems security incident occurs there should be on-call experts who can quickly control and contain sophisticated intrusions, limit damage, eliminate the problem, and restore normal operations.

Intrusion detection consists of the real-time identification of unauthorized use, misuse, and abuse of computer assets by both internal network users and external hackers. Intrusion detection is a challenging task because of the proliferation of network connectivity, heterogeneous computer environments, mixed operating systems, various communication protocols and a significant assortment of popular and proprietary applications.

Incident detection should be accomplished in the target architecture with the use of both network and host-based automated detection software tools. Network intrusion detection utilizes traffic analysis to compare session data against a known database of popular operating system and application attack signatures.

Host-based detection analyzes operating system and application system logs and events to compare system events against a database of known security violations and custom policies. Both detection methods react by logging files or sessions, alerting the administrator, possible termination of the session/activity, and allow for hardening of a firewall. The combination of network and host-based intrusion detection software provides significant attack protection and policy enforcement.

Intrusion response consists of the real-time decisions and actions taken to minimize incident-related effects on the activity's assets and to mitigate residual security risk based on available evidence from the incident. An IHS Computer Emergency Response Team (CERT) should be chartered by the CIO to be responsible for real-time detection of and response to potential security incidents. The CERT responsibilities should be restricted to a dedicated staff in support of IHS's separation of duty policy.

The CERT should be:

- Continually aware of pending virus threats and be prepared with countermeasures;
- Proactive in identifying potential intrusions and ready to counter threats to information assets;
- Responsible for communicating existing threats and response procedures to users and managers throughout the enterprise;
- Responsible for Department of Health and Human Services reporting requirements; and
- The coordination point for incident responses that require participation of organizations scattered throughout IHS to respond effectively.

## **ARCHITECTURE MAINTENANCE AND COMPLIANCE**

Procedures for maintaining and enforcing the IHS IT Security Architecture should be developed that detail how maintenance and governance are integrated into the EA process and should discuss some of the features unique to IT security. The IT Architecture management and governance process is particularly important for security because security is best when designed into system, rather than being retrofitted, as described in the basic security design principles presented previously in this document (IHS Information Security Principle #7). A documented process is also necessary to maintain pace with the rapidly developing security technology and threat environment.

## **ARCHITECTURE MANAGEMENT**

The stimulus for changes to the Security Architecture may arise from four sources: 1) a new information system is upgraded or developed; 2) a change in regulation occurs; 3) a change in technology occurs; or 4) a new threat arises. The ITA Security Architecture Committee [Currently there is no such group in IHS] is a critical component in maintaining the architecture.

A Security Architecture Committee should track environmental changes to determine when it is necessary to submit a Security Architecture change proposal and evaluate and facilitate change requests that are sourced from other parts of the IHS community. New policies, once appropriately approved, will become part of the Security Architecture of the ITA.

Exhibit A-3 identifies some of the emerging technologies and standards that will be candidates for incorporation into the Security Architecture in the near future.

<b>Emerging Technology</b>	<b>Description</b>	<b>Importance to IHS Security Architecture</b>	<b>Projected Timeframe for Emergence</b>
IP Version 6	The update to the current Internet Protocol (IP version 4).	Offers link level integrity and privacy.  Key to VPNs and prevention of spoofing attacks.  Currently not in wide use.	5 years for full availability
Common Criteria	An international scale for ranking the assurance level of an information system.	Provides a measure of system assurance level.  Not widely implemented and few evaluation labs.	2 years
FIPS 140-2	Update of the current standard (includes lists of encryption).	A draft on the verge of approval.	1 year
AES	The replacement for DES as the national standard symmetric key encryption algorithm.	Replacement for DES – Rijndael algorithm selected October 2000.	5+ years for full adoption.
Public Key Enabled Kerberos	Non-proprietary protocol for secure, single sign-on network authentication.	Mature (in secret key implementation) open sources protocol.  Native network authentication for Windows 2000.	2 to 3 years for public enabled Kerberos variant.

**Exhibit A-3 Emerging Technologies – Candidates for Inclusion in IHS Security Architecture**

**ARCHITECTURE COMPLIANCE**

---

Compliance with Security Architecture should be embedded in the IT investment review process and the System Development Processes. IHS will use investment review and a proactive implementation program to evolve from the current to the target Security Architecture.

**SUMMARY**

[TBD]

**SOURCES**

[TBD]

## **HIPAA SECURITY SERVICES**

### **HIPAA SECURITY REQUIREMENTS**

---

HIPAA security requirements were established for healthcare organizations to safeguard the integrity, confidentiality, and availability of its electronic data. The four major service areas required by HIPAA are described below. In each section, a list of services that are expected or required is specified.

#### **1. ADMINISTRATIVE PROCEDURES**

---

Administrative procedures are put in place to guard data integrity, confidentiality, and availability – these are documented, formal practices to manage the selection and execution of security measures to protect data and the conduct of personnel in relation to the protection of data.

- Certification of computer systems is a detailed process used to assure that the security requirements of a computer system are properly implemented.
- Chain of trust agreements are common in complex computing environments. As part of the certification process, all service level agreements and information processing agreements between organizations must be examined to determine if the contractual agreements properly address the security requirements of the computer systems and business operations.
- Contingency plans are required of all systems processing sensitive information and necessary for any system that is critical to the operations of an organization. These plans should be detailed enough to permit an organization to smoothly transition from normal operations into an emergency situation without compromising the security of the computer systems or organization.
- Formal mechanisms for processing records are required to assert that a system meets its security requirements. Details should include both the routine and non-routine aspects of record handling including transmission, dissemination and disposal of this information.
- Information access control is the basic mechanism used to limit access to sensitive information. Access control must support the security requirements of the computer systems and must be covered in the policies and procedures of an organization.
- Internal audit should be an ongoing process used by an organization to determine the security posture of the organization or the

- compliance of the organization or computer system with its requirements.
- Personnel security is a basic component of access control. Personnel security is important to ensure that authorized personnel have access to information and to prevent unnecessary or inadvertent access to sensitive information.
  - Configuration management is an important key to controlling critical assets of computer systems. Configuration management provides the means to monitor and control both the software and hardware configurations of important information systems.
  - Security incident procedures are used to report security violations and breaches and conduct forensics analysis of the events. The procedures include instructions for reporting events as well as instructions on responding to events.
  - Security management process is a formal process to handle the maintenance of the policies and processes of security. Security management processes must address risk analysis, risk management, security policy and sanctions.
  - Termination procedures are closely tied to personnel security in that they specify the actions that must be taken when a user's access is terminated. These procedures also include actions that must be taken when the access rights of a user change, for example, when the user is assigned to a different job function.
  - Training is key to protecting computer systems. Training should be focused on the information in the user's possession and the procedures that must be followed to protect the confidentiality and integrity of that information.

## **2. PHYSICAL SAFEGUARDS**

---

Physical safeguards describe security measures used to guard data integrity, confidentiality, and availability – these relate to the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Physical safeguards also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

- Roles and responsibilities are required of all security programs. The roles and responsibilities should be tied to the security policy and they assign specific security duties to individuals.
- Media controls are a part of the configuration management processes used to control the insertion and removal of hardware and software.

Media control must address all of the basic security components used for access to information, namely, access control, accountability, backup, storage, and disposal.

- Physical access controls include a wide range of controls to regulate access to the physical space where a computer system resides or where a computer system may be accessed. These controls should include disaster recovery and emergency modes of operation. In addition, physical access control can be used to supplement identification and authorization procedures.
- Securing access to computer systems and workstations is another aspect of physical access controls. The controls should specifically address physical safeguards used to protect workstations and prevent unauthorized access to information.
- Security awareness training is important to protecting the overall security of the environment. Users are the first line of defense against attack. Increasing their awareness of security issues will improve the organization's ability to quickly detect attacks and violations in the early stages when the damage can most likely be mitigated.

### **3. TECHNICAL SECURITY SERVICES**

---

Technical security services refer to those services used to guard data integrity, confidentiality, and availability – these include the processes that are put in place to protect, control and monitor information access.

- Access controls as a technical service are designed to implement the access control policy and procedures. Access controls specify the mechanisms used to limit access to information to authorized personnel.
- Audit controls as a technical service are designed to provide a manner to record and examine system activities and access to information. These audit trails are important to diagnosis and tracing security problems.
- Authorization controls are the mechanisms use to obtain consent and ensure that information is only accessible to authorized individuals.
- Data authentication and integrity is the process that ensures the data has not been altered or destroyed in an unauthorized manner. Mechanisms to support data authentication include checksums and digital signatures.
- Entity authentication is the process of irrefutably identifying authorized users, programs, and processes and denying access to unauthorized users, programs, and processes

#### **4. TECHNICAL SECURITY MECHANISMS**

---

Technical security mechanisms include the processes that are put in place to prevent unauthorized access to data that is transmitted over a communications network.

- Communications and network controls are a general category of controls used to protect the communications as they are transmitted across networks (wireless, wire, or fiber).
- Digital signatures are used in the identification and authentication of individuals and entities.

#### **HIPAA ELECTRONIC SIGNATURE REQUIREMENTS**

---

Various technologies may fulfill one or more of the requirements for electronic signatures. If electronic signatures would be used, certain implementation features must be included, specifically:

- Message integrity
- Non-repudiation
- User authentication

## APPENDIX B - GLOSSARY OF TERMS

### A

**ACCESS:** (1) The ability of a subject to view, change, or communicate with an object in a computer system. Typically, access involves information between the subject and the object (for example, a user reads a file, a program creates a directory). [O'Reilly, 1992] (2) The provision of an opportunity to approach, inspect, review, and use data or information. Refers to such actions by the individual receiving health care, health care services providers, and any other individual or entity who has appropriate authorization for such actions. [CPRI, 1995b]

**ACCESS CONTROL:** (1) Preventing unauthorized use of a resource. [ISO 7498-2] (2) Information use policy to determine who can have access to what data/information (both within and external to the organization adopting the access control policy); policies and procedures preventing access by those who are not authorized to have it. [Institute of Medicine, 1994].

**ACCESS CONTROL LIST:** A list of entities, together with their access rights, which are authorized to access a resource. [CORBA Security Services, 1997]

**ACCOUNTABILITY:** (1) The property that ensures that an entity's actions can be traced. [ISO 7498 - 2] (2) The concept that individual persons or entities can be held responsible for specified actions, such as obtaining informed consent or breaching confidentiality [National Research Council, 1991]

**ADMINISTRATIVE DATA/INFORMATION:** Data/information collected during the course of a health care event unrelated to the status of the individual's health or health care. Includes demographics, provider identification, caregiver identification, date and time of care, and other such data providing the who, what, when, and where of data capture. [CPRI, 1995a]

**AMERICAN NATIONAL STANDARDS INSTITUTE (ANSI):** ANSI is a privately funded, non-profit organization that coordinates developing voluntary standards in the United States and approves standards (as American National Standards). It coordinates and manages U.S. participation in several non-governmental international standards organizations' work, including ISO.

**AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE (ASCII):** A widely used system to encode characters for processing and transmission between data processing systems, data communication systems, and associated equipment.

**APPLICATIONS:** The computer programs and systems that allow people to interface with the computer and programs that collect, manipulate, summarize, and report data and information.

**ARCHITECTURE:** The style or method of design and construction that comprises the elements of an information system and defines the purpose and interrelationships of those elements.

**ASSURANCE:** (1) A measure of confidence that a system's security features have been implemented and work properly. [O'Reilly] (2) Justified confidence in a system's security. (3) Development, documentation, testing, procedural, and operational activities carried out to ensure that a system's security services provide the claimed protection level. [CORBA Security Services, 1997]

**ASYMMETRIC ENCRYPTION:** A form of crypto system in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public-key encryption. [Stallings]

**ASYNCH:** Asynchronous; without regular time relationship; unexpected or unpredictable with respect to executing a program's instructions; a physical data transfer to or from a device that occurs without a regular or predictable time relationship.

**ASYNCHRONOUS TRANSFER MODE (ATM):** A high-speed connection-oriented data transmission method that provides bandwidth on demand through packet-switching techniques using fixed-sized cells. ATM supports both time-sensitive and time-insensitive traffic, and is defined in CCITT standards as the transport method for B-ISDN services. Cell-switching technology that operates at high data rates: up to 622 MBPS currently, but potential data rates could reach GB. ATM runs on an optical fiber network that uses Synchronous Optical Network (SONET) protocols for moving data between ATM switches.

**ATTACK:** (1) The act of aggressively trying to bypass security controls. The fact that an attack is made does not mean it will succeed. The degree of success depends on the system's vulnerability and the effectiveness of existing countermeasures. [Fites and Kratz, 1993] (2) An attempt to bypass a system's security controls. An active attack alters data. A passive attack releases data.

**AUDIT:** To record independently and later examine system activity, such as logins/logouts, file accesses, security violations). See security audit. [O'Reilly, 1992]

**AUDIT EVENT:** The data collected about a system event to include in the system audit log. [CORBA Security Services, 1997]

**AUDIT TRAIL:** (1) Data collected and potentially used to facilitate a security audit. [ISO 7498-2] (2) The chronological set of records that provides evidence of system activity. These records can be used to reconstruct, review, and examine transactions from inception to output of final results. The records can also be used to track system use and detect and identify intruders. [O'Reilly, 1992] (3) Documentary evidence of monitoring each operation of individuals on health information. [National Research Council, 1991] (4) Audit trails may be comprehensive or specific to the individual and information. For example, an audit trail may be a record of all actions taken by anyone on a particularly sensitive file. [OTA, 1993]

**AUTHENTICATION:** (1) The process of verifying the identity of an end user or process. Authentication may be accomplished using various methods, such as user ID and password, digital signature, or biometrics devices. (2) The corroboration that an entity is the one claimed. [ISO 7498 - 2] (3) The process of proving that a subject, a user or a system, is what the subject claims to be. Authentication is a measure used to verify the subject's eligibility and ability to access information. It protects against using a system fraudulently or fraudulent information transmission. There are three classic ways to authenticate oneself: (1) something you know, (2) something you have, and (3) something you are. [O'Reilly, 1992] (4) Providing assurance regarding the identity of subject (author) or object (information). [ASTM 1762] (5) Authentication of data origin is corroboration that the data source is received as is claimed [ASTM E1762] (6) User authentication is providing assurance of the claimed identity of an individual or entity [ASTM E1762].

**AUTHENTICITY:** A security principle that ensures that a message is received in exactly the form in which it was sent. See also message authentication and message authentication code. [O'Reilly, 1992]

**AUTHORIZE:** Granting rights, which includes granting access based on access rights. [ISO 7498-2]

**AUTHORIZATION:** (1) The process of determining whether the end user's use of resources is permitted and of granting appropriate systems, network, or resource access. Authorization prevents unauthorized access and deters

attempts to gain access. (2) The granting of rights, which includes the granting of access based on access rights. [ISO 7498 - 2]

**AUTHORIZED DISCLOSURE:** The release of personally identifiable information to a third party upon authorization. [Abdelhak, 1996]

**AVAILABILITY:** (1) The property of being accessible and useable upon demand by an authorized entity. [ISO 7498 - 2] (2) The probability that system functional capabilities are ready for use by a user at any time, where all time is considered, including operations, repair, administration, and logistic time. Availability is further defined by system category for both routine and priority operations.

## *B*

---

**BACKBONE:** A central high-speed network that connects smaller, lower speed, independent networks. The NSFnet is an example.

**BACK-END DATABASE:** An application running on a server that stores data and responds to requests for those data from front-end applications running on workstations and networked PCs. (See CLIENT/SERVER and FRONT-END DATABASE).

**BANDWIDTH:** The frequency range an information-bearing signal occupies or that a transmission medium can accommodate.

**BATCH:** Form of processing whereby input of a type is kept together and then processed at one time, generally considered an older style of processing but still necessary for some applications.

**BINARY:** Having two components or possible states; usually represented by a code of zeros and ones.

**BIT:** The smallest information unit in a computer, equivalent to a single zero or one. The word "bit" is a contraction of binary digit.

**BITS PER SECOND (BPS):** Communications speed, the rate at which data travels from one site to another. (Example: 56 Kilo BPS.)

**BRIDGE:** A device that interconnects LANs using the bottom two OSI layers.

**BROWSER:** WWW client program designed to navigate or browse the Internet. They are generally formatted, include graphics, and feature hyperlinks.

**BYTE:** A sequence of bits, usually eight, treated as a unit for computation, typically an alpha or numeric character.

## C

---

**C:** A general purpose, small, and concise programming language developed at Bell Laboratories in conjunction with the UNIX operating system.

**CACHE:** CACHE memory is a small area of very fast RAM used to speed data exchange. Also, a file or directory included on your computer's hard drive that automatically stores the text and graphics from a web page you pull up, which, in turn, allows you to go back to that web page, without having to wait for the information to reload.

**CENTRAL PROCESSING UNIT (CPU):** The part of a computer, composed of an arithmetic logic unit, a control unit, and a small amount of memory that interprets and executes instructions. (*See MAINFRAME COMPUTER*)

**CERTIFICATION:** (1) The technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. [O'Reilly, 1992] (2) The administrative act of approving a system for use in a particular application. [National Research Council, 1991]

**CERTIFICATION AUTHORITY:** (1) A party trusted to vouch for the binding between names or identities and public keys. In some systems, certification authorities generate public keys. [CORBA Security Services, 1997] (2) A trusted issuer of certification. [National Research Council, 1991]

**CLIENT:** A computer that is seeking data from another computer-the server.

**CLIENT/SERVER:** A distributed computing system in which the client is the requesting program, sending requests to servers across a network, and the server provides a service in response to clients' requests that allows access to the files and databases on the server computer.

**CLINICAL DATA/INFORMATION:** Data/information related to an individual's health and health care collected from or about an individual receiving health care services, including a caregiver's objective measurement or subjective evaluation of a patient's physical or mental state; descriptions of an individual's health history and family health history; diagnostic studies; decision rationale; descriptions of procedures performed; findings; therapeutic interventions; medications prescribed; description of responses to treatment;

prognostic statements; and descriptions of socio-economic and environmental factors related to the patient's health. [CPRI, 1996b; ASTM 1769]

**CLINICAL DATA REPOSITORY:** A repository of clinical information normally residing on one or more independent platforms for use by clinicians and other personnel to support patient-centric care. The data is retrieved from heritage, transaction-oriented systems and is organized in a format to support clinical decision-making that supports patient care.

**COAXIAL CABLE:** A transmission medium composed of an insulated copper wire inside a tubular conductor.

**COMMERCIAL OFF-THE-SHELF (COTS):** Refers to an item of hardware or software a contractor produced and is available for general purchase. Such items are at the unit level or higher. Such items must have been sold and delivered to government or commercial customers, must have passed customer's acceptance testing, be operating under customer's control, and within the user environment. Such items must have meaningful reliability, maintainability, and logistics historical data.

**COMMON BUSINESS-ORIENTED COMPUTER LANGUAGE (COBOL):** A third-generation (3GL) programming language.

**COMMON OBJECT REQUEST BROKER ARCHITECTURE (CORBA):** CORBA allows applications to communicate with one another no matter where they are located or who has designed them. CORBA version 1.1 was introduced in 1991 by Object Management Group (OMG) and defined the Interface Definition Language (IDL) and the Application Programming Interfaces (API) that enable client/server object interaction within a specific implementation of an ORB. CORBA 2.0, adopted in December of 1994, defines true interoperability by specifying how ORBs from different vendors can interoperate. The ORB is the Middleware that establishes the client-server relationships between objects. Using an ORB, a client can transparently invoke a method on a server object, which can be on the same machine or across a network. The ORB intercepts the call and is responsible for finding an object that can implement the request, pass it the parameters, invoke its method, and return the results. The client does not have to be aware of where the object is located, its programming language, its operating system, or any other system aspects that are not part of an object's interface. In so doing, the ORB provides interoperability between applications on different machines in heterogeneous distributed environments and seamlessly interconnects multiple object systems.

**COMMUNICATION PROTOCOL (CP):** A set of rules governing the exchange of information between devices on a data link.

**COMPACT DISC-READ ONLY MEMORY (CD-ROM):** Read only direct access mass storage medium. One of a variety of laser optical disc storage formats for computer programs, sound, still images, text, and/or video.

**COMPATIBILITY:** The ability of two or more systems or components to perform a set of required functions while sharing the same hardware or software environment.

**COMPUTER-AIDED DESIGN (CAD):** The application of **IT** to elements of the design process for manufactured, assembled, and constructed products. It usually covers both drafting applications and modeling.

**COMPUTER-BASED PATIENT RECORD SYSTEM:** The people, data, rules and procedures, processing and storage devices, and communication and support facilities that provide the capture, storage, processing, communication, security, and presentation of computer-based patient record information. [CPRI, 1995a]

**CONFIDENTIALITY:** (1) A condition in which information is shared or released in a controlled manner. [National Research Council, 1997] (2) The property that information is not made available or disclosed to unauthorized individuals, entities or processes. [ISO 7498 - 2] (3) A security principle that keeps information from being disclosed to any one not authorized access. [O'Reilly] (3) The act of limiting disclosure of private matters maintaining the trust that an individual has placed in entrusted with private matters. [CPRI, 1995b] (4) The status accorded to data or information indicating that it is sensitive and, therefore, needs to be protected against theft or improper use and must be disseminated to authorized individuals or organizations only. [Ball and Collen, 1992; OTA, 1993]

**CONFIGURATION MANAGEMENT (CM):** A discipline applying technical and administrative direction and surveillance to: (a) identify and document a configuration item's functional and physical characteristics (b) control changes to those characteristics and, (c) record and report changes to processing and implementation status.

**CONNECTIVITY:** The potential of a computer-based patient record system to establish links to or interact effectively with another computer system. [Institute of Medicine, 1994]

**CONSULTATIVE COMMITTEE FOR INTERNATIONAL TELEPHONE AND TELEGRAPHY (CCITT):** An international committee that specifies international communication standards.

**CONTINGENCY PLAN:** A plan to respond to a system emergency, including performing backups, preparing critical facilities that can be used to facilitate continuity of operations in an emergency, and recovering from a disaster. Synonymous with Disaster Recovery Plan. [O'Reilly, 1992]

**CREDENTIALS:** Information describing a user's or other principal's security attributes (identity and privileges). Access control uses credentials that are claimed through authentication or delegation. [CORBA Security Services, 1997]

**CRYPTANALYSIS:** The branch of cryptology dealing with breaking a cipher to recover information or forging encrypted information that will be accepted as authentic. [Stallings, 1995]

**CRYPTOGRAPHY:** (1) The branch of cryptology dealing with designing algorithms for encryption and decryption, intended to ensure message secrecy and authenticity. [Stallings, 1995] (2) The study of encryption and decryption. From the Greek "kryptos" meaning "hidden" and "graphia" meaning "writing". [O'Reilly, 1992] (3) The art of keeping data secret, primarily by using mathematical or logical functions that transform intelligible data into seemingly unintelligible data and back again. [National Research Council, 1991]

**CURRENT PROCEDURAL TERMINOLOGY (CPT):** CPT is a coding system primarily used to encode outpatient procedures for billing and reimbursement purposes. The American Medical Association in 1966 developed the CPT coding system. Each year, an annual publication is prepared, that makes changes corresponding with significant updates in medical technology and practice.

## *D*

---

**DATA:** A sequence of symbols to which meaning may be assigned. [National Research Council, 1991]

**DATABASE:** A collection of related information about a subject organized in a useful manner that provides a base or foundation for procedures, such as retrieving information, drawing conclusions, and making decisions.

**DATABASE MANAGEMENT SYSTEM (DBMS):** A system to store, retrieve, and manipulate data in an organized, modeled fashion, usually consisting of dictionary, manipulation, security, and access components.

**DATA DICTIONARY (DD):** An data information repository, such as its meaning, relationships to other data, origin, usage, and format that helps management, database administrators, systems analysts, and application programmers plan, control, and evaluate collecting, storing, and using data.

**DATA ENCRYPTION STANDARD (DES):** (1) The National Institute of Standards and Technology (NIST) Data Encryption Standard, which the U.S. government adopted as Federal Information Processing Standard (FIPS) Publication 46, which allows only hardware implementations of the U.S. Government official data encryption algorithm. (2) A private key encryption algorithm adopted as the federal standard to protect sensitive unclassified information and used extensively to protect commercial data. [O'Reilly, 1992]

**DATA/INFORMATION SECURITY:** (1) The result of effective protection measures that safeguard data/information from undesired occurrences and exposure to accidental or intentional disclosure to unauthorized persons, accidental or malicious alteration, unauthorized copying, loss by theft and destruction by hardware failures, software deficiencies, operating mistakes, or physical damage by fire, water, smoke, excessive temperature, electrical failure, or sabotage. [Institute of Medicine, 1994] (2) Protecting the integrity, availability, and confidentiality of computer-based information and resources used to enter, store, process, and communicate it. [NIST, 1994]

**DATA INTEGRITY:** (1) The property that unauthorized users have not undetectably altered or destroyed data in an unauthorized manner. [CORBA Security Services, 1997] (2) A process to ensure that data are not destroyed or modified. Also, the formal definition of comprehensive rules, and the consistent application of those rules, to assure high integrity data. It consists of techniques to determine how well data are maintained in the data resource and to ensure that the data resource contains data that have high integrity. Data integrity includes techniques for data value integrity, data structure integrity, data retention integrity, and data derivation integrity.

**DATA MART:** (1) A data mart is a subject-specific data warehouse that provides information specific to an individual department or business area, such as radiology. Each data mart has its own data, infrastructure, and format and may be populated from data in the corporate data warehouse. (2) A database that is read only, except for new record creation. It contains specialized views, typically business process centric, typically by recent quarter or fiscal year. It is frequently used for business decision support and

third-party report generation and focuses on solving a specific business problem in a single department or subject area.

**DATA MINING:** A process that uses a variety of data analyses tools to discover data patterns and relationship. A data relationships model is produced that may be based on decision trees, statistics, artificial intelligence, such as neural nets. Data mining emphasizes exploratory analysis rather than confirmatory analysis. In confirmatory analysis, the user has a hypothesis and either confirms or refutes it. In exploratory analysis, the user finds suitable hypotheses to confirm or refute. Data mining tools, not the user, take the initiative in data analysis. This contrasts with OLAP tools, which are user driven. Another characteristic of data mining tools is their ability to analyze large data amounts, making them favorable tools for fully exploiting operational data sets and data warehouses. To that end, data preparation is key.

**DATA MODEL:** A representation, often expressed graphically, of data elements and their relationships. A data model can be logical or physical. A logical data model represents the classes of data elements, such as a patient, their attributes, such as patient name, and their relationships to one another. Logical data models are usually developed during the database design process to represent data requirements and as an implementation-independent design. A physical data model describes the structural properties that define all entries represented in a database and all the relationships existing among them. Physical models strive to implement logical models based on the target database management system and on the intended use of the data.

**DATA MODELING:** A structured method to represent and describe the data used in a business function automated system. Its primary function is to define the attributes of and relationships among data items.

**DATA REGISTRY:** A place to keep data characteristics facts, such as metadata, that are necessary to describe, inventory, analyze, and classify data. A data registry supports data sharing with common data cross-system and cross-organization descriptions. Shareable data units have precise identifiers, meanings, structures, and values and are consistently deployed among users and systems and are centrally administered within an organization. Data registries are organized into federations for interchange among many enterprises. A data registry helps shared data users to have a common understanding of a unit of data's meaning, representation, and identification. Just as a data registry helps users understand like data units, registries also help users understand differences of similar but different data units.

**DATA REGISTRATION AUTHORITY:** An individual or group responsible for administering the data registry and who acts as a resource to the registry's clients to establish metadata about registered data and their applications.

**DATA WAREHOUSE:** (1) A subject-oriented, integrated, time-variant, on-volatile data collection supporting management's decision making process. A consistent historical data repository can be easily accessed and manipulated to support decisions. (2) Implementing an informational database used to store sharable data sourced from an operational database-of-record. It is typically a subject database that allows users to tap into a company's vast store of operational data to track and respond to business trends and facilitate forecasting and planning efforts. (3) An integrated (cross-functional), complete, historical, non-volatile data repository obtained from a variety of sources, such as operational databases and external sources that can be accessed and manipulated for strategic decision support. Data are usually extracted, transformed (including cleansing) and loaded into the warehouse. Managers, analysts, researchers, and others with a need to perform reporting, analysis, and data mining are the primary users of a data warehouse. Data warehouses are typically implemented at the corporate level and provide strategic analysis capability often to the lowest level of data granularity. A data warehouse is created based on corporate subject areas and is usually built and owned by centrally coordinated organizations.

**DECISION SUPPORT SYSTEM (DSS):** Database(s), warehouse(s), and/or mart(s) in conjunction with reporting and analysis software optimized to support timely business decision making. A computer-based information system that is designed to improve human decision making processes and outcomes. Most decision support systems are developed to support an individual decision-maker, such as a manager or an engineer, but a number of decision makers use some to arrive at a common decision, called group decision support systems. An example of a group decision support system is the executive information system (EIS), which gives decision makers access to the same information system and supports individual or discrete decisions.

**DECRYPTION:** (1) The translation of encrypted text or data (called cipher text) into original text (called plain text). Sometimes called "deciphering." [O'Reilly, 1992] (2) The process of decoding a message so that its meaning becomes obvious. [OTA, 1993]

**DEVELOPMENT:** Building an application system that carries out an automated process, particularly employing a new method or replacing a manual effort.

**DIAL-UP:** To connect to a computer by calling it on the telephone (usually via a modem).

**DIGITAL SIGNATURE:** (1) Data appended to, or cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the data unit's source and integrity and protect against forgery, for example, by the recipient. [ISO 7498 - 2] (2) An authentication mechanism that enables the creator of a message to attach a signature code. The signature guarantees the message source and integrity. [Stallings] (3) An authentication tool that verifies a message's origin and the sender's and receiver's identity. It can be used to resolve any authentication issues between the sender and receiver. A digital signature is unique for every transaction. [O'Reilly, 1992] (4) A means to guarantee the authenticity of a set of input data the same way a written signature verifies a paper document's authenticity. A cryptographic data transformation that allows a data recipient to prove the data source and integrity and protect against forgery. Specifically, an asymmetric cryptographic technique in which each user is associated with a public key distributed to potential verifiers of the user's digital signature used to encrypt messages destined for other users, and a private key known only the user knows and is used to decrypt incoming messages. To sign a document, the document and private key are input to a cryptographic process that outputs a bit string (the signature). To verify a signature, the signature, document, and user's public key are input to a cryptographic process, which returns an indication of success for failure. Any document modification after it is signed will cause the signature verification to fail (integrity). If the signature were computed using a private key other than the one corresponding to the public key used for verification, the verification will fail (authentication). [ASTM E1762]

**DIRECTORY SERVICE:** A system that provides locator services that are restricted to finding the location of a service, location of data, or translation of a common name into a network specific address. It is analogous to telephone books and supports distributed directory implementations.

**DISASTER RECOVERY:** The process whereby an enterprise would restore any loss of data in the event of fire, vandalism, natural disaster, or system failure. [CPRI, 1996c]

**DISCLOSURE:** The release of information to third parties within or outside the health care provider organization from an individual's record with or without the consent of the individual to whom the record pertains. A multitude of internal and external health information users exist for which various disclosure policies may apply. For instance, when patients present to a health care facility or provider for treatment, it is reasonable to assume they are

authorizing the caregiver to have information about their condition and treatment. However, such assumptions should not extend to all health care provider organization employees, but only those with a need to know. Disclosures for quality monitoring, educational purposes, research, administrative purpose, payment purposes, attorneys, law enforcement personnel and agencies, family members, and the patients themselves all must be conducted according to institutional policies. [CPRI, 1995b; CPRI, 1995c]

**DISTRIBUTED DATABASE:** A database whose objects (tables, views, columns and files) reside on more than one system in a network and can be accessed or updated from any system in the network.

**DISTRIBUTED SYSTEMS:** Refers to computer systems in multiple locations throughout an organization working in a cooperative fashion, with the system at each location serving the needs of that location but also able to receive information from other systems and supply information to other systems within the network.

**DOCUMENT TYPE DEFINITION (DTD):** A DTD is the formal definition of the elements, structures, and rules for marking up a given type of SGML document. You can store a DTD at the beginning of the document or externally in a separate file.

**DOMAIN:** The set of objects that a subject is allowed to access. [O'Reilly, 1992]

**DOWNLOAD (D/L):** The transfer of mainframe information/data/files to mini or microcomputers or the transfer of downloaded information from a central file server to other processors.

## *E*

---

**ELECTRONIC COMMERCE (EC):** The end-to-end digital exchange of all information needed to conduct business. Examples include EDI transactions, electronic mail, archives, audit trails, and all forms of records, including graphical images.

**ELECTRONIC DATA INTERCHANGE (EDI):** The inter-organizational, computer-to-computer exchange of structured information in a standard, machine-processable format.

**ELECTRONIC FUNDS TRANSFER (EFT):** EFT is one of the electronic commerce technologies that allows funds transfer from the bank account of one person or organization to that of another. EFT also refers to the action of using this technology.

**ELECTRONIC MAIL (EMAIL):** Correspondence sent by computer users to each other electronically. Mail can include text, graphics, or audio files depending on the capability of the computer.

**ELECTRONIC SIGNATURE:** The attribute affixed to an electronic document to bind it to a particular entity. An electronic signature process secures the user authentication (proof of claimed identity, such as by biometrics fingerprints, retinal scans, and hand-written signature verification, tokens or passwords at the time the signature is generated; creates the logical manifestation of signature, including the possibility for multiple parties to sign a document and have the order of application recognized and proven, and supply additional information, such as user-specific time stamp and signature purpose; and ensures the signed document's integrity to enable transportability, interoperability, independent verifiability, and continuity of signature capability. Verifying a signature on a document verifies the document's integrity and associated attributes and verifies the signer's identity. There are several technologies available for user authentication, including passwords, cryptography, and biometrics. [ASTM 1762]

**ENCRYPTION:** (1) The cryptographic transformation of data to produce cipher text. [ISO 7498-2] (2) The process of encoding a message so that it's meaning is not obvious. [OTA, 1993] (3) A method of ensuring data secrecy. The message is encoded using a key available only to the sender and the receiver. The encoded message is sent to the receiver and then decoded upon receipt.

**ENHANCEMENT:** Upgrading of an existing system, such as adding new functions or reports.

**ETHERNET:** Networking architecture, a bus-structured LAN designed originally at Xerox Corporation. See IEEE 802.3 for technical specifications.

**EXECUTIVE INFORMATION SYSTEMS (EIS):** Decision support software; a wide variety of software developed for executive (manager) use to help organize information for decision making.

**EXPERT SYSTEMS:** A practical development of Artificial Intelligence (AI) which requires creating a fact and rules knowledge base human experts and uses furnish as a defined set of rules (inference engine) to access this information to suggest solutions to problems.

**EXTENDED BINARY CODED DECIMAL INTERCHANGE CODE (EBCDIC):** An IBM system for encoding letters, numerals, punctuation marks, and signs that

accommodates twice as many symbols and functions as ASCII by using eight-place binary numbers instead of seven-place numbers.

**EXTENSIBLE MARKUP LANGUAGE (XML):** A standard from the WWW Consortium (W3C) that provides tagging information content within documents, offering a means to represent content in a format which is both human and machine readable. Through using customizable “style sheets” and “schemas” information can be represented in a uniform way, allowing for interchange of both content (data) and format (meta-data).

**EXTRANET:** When a company or organization extends information normally available exclusively on their Intranet out to the public, via the Internet.

## *F*

---

**FEDERAL INFORMATION PROCESSING STANDARD (FIPS):** Standards published by the U.S. National Institute of Standards and Technology, after approval by the Department of Commerce; used as a guideline for federal procurements.

**FILE TRANSFER PROTOCOL (FTP):** The Internet standard high level protocol to transfer files from one computer to another.

**FIREWALL:** (1) A computer system that sits between the Internet and a company's WAN or LAN. It is a means of automatically limiting what a company's computer system will pass along to outside computer systems. It acts as an active gateway to keep non-company entities from accessing company confidential data. (2) A dedicated computer equipped with safeguards that acts as a single, easily defined, Internet connection [Cheswick and Bellovin, 1994]

**FLEXIBILITY:** The ease with which a system or component can be modified for use in applications or environments other than those for which it was specifically designed.

**FRAME RELAY:** An ANSI and CCITT defined LAN/WAN networking standard for switching frames in a packet mode similar to X.25 but at higher speeds and with less nodal processing (assuming fiber transmission).

**FREEDOM OF INFORMATION ACT:** A U.S. law that requires records pertaining to the executive branch of the Federal government be available to the public except for matters that fall within exempted areas, including "medical files and similar files, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." [U.S.C. §552]

## G

---

**GATEWAY:** (1) A device in the computer communications environment that directs information traffic. Gateways are often employed to connect a network under one organization's control (an internal network) to a network another organization controls (an external network, such as a public network). Thus gateways are natural points at which to enforce access control policies. [National Research Council, 1991] (2) A computer system that transfers data between normally incompatible applications or networks or which allows users of one system or network to gain access to another network or system and provides protocol translation as needed.

**GIGABYTE:** A billion bytes of data.

**GOAL:** A general statement of direction.

**GRAPHICAL USER INTERFACE (GUI):** A graphics-based system that incorporates visual representations of data and processes, using icons, pull-down menus, and a mouse. Examples are Windows on the MS DOS platform, the Macintosh's Standard User Interface and OS/2 Presentation Manager.

**GroupWare:** A class of applications that use collaborative data stored on a server. Examples are electronic mail, group scheduling, and project management applications.

## H

---

**H.261:** An international video conferencing standard.

**H.320:** An international video conferencing standard.

**H.323:** A set of international video conferencing standards.

**HARDWARE:** The physical apparatus of a computer system.

**HEALTH CARE DATA:** Data that the automated information system inputs, stores, processes or outputs. Data that support the health care establishment's business functions. These data may relate to person-identifiable records or may be part of an administrative system where persons are not identified.

**HEALTH LEVEL 7 (HL7):** HL7 is the dominant standard for peer-to-peer exchange of clinical, text-based information.

**HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA):** Congressional law passed in 1996 that requires the HHS to implement regulations that will require using specific standards related to health care claims, code sets, identifiers (individual, provider, employer, and health plan), and security.

**HYPERLINKS:** An image or text that usually stands out in a document by color or size or instruction which links you to another document or a different point in the same document. The link will give an indication as to where the user will be sent. The user will click on the link with a mouse and arrive at the destination advertised by the link.

**HYPERTEXT MARKUP LANGUAGE (HTML):** The language used to create a web page. It is a subset of SGML. It provides verbal cues, which act as commands that a browser interprets when downloading an HTML file, in the text of an HTML document.

**HYPERTEXT TRANSFER PROTOCOL (HTTP):** Protocol used on the WWW to exchange HTML documents.

## *I*

---

**ICON:** In graphical environments, a small graphic image displayed on the screen to represent an object that can be manipulated by the user. Provides a user-friendly interface that allows the user the option to manipulate computer functions without knowing specific commands.

**IDENTIFICATION:** The process of telling a system the identity of a subject (e.g., a user or another system). Usually, this is done by entering a name or presenting a token to the system. See also authentication. [O'Reilly, 1992]

**IHS CORPORATE DATABASE:** A database that contains aggregated, IHS-wide data. The data is primarily obtained from operational systems in the field. The database will normally serve one of the following purposes: operational data store, transaction processing, data warehouse, or data mart. The database is normally used to support program management or other decision making at a national level.

**INFORMATION:** (1) Data that has been processed to a point where it conveys knowledge or represents a usable statement of fact. (2) Data to which meaning

is assigned, according to context and assumed conventions. [National Security Council, 1991]

**INFORMATION ENGINEERING:** A methodology for developing an integrated information system based on the sharing of common data, with emphasis on decision-support needs as well as transaction processing requirements. It uses a logical data model as the basis for systems development.

**INFORMATION INFRASTRUCTURE:** A structured collection of information system components and organization processes that enable the flow of necessary information to effect enterprise integration.

**INFORMATION MANAGEMENT (IM):** The creation, use, sharing, and disposition of information as a resource critical to the effective and efficient operation of functional activities. The structuring of functional processes to produce and control the use of data and information within functional activities, information systems, and computing and communications infrastructures.

**INFORMATION SUPERHIGHWAY:** The Information Superhighway is a network that will potentially connect every government agency, business, and citizen providing a means of rapid access to information (in digital form) and electronic communication to every business and citizen in the country. The purpose of the information superhighway is to provide an infrastructure for, among other things, electronic commerce, in a variety of forms including electronic banking, electronic data interchange, inventory managing, taxpaying, video conferencing, medical diagnosing, and virtually any other business activity. The closest approximation to the Information Superhighway at this time is the Internet.

**IT:** (1) The merging of computing and high-speed communications links carrying data, sound, and video. (2) The department responsible for all mainframe, telecommunications, media, television, video, micro computing and technical services.

**EA:** (1) An integrated framework that enables the evolution and maintenance of existing IT systems and guides future technology acquisitions. (2) The structures or components, their relationships, and the principles and guidelines governing their design and evolution over time (IEEE). (3) A series of principles, guidelines or rules used by an enterprise to direct the process of acquiring, building, modifying and interfacing IT resources throughout the enterprise. These resources can include equipment, software,

communications, development methodologies, modeling tools and organizational structures.

**INFORMED CONSENT:** The Department of Veterans Affairs requires that for consent to be valid, the patient must be informed. It therefore must be "a freely given consent that follows a careful explanation by a caregiver to a patient or patient's representative of the proposed diagnostic or therapeutic procedure or course of treatment...the patient should be given the opportunity to ask questions, to indicate comprehension of the information provided, and to grant permission freely and without any coercion for performance of a procedure or course of treatment, as well as the opportunity to withhold or revoke such permission at any time without prejudice." [Huffman, 1985] (2) Regulations promulgated by the HHS for consent by human subjects in medical treatment (4 CFR Section 46.116) provides that informed consent to release of information should include the elements of disclosure, voluntariness, comprehension, and competence to consent. [OTA, 1993]

**INFRASTRUCTURE:** System of wire, hardware, software and facilities that enables the connection of voice-data-video devices and the transmission of voice-data-video information from device to device.

**INSTALLED BASE:** The current environment.

**INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE):** An organization of engineers, scientists and students involved in electrical, electronics, and related fields that also functions as a publishing house and standards-making body.

**INTEGRATED:** Interrelated entities that result in a synergistic effect but that may also create extensive interdependencies.

**INTEGRATED CASE (I-CASE):** Computer-aided systems engineering (CASE) software that automates the systems analysis, design, and programming necessary for systems development. I-CASE refers to environments that enforce the seamless integration of deliverables for all phases of the software life cycle.

**INTEGRATED SERVICES DIGITAL NETWORK (ISDN):** A CCITT defined digital network standard for integrated voice and data network access, services, and user network messages.

**INTEGRITY:** (1) The property that data has not been altered or destroyed in an unauthorized manner. [ISO 7498 - 2] (2) A security principle that keeps

information from being modified or otherwise corrupted either maliciously or accidentally. Integrity protects against forgery or tampering. [O'Reilly] (3) The property that an object (health data or information) is modified only in a specified and authorized manner. [Ball and Collen, 1992] (4) Data integrity (the accuracy and completeness of the data), program integrity, system integrity, and network integrity are all relevant to consideration of computer and system security. [National Research Council, 1991]

**INTERNATIONAL CLASSIFICATION OF DISEASES (ICD):** ICD is developed by the World Health Organization and is designed for the classification of morbidity and mortality information for statistical purposes, and for the indexing of hospital records by disease and operations, for data storage and retrieval. The 9<sup>th</sup> revision (ICD-9) is in current use and a 10<sup>th</sup> revision is underway. Diagnoses and procedures coded in ICD-9-CM (Clinical Modification) determine the DRG that controls reimbursement by U.S. Public Health Service and Health Care Financing Administration programs, and most other payers.

**INTERNATIONAL STANDARDS ORGANIZATION (ISO):** ISO is the international standards organization that is similar in function to ANSI. They do not create standards but, as with ANSI, provide a means of verifying that a proposed standard has met certain requirements for due process, consensus, and other criteria by those developing the standard. After this verification the standard is approved by ISO as an international standard.

**INTERNATIONAL STANDARDS ORGANIZATION/OPEN SYSTEM**

**INTERCONNECTION (ISO/OSI):** A standard approach to network design developed by the International Standards Organization that introduces modularity by dividing the complex set of functions into more manageable, self-contained, functional elements. OSI is a seven-layer framework for implementing open systems rules and regulations.

**INTERNATIONAL STANDARDS ORGANIZATION TECHNICAL COMMITTEE**

**215 (ISO TC 215):** The ISO TC 215 on Health Informatics develops and/or adopts standards in the field of health information and communications technology. This committee can have a significant impact on health care standards. It can also fast track the international adoption of existing European and/or US standards.

**INTERNATIONAL TELECOMMUNICATION UNION (ITU):** An international committee that promotes international telecommunication standards.

**INTERNET:** Generally any collection of distinct networks working together as one. Specifically, the world-wide "network of networks" that are connected to each other, based upon an Internet Protocol (IP), the network layer in the TCP/IP Protocol and that all share a common addressing scheme. The Internet provides file transfer, remote login, electronic mail, news and other services.

**INTERNET ENGINEERING TASK FORCE (IETF):** An organization that reviews and issues Internet standards. [CORBA Security Services, 1997]

**INTERNET PROTOCOL (IP):** A standard that describes how packets of data are transported across the Internet and recognized as an incoming message.

**INTERNET SERVICE PROVIDER (ISP):** A company that provides access to the Internet for other companies and/or individuals. They are NOT commercial services such as Prodigy, America Online, CompuServe, or Microsoft Network. A subscriber must use browser software such as Netscape to access the World Wide Web. Often, ISPs will also provide email and web site creation and maintenance capability for the user(s).

**INTEROPERABILITY:** The ability of two or more systems or components to exchange and use information.

**INTERPROCESS COMMUNICATION:** Communication between two processes, whether the processes reside on the same or different machines.

**INTERRUPT REQUEST (IRQ):** A method used to get the attention of the computer system in order to have the system perform a task.

**INTRANET:** A network available via the Internet, but only accessible by users within a specific organization.

**INTRUDER:** An individual who gains, or attempts to gain, unauthorized access to a computer system or to gain unauthorized privileges on that system. [Stallings, 1995]

**ISO 9000:** A series of international standards that provides quality management guidance and identifies quality system elements that are necessary for quality assurance. In other words, the ISO 9000 series standards have two main roles: to provide guidance for suppliers of all types of products that wish to implement effective quality systems (or improve existing ones); and to provide the generic requirements against which that quality system can be evaluated.

*J*

---

**JAVA:** A programming language that can be used to extend the capabilities of a web browser. JAVA programs are referred to as applets when they are transferred from one machine and executed on another via a browser.

**JOINT APPLICATIONS DESIGN (JAD):** A software design methodology that draws users and information systems professionals together to jointly design systems in facilitated working groups.

**JOINT COMMISSION ON ACCREDITATION OF HEALTH CARE**

**ORGANIZATIONS (JCAHO):** An organization that certifies the compliance of hospitals with a number of specific accreditation standards. The 1996 JCAHO Accreditation Manual for Hospitals specifies information management (IM) standards. IM.2 states that the "confidentiality, security and integrity of data and information are maintained." IM.2.2 states that "the hospital determines appropriate levels of security and confidentiality for data and information . . ." and continues by stating that the "collection, storage and retrieval systems are designed to allow timely and easy use of data and information without compromising its security and confidentiality." IM.2.2.3 states that "records and information are protected against loss, destruction, tampering and unauthorized access or use." The intent of these standards is to ensure that a hospital maintains the security and confidentiality of data and is especially careful about preserving the confidentiality of sensitive data. The hospital is expected to determine the level of security and confidentiality maintained for different types of information. Access to each category of information is based on need and defined by job title and function.

**JOINT PHOTOGRAPHIC EXPERTS GROUP (JPEG):** A graphics format which, along with GIF, is widely used on the World Wide Web. Its superior compression capability and ability to show millions of colors makes it the choice format for more complex images such as photographs and artwork.

*K*

---

**KERBEROS:** The name given to Project Athena's code authentication service. [Stallings, 1995]

**KERMIT:** A telecommunications protocol used to emulate a terminal and to send files from one computer to another.

**KEY:** (1) In cryptography, a secret value that's used to encrypt and decrypt messages. A sequence of symbols (often a large number) that's usually known only to the sender and the receiver of the message. See also private key

encryption and public key encryption. [O'Reilly, 1992] (2) An input that controls the transformation of data by an encryption algorithm [National Research Council, 1991]

**KILOBYTE (KB):** 1,024 bytes (1,024 being one K, or two to the 10th power): Often used as a measure of memory capacity.

## *L*

---

**LANGUAGE:** A set of rules or conventions to describe a process to a computer.

**LARGE-SCALE INTEGRATION (LSI):** The placement of thousands of electronic gates on a single chip. This makes the manufacture of powerful computers possible.

**LASER:** Technology of reading/writing data on durable media using a laser light source or producing print on dry toner image engines.

**LEGACY SYSTEM:** A functioning computer software application using conventional methodologies; usually a significant portion of the current installed base.

**LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL (LDAP):** A set of protocols for accessing information directories. LDAP was originally intended to give clients on desktop computers access to X.500 directories. It has many similarities to X.500. Like X.500 LDAP defines a global directory structure, including how the information in a directory is to be organized and also the protocol for accessing the information. Unlike X.500 it is simpler in concept and more easily implemented. It also supports TCP/IP. In common with X.500 the LDAP information model is based on the entry, which contains information about some object (e.g., a person). Entries may include a mix of information such as JPEG photographs, sounds, URLs and PGP keys. Directory entries are arranged in a hierarchical tree-like structure. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

**LINK ENCRYPTION:** A type of encryption in which a message is encrypted when it is transmitted and is decrypted when it is received. Contrast with end-to-end encryption.[O'Reilly, 1992]

**LOCAL AREA NETWORK (LAN):** A system of computer hardware and software that links computers, printers, and other peripherals into a network suitable

for data transmission in a limited geographic area and that allows easy interconnections between all components of the network.

**LOGICAL OBSERVATION IDENTIFIERS, NAMES, AND CODES (LOINC):** The LOINC™ database provides a set of universal names and ID codes for identifying laboratory and clinical observations. LOINC codes are used to facilitate the exchange and pooling of clinical laboratory results, such as blood hemoglobin or serum potassium, for clinical care, outcomes management, and research.

**LOGIN:** (1) The process of identifying oneself to, and having one's identity authenticated by, a computer system. [O'Reilly, 1992] (2) A log on command that gains access to another computer, network, or on-line service, generally including personal identification information and a password.

## *M*

---

**MACHINE LANGUAGE:** A set of binary-code instructions capable of being understood by a computer without translation.

**MACHINE-READABLE CODE (MARC):** Inventory cataloging and coding system, read/write by computer.

**MAGNETIC TAPE:** Magnetic tape is the physical medium for storage and delivery of data in digital form. It is a stable technology that is able to handle large volumes of data.

**MAGNETO-OPTICAL (MO):** A high-density, re-writeable recording method that uses a combination of magnetic disk and optical methods.

**MAINFRAME COMPUTER (CPU, M/F):** One of the largest types of computer, usually capable of serving many users simultaneously, with exceptional processing speed.

**MAINTENANCE:** Any modification required to keep a system operating at its intended level.

**MANAGEMENT INFORMATION SYSTEMS (MIS):** The total of all information resources, manual and automated, and their application to the normal functions of running an organization - management, administration, problem solving, etc.

**MANDATORY ACCESS CONTROL (MAC):** (1) An access control regime wherein resource access control policy information is always managed by a designated authority, regardless of who creates the resources. [CORBA Security Services, 1997] (2) A means of restricting access to objects that is based on fixed security attributes assigned to users and to files and other objects. The controls are mandatory in the sense that they cannot be modified by users or their programs. [Stallings, 1995] Contrast with discretionary access control.

**MARKUP:** Tags that are added to the data of a document in order to convey information about the data.

**MASSIVELY PARALLEL SYSTEMS:** Tightly coupled multi-processing computers that house 100 or more central processing units (CPUs), each with its own memory.

**MASTER PERSON INDEX (MPI):** (1) The means for locating a patient record in a numeric identification system. [Abdelhak, 1996] (2) A cross-reference or index of patients that includes the patient's related identifiers and other patient identifying information. It is used to associate a patient's identifiers among multiple ID-assigning entities, possibly including a clinical data repository, to support the consolidation and sharing of a patient's health care information. (3) It has generally referred to an index within a given health care facility, in which case it serves as a patient directory. [CPRI, 1996a]

**MEDIUM ACCESS CONTROL (MAC):** IEEE 802 defined media specific control protocol.

**MEGABYTE (Mb):** One million bytes of data (1,048,576 bytes).

**MEGAHERTZ (MHz):** A unit of measurement equal to one million electrical vibrations or cycles per second. Commonly used to compare the clock speeds of computers.

**MESSAGE AUTHENTICATION:** Ensuring, typically with a message authentication code, that a message received (usually via a network) matches the message sent. [O'Reilly, 1992]

**MESSAGE AUTHENTICATION CODE (MAC):** A code calculated during encryption and appended to a message. If the message authentication code calculated during decryption matches the appended code, the message was not altered during transmission. [O'Reilly, 1992] Sometimes the acronym "MAC" is used for message authentication code.

**MESSAGING APPLICATION PROGRAMMING INTERFACE (MAPI):** The Microsoft Windows Messaging Application Programming Interface that is part of WOSA (Windows Open Services Architecture).

**METADATA:** In data processing, metadata is definitional data that provides information about or documentation of other data managed within an application or environment. For example, metadata would document data about data elements or attributes, (name, size, data type, etc.) and data about records or data structures (length, fields, columns, etc.) and data about data (where it is located, how it is associated, ownership, etc.). Metadata may include descriptive information about the context, quality and condition, or characteristics of the data.

**METROPOLEAN AREA NETWORK (MAN):** A MAC level data and communications network which operates over metropolitan or campus areas and recently has been expanded to nationwide and even worldwide connectivity of high-speed data networks. A MAN can carry video, data, and has been defined as both the DQDB and FDDI standard sets.

**MICROPROCESSOR:** A single chip containing all the elements of a computer's central processing unit; also called a computer chip.

**MICROSOFT INTERNET EXPLORER:** A Web browser created by Microsoft.

**MIDDLEWARE:** Software that interprets requests between a PC or workstation application and an antiquated database running on a mainframe. Also used to describe software that helps an application communicate with an underlying operating system. Middleware is also frequently used as a mechanism for communication between distributed application processes.

**MILLIONS OF INSTRUCTIONS PER SECOND (MIPS):** Measured in millions, i.e. 19 MIPS is nineteen million machine instructions per second, a measure used to compare relative computing power.

**MINICOMPUTER:** A mid-size computer smaller than a mainframe and usually with much more memory than a microcomputer.

**MODEL:** An abstract representation of a process, device, or system that accounts for all of its known properties.

**MODULATOR/DEMODULATOR (MODEM):** An external or internal device attached to a computer that translates digital information into analog form and back again. This device enables computers to communicate over telephone

lines. Telecommunications software is required to act as an interface between the computer and its modem and other computers and telecommunications software.

**MONITOR:** A television-like output device for displaying data, typically based on a cathode ray tube but can also be of an LCD or other variety.

**MOTION PICTURES EXPERTS GROUP (MPEG):** An emerging standard for compression of full motion images driven by the same committee as the Joint Photographic Experts Group (JPEG) standard.

**MULTIMEDIA:** Software that incorporates graphics, video, text and sound into an interactive computer presentation or database of information.

**MULTIPURPOSE INTERNET MAIL EXTENSIONS (MIME):** A standard protocol for exchanging attachments (audio, video, graphics, etc.) to email messages over the Internet.

**MULTIDIMENSIONAL OLAP (MOLAP):** A type of OLAP that enables multidimensional analysis of typically aggregated data stored in proprietary, multidimensional databases. MOLAP tools often provide the capability to “reach-through” and retrieve detailed data from relational sources.

## *N*

---

**NANOSECOND (Ns):** A billionth of a second, a common unit of measure of computer operating speed.

**NATIONAL COMMITTEE FOR INFORMATION TECHNOLOGY STANDARDS (NCITS):** Formerly known as X3, NCITS is an ANSI Accredited Standards Committee on IT. It is responsible for developing standards in technology areas such as multimedia, storage media, database, security, programming languages, etc.

**NATIONAL INFORMATION INFRASTRUCTURE (NII):** A concept conceived by the Clinton Administration and an alliance of computer, software, cable, and phone companies. The proposed concept would be the electronic network of tomorrow and would use phone line, cable systems, and high-speed data-networks to link everyone, including government agencies, universities, company presidents, and private citizens. The concept envisions vast amounts of services, entertainment, and information being made readily available through computers, televisions, telephones, and other means of electronic communication.

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST):** Created in 1901 as the National Bureau of Standards and renamed in 1988, the National Institute of Standards and Technology (NIST) works to strengthen U.S. industry's international competitiveness, advance science, and improve public health, safety and the environment. NIST conducts science and engineering research in commercially important fields.

**NATIONAL PROVIDER IDENTIFIER (NPI):** A unique identifier for all health care providers (individuals and organizations) in the U. S. that will be used in administrative, financial and other electronic transactions. The NPI will be assigned by the National Provider System.

**NATIONAL PROVIDER SYSTEM:** A system to generate and maintain unique identifiers for all health care providers (individuals and organizations) in the U.S. The NPS will be administered by the Health Care Finance Administration (HCFA) of the HHS.

**NATIONAL RESEARCH AND EDUCATION NETWORK (NREN):** A group that shares research and education information over a computer network.

**NETSCAPE:** A Web browser created by Netscape Communications Corporation.

**NETWORK:** The means for one computer or device to work and communicate with another. It is a combination of software and hardware that supports transmission of information from one computer to another.

**NETWORK ARCHITECTURE:** A set of design principles, including the organization of functions and services, used as the basis for design and implementation of a user application network.

**NETWORK INFORMATION CENTER (NIC):** Any organization responsible for supplying information about any network.

**NETWORK NEWS TRANSPORT PROTOCOL (NNTP):** An extension of the TCP/IP protocol that describes how newsgroup messages are transported between compatible servers.

**NEURAL NETWORK:** A computer architecture that enables redundancy, self-reparation of communications paths, and supports high traffic loads through routing decisions.

**NEWSGROUP:** Allows members to go onto the Internet to read collected articles about a specific topic; while Listserves sends the same kind of information to a member's email box.

**NODE:** A junction of communications paths in a network.

**NON-REPUDIATION:** (1) The provision of evidence which will prevent a participant in an action from convincingly denying his responsibility for the action. [CORBA Security Services, 1997] (2) Proof (to a third party) that only the signer could have created a signature. A basis of legal recognition of electronic signatures. [ASTM E1762]

---

## O

---

**OBJECT:** From the Orange Book definition "A passive entity that contains or receives information. Access to an object potentially implies access to the information it contains. Examples of objects are records, blocks, pages, segments, files, directories, directory trees, and programs, as well as bits, bytes, words, files, processors, video displays, keyboards, clocks, printers, network nodes, etc." [O'Reilly, 1992]

**OBJECT BROKER TECHNOLOGY:** Technology that allows application processes to communicate across a network using an object-oriented architecture.

**OBJECT-ORIENTED SYSTEMS:** Systems composed of objects (conceptual or programmatic abstractions that include data and functionality encapsulated in a single unit) that communicate with one another using explicitly defined interfaces.

**OBJECTIVE:** Specific accomplishments necessary to the attainment of goals.

**OFFICE DOCUMENT ARCHITECTURE / OFFICE DOCUMENT**

**INTERCHANGE FORMAT (ODA/ODIF):** An explicit document architecture and interchange format standard which allows exchange of compound documents (i.e., documents composed of various content types, such as character, raster graphics, and geometric (Computer) graphics content.

**OBJECT LINKING AND EMBEDDING (OLE):** A method that establishes a way to transfer and share information between applications.

**OBJECT ORIENTED PROGRAMMING SYSTEM (OOPS):** A method of applications development based on the assembly of functional modules.

**ON-LINE ANALYTICAL PROCESSING (OLAP):** A style of decision support processing that enables analysts, managers, and executives to gain insight into data through interactive access. Measures (e.g., cost per patient) are analyzed via dimensions (e.g., time, provider, medical center, line-of-care) and attributes of the dimensions or members (e.g., attributes of time are month, fiscal quarter, and fiscal year). OLAP is a rapid, iterative process, in which the user slices the data across any dimension or member. Data navigation capabilities including “drill down” to lower levels of detail data, “drill-up” to the most summarized data, and “drill across” to different data views are typically provided via a client or web browser graphical user interface (GUI). OLAP capabilities can include trend analysis over time, what-if analysis, modeling, and forecasting.

**OPEN COMPUTING:** A movement spawned by the UNIX community to make computers and software that are standardized along published specifications so that hardware and software can be interchanged.

**OPEN SYSTEM:** A system capable of communicating with other open systems by virtue of implementing common nonproprietary standard protocols.

**OPEN SYSTEMS ARCHITECTURE:** Use of standardized technology and structures for hardware, operating system, databases, fault tolerances, and networking and communications transport. [ASTM E1769]

**OPEN SYSTEMS FOUNDATION (OSF):** A group that supports open computing.

**OPEN SYSTEMS INTERCONNECTION (OSI):** A standard approach to network design developed by the International Standards Organization that introduces modularity by dividing the complex set of functions into more manageable, self-contained, functional elements. OSI is a seven-layer framework for implementing open systems rules and regulations.

**OPERATING SYSTEM:** A complex program used to control, assist, or supervise all other programs that run on a computer system.

**OPERATING SYSTEM/2 (OS/2):** An IBM microcomputer based operating system for use on Micro Channel based PCs. It includes a GUI (Graphical User Interface).

**OPERATIONAL ASSURANCE:** Confidence that a trusted system’s architecture and implementation enforce the system’s security policy. In the Orange Book,

the set of operational assurances includes system architecture, system integrity, covert channel analysis, and trusted recovery. [O'Reilly, 1992]

**OPERATIONAL DATA STORE (ODS):** A database where transactions are processed (recorded, updated, and deleted). It contains recent data and is likely to be highly volatile. An operational data store (ODS) consolidates data from multiple transactional systems and provides a near real-time, semi-integrated view of volatile, current, limited history, data. An ODS may be organized around an organization's major subject areas (e.g., patient, provider) and is used by analysts for operational decisions. The ODS may also be used as a staging area to drive a data warehouse or data mart.

**OPTICAL CHARACTER RECOGNITION (OCR):** The process by which text on paper is scanned and converted into text files by a computer system.

**OPTICAL DISK:** An unalterable optical storage medium that allows large amounts of data to be permanently written to it. An optical disk is read using laser and magnetic technology and has a useful life span of 100 plus years.

**OWNERSHIP:** It is a generally accepted principle that the primary patient record is maintained and owned by the health care provider. This principle is established by statutes and licensing regulations in many states, which grant the provider control over the physical document, but give the patient ownership-type rights to the information contained in the record. Therefore, the patient generally has control over the release of patient-identifiable (confidential) information, except in circumstances identified by case law, by federal or state statutes and regulations, and by provider policy. [CPRI, 1994]

## *P*

---

**PACKET:** A unit of data, consisting of binary digits including data and call-control signals, switched and transmitted as a composite whole.

**PACKET SWITCHING:** A data transmission technique where physical resources on a path are switched on a per packet basis, using control information in the header of each packet. It can operate in either a connection-oriented or connectionless mode.

**PAGE-DESCRIPTION LANGUAGE (PDL):** Software that instructs a printer in composing various elements (e.g., text, graphics, images) of a printed page.

**PARSER:** A parser is a specialized software program that recognizes SGML and markup in a document. A parser that reads a DTD and checks and reports on markup errors is a validating SGML parser. A parser can be built into an

SGML editor to prevent incorrect tagging and to check whether a document contains all the required elements.

**PASSWORD:** (1) Confidential authentication information composed of a string of characters. [ISO 7498 - 2] (2) A sequence that an individual presents to a system for purposes of authentication. [National Research Council, 1991]

**PATHNAME:** The combination of a file and the directory in which it resides. (E.g. If this glossary was the directory "glossary," and this definition was a file named "pathname," the pathname would be "glossary/pathname.").

**PCMCIA:** Personal Computer Memory Card International Association.

**PERSONALLY IDENTIFIABLE HEALTH INFORMATION:** Health information that contains an individual's identifiers (e.g., name, social security number, birth date) or contains a sufficient number of variable to allow identification of an individual. [OTA, 1993, Institute of Medicine, 1994]

**PHYSICAL SECURITY:** (1) Protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion. Also covers the use of locks, keys, and administrative measures used to control access to computer systems and facilities. [O'Reilly, 1992] (2) The measures used to provide physical protection of resources against deliberate and accidental threats. [CORBA Security Services, 1997]

**POINT TO POINT PROTOCOL (PPP):** A means to send packets of information over point-to-point serial connections between computers.

**PORTABILITY:** The ease with which a system or component can be transferred from one hardware or software environment to another.

**PORTABLE DOCUMENT FORMAT (PDF):** The native file format for Adobe Acrobat, it can represent documents containing graphics, text, images, color, or any combination thereof. It is device and resolution independent.

**PORTABLE OPERATING SYSTEM INTERFACE (POSIX):** This standard defines a C programming language source interface to an operating system environment. Computing professionals involved in system and application software development and implementation use this standard.

**PRIMARY PATIENT RECORD (PRIMARY RECORD OF CARE):** The primary legal record documenting the health care services provided to a person in any

aspect of health care delivery. This term is synonymous with medical record, health record, client record, and residence record. When stored in a computer system and used by caregivers while providing patient care services to review patient data, receive decision support, and document their own observations, actions, or instructions it is synonymous with all terms associated with computer-based patient record. [ASTM E1384; CPRI, 1996d]

**PRIVACY:** (1) An individual's desire to limit the disclosure of personal information. [NRC, 1997] (2) The right of individuals to keep information about themselves from being disclosed to anyone. [CPRI, 1995c] (3) As set forth by Samuel Warren and Louis Brandeis in a 1890 article that first enunciated the concept of privacy as a legal interest deserving an independent remedy, privacy was described as "the right to be let alone." Further, Alan Westin conceived of privacy as "an instrument for achieving individual goals of self realization." [OTA, 1993] (4) Ball and Collen describe privacy as the right of an individual to be left alone, to withdraw from the influence of the environment; to be secluded, not annoyed, and not intruded upon by extension of the right to be protected against physical or psychological invasion or against the misuse or abuse of something legally owned by an individual or normally considered by society to be property. [Ball and Collen, 1992] (5) A security principle that protects individuals from the collection, storage, and dissemination of information about themselves and the possible compromises resulting from unauthorized release of that information. [O'Reilly, 1992]

**PRIVACY ACT OF 1974:** A U.S. law that grants people certain rights to information collected about them by the federal government and its agencies. These rights include finding out what information has been collected, to see and have a copy of the information, to correct or amend the information, and to exercise limited control of the disclosure of that information to other parties. [U.S.C. §552a(b), 1977]

**PRIVATE KEY:** (1) One of the two keys used in an asymmetric encryption system. For secure communication, the private key should be known only to its creator. [Stallings, 1995] (2) A key in an asymmetric algorithm; the possession of this key is restricted, usually to one entity. [ASTM E1762]

**PRIVATE-KEY ENCRYPTION:** A type of encryption that uses a single key to both encrypt and decrypt information. Also called symmetric, or single-key, encryption. Contrast with public key encryption. [O'Reilly, 1992]

**PRIVILEGE:** (1) A right granted to a user, a program, or a process. For example, certain users may have the privileges that allow them to access certain files in a system. Only the system administrator may have the

privileges necessary to export data from a trusted system. [O'Reilly, 1992] (2) A security attribute that need not have the property of uniqueness and which may be shared by many users and other principals. Examples of privileges include groups, roles, and clearances. [CORBA Security Services, 1997]

**PROFILING:** The selecting of standards for a particular application.

**PROGRAM EVALUATION REVIEW TECHNIQUE (PERT) CHART:** A project management chart illustrating task relationships and dependencies.

**PROPRIETY STANDARD (Defacto Standard):** A standard which has been endorsed by industry or government as the accepted international standard, but not officially approved by an accredited standards body such as ISO.

**PROTOCOL:** A mutually determined formal agreement - standard - that determines the form and style of communication that assures reliable information transfers between computers.

**PUBLIC KEY:** (1) One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key.[Stallings, 1995] (2) In a public-key (asymmetric) crypto-system, the component of a key pair which is revealed. [CORBA Security Services, 1997] (2) A key in an asymmetric algorithm, that is publicly available. [ASTM E1762]

**PUBLIC KEY CERTIFICATE:** (1) An agreement that binds a user's name to a public key, signed by a trusted issuer. A framework for the use of public key certificates was defined in Consultative Committee on International Telephony and Telegraphy (CCITT) standard X.509. [National Research Council, 1991] The certificate contains the user's name and public key, the certification authority's name, a serial number, and a validity period. [ASTM E1762]

**PUBLIC-KEY CRYPTO-SYSTEM:** An encryption system that uses an asymmetric-key (q.v.) cryptographic algorithm. [CORBA Security Services, 1997]

**PUBLIC-KEY ENCRYPTION:** A type of encryption that uses two mathematically related keys. The public key is known within a group of users. The private key is known only to its owner. Asymmetric encryption. Contrast with private key encryption. [O'Reilly, 1992]

**PUBLIC KEY INFRASTRUCTURE (PKI):** A system of digital certificates, Certificate Authorities, and other registration authorities that verify and

authenticate the validity of each party involved in an Internet transaction. The concept of a PKI is currently evolving and there is no single PKI or even a single agreed-upon standard for setting up a PKI. However, nearly everyone agrees that reliable public key infrastructures are necessary before electronic commerce can become widespread.

## *Q*

---

**QUERY:** The ability to interrogate databases without predetermined designs and/or programming expertise.

**QUERY LANGUAGE:** A defined set of syntax and commands used to submit queries to a text retrieval system.

## *R*

---

**RANDOM ACCESS MEMORY (RAM):** A form of temporary internal storage whose contents can be retrieved and altered by the user; also called read-and-write memory.

**RAPID APPLICATION DEVELOPMENT (RAD):** A development lifecycle designed to give much faster development and higher quality results than the traditional lifecycle.

**READ-ONLY MEMORY (ROM):** Permanent internal memory containing data or operating instructions that cannot be altered.

**REAL TIME:** Programs which process immediately as information is received rather than accumulating data for long periods and processing all of it at one time (batch).

**RECOVERY:** The restoration of an information system back to an error-free and secure state from which normal operation can resume. [O'Reilly, 1992]

**REDUNDANT ARRAYS OF INDEPENDENT DISKS (RAID):** A technology that provides protection from data loss by providing a level of redundancy immediately within the array. The array contains removable disk drive modules that are automatically rebuilt in the event of a device failure without causing the system to shut down.

**REFERENCE ARCHITECTURE:** (1) A specific technical framework defined by basic political, economic, functional, and technical constraints which guides future planning and implementation and is essential to understanding both

how the current systems operate and how evolution of systems can and should proceed. (2) An abstraction, or model, of the relationships between business processes, information needs, application systems, data definitions, and delivery systems or infrastructure.

**RELATIONAL DATABASE:** A collection of related (usually through a common field) data files.

**RELATIONAL DATABASE MANAGEMENT SYSTEM (RDBMS):** A system for storing data based on an architecture of relational calculus and/or relational algebra in which the database is organized and accessed according to the relationships between data items. Primary components are a Data Dictionary, Data Manipulation Language, Query Facility, Data Security System, and various/interactive systems.

**RELATIONAL OLAP (ROLAP):** A type of OLAP that enables multidimensional analysis of data stored in a relational database through a dictionary layer of meta-data and a calculation engine.

**RELEASE OF INFORMATION:** The disclosure of documents containing patient-identifiable information to a third party requester. [Huffman, 1985]

**RELIABILITY:** (1) A measure of consistency of data items based on their reproducibility and an estimation of their error of measurement. [Institute of Medicine, 1994] (2) The duration or probability of failure-free performance under stated conditions; or the probability that an item can perform its intended function for a specified interval under stated conditions.

**REMOTE LOG-IN:** A network service that allows a user on one machine to connect to another machine across a network and interact as if directly connected to the remote machine.

**REMOTE PROCEDURE CALL (RPC):** A software interface in which the actual execution of the body of the software program (procedure) takes place on a physically distinct processor from that on which call is made.

**REPLAY:** The recording of a legitimate message and the later, unauthorized re-sending of the message. [O'Reilly, 1992]

**REPORT PROGRAM GENERATOR II (RPGII):** A commercially oriented programming language specifically designed for writing application programs that meet common business data processing requirements.

**REPOSITORY:** A facility for storing descriptions and behaviors of objects in an enterprise, including requirements, policies, processes, data, software libraries, projects, platforms and personnel, with the potential of supporting both software development and operations management.

**REPUDIATION:** (1) The denial by a message sender that the message was sent, or by a message recipient that the message was received. [O'Reilly, 1992] (2) Denial by one of the entities involved in a communication of having participated in all or part of the communication. [ASTM 1762]

**RIVEST, SHAMIR AND ADELMAN (RSA):** The inventors of a public key encryption algorithm that has become a de facto standard for data sent over the Internet. The RSA public-key encryption algorithm relies on the inability to factor large numbers of a special type and, therefore, an extraordinary amount of computer processing power and time is required to break a public key created by the RSA algorithm.

**ROLE:** A privilege attribute representing the position or function a user represents in seeking security authentication. A given human being may play multiple roles and therefore require multiple role privilege attributes. [CORBA Security Services, 1997]

**ROUTER:** A device that operates at the Network layer of the OSI model and links the data link layer and Physical layers of the OSI stack. Routers are used to interconnect multiple networks, potentially using different high-level protocols.

**RS-232:** A mechanical and electrical standard that permits the transfer of information between computers and communications equipment, and is also used to connect terminals, printers, and other peripheral devices.

**RSA ALGORITHM:** (1) An asymmetric encryption algorithm invented by Ron Rivest, Adi Shamir, and Len Adelman. A public-key algorithm based on exponentiation in modular arithmetic. It is the only algorithm generally accepted as practical and secure for public-key encryption. [Stallings, 1995] (2) A public key crypto-system, invented and patented by Ronald Rivest, Adi Shamir, and Leonard Adelman, based on large prime numbers. [National Security Council] (3) RSA is the most well known asymmetric algorithm. [ASTM E1762]

## S

---

**SCALABILITY:** The capability of a system to perform acceptably on any size computer depending on the needs of the user; implies minimal change to accommodate this variance.

**SEARCH ENGINE:** A web site that allows you to search for information throughout the World Wide Web. Many of the search engines allow you to narrow or broaden your search by subject or by locations. Alta Vista, Excite, Yahoo and HotBot offer some of the more popular search engines.

**SECRET KEY:** A key in a symmetric algorithm; the possession of this key is restricted, usually to two entities. [ASTM E1762]

**SECRET KEY CRYPTO-SYSTEM:** A crypto system that uses a symmetric-key (q.v.) cryptographic algorithm. [CORBA Security Services, 1997]

**SECURE ELECTRONIC TRANSACTION (SET):** A new standard that will enable secure credit card transactions on the Internet. Most of the major participants in electronic commerce, including Microsoft, Netscape, Visa, and MasterCard, have endorsed SET. SET supports digital signatures that can be used by merchants to verify that buyers are who they claim to be. The SET standard allows buyers to transmit their credit card number directly to the credit card issuer for verification and billing without the merchant seeing the number.

**SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS (S/MIME):** An extension to the MIME protocol that supports encryption of email messages.

**SECURE TIME:** A reliable Time service that has not been compromised, and whose messages their recipients can authenticate. [CORBA Security Services, 1997]

**SECURE SOCKETS LAYER (SSL):** A security protocol that provides communications privacy over the Internet between two communicating applications. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. This protocol was originally developed by Netscape Communications. The Internet Engineering Task Force is developing version 3.0 of this protocol.

**SECURITY:** (1) The combination of availability, confidentiality, integrity and accountability. Freedom from risk or danger. Safety and the assurance of safety. [O'Reilly, 1992] (2) Means to control access and protect information from accidental or intentional disclosure to unauthorized persons and from alteration, destruction, or loss. [CPRI, 1995b] (3) Protection of information systems against unauthorized access to or modification of information, whether

in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. [National Security Council]

**SECURITY AUDIT:** (1) An independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policies and operational procedures, to detect security breaches and to recommend any indicated changes in control policy and procedures. [ISO 7498 - 2] (2) The facility of a secure system that records information about security-relevant events in a tamper-resistant log. Often used to facilitate an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend changes in control, policy and procedures. [CORBA Security Services, 1997]

**SECURITY DOMAIN:** A set of information system assets for which an organization (or user) has responsibility for the implementation and maintenance of security. [Stallings, 1995]

**SECURITY LEVEL:** A representation of the sensitivity of information, derived from a sensitivity label (consisting of a classification and categories). [O'Reilly, 1992]

**SECURITY MANAGEMENT:** Security management services provide secure system set-up and initialization, control of security policy parameters, management of user registration data and system resources and restrictions on the use of administrative functions.

**SECURITY POLICY:** (1) A statement of the set of rules, measures and procedures that determine the physical, procedural and personnel security controls imposed on the management, distribution and protection of assets. [Stallings, 1995] (2) The framework within which an organization establishes needed levels of information security to achieve the desired confidentiality goals. A policy is a statement of information values, protection responsibilities, and organization commitment for a system. It is a set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information. [OTA, 1993] (3) The American Health Information Management Association recommends that security policies apply to all employees, medical staff members, volunteers, students, faculty, independent contractors, and agents. [AHIMA, 1996c] (4) From the Orange Book definition "The set of laws, rules, and practices that regulate how an organization

manages, protects, and distributes sensitive information.” [O’Reilly, 1992] (5)  
The data that defines what protection a system’s security services must provide. There are many kinds of security policy, including access control policy, audit policy, message protection policy, non-repudiation policy, etc. [CORBA Security Services, 1997]

**SECURITY SERVICE:** Code that implements a defined set of security functionality. Security services include Access Control, Audit, Non-repudiation, and others. [CORBA Security Services, 1997]

**SENSITIVE INFORMATION:** Information that, if lost or compromised, would negatively affect the owner of the information, would jeopardize the ability of the system to continue processing, and/or would require substantial resources to recreate. According to the U.S. government (NTISSP 2), "information the disclosure, alteration, loss, or destruction of which could adversely affect national security or other federal government interests." [O’Reilly, 1992]

**SENSITIVITY:** The degree of importance assigned to information denoting its need for protection against confidentiality related security breaches.

**SENSITIVITY LABEL:** (1) A security level associated with the content of the information. [National Security Council] Society has historically considered information that has a heightened potential for causing harm to the patient or data subject, or to others, such as the subject's spouse, children, friends, or sexual partners. The degree to which the information will cause public humiliation, stigmatization, lost employment, insurance problems, or loss of family and friends all contributes to it being identified as "sensitive." Records that contain information about socially or politically prominent persons have also been accorded special protections. Society is beginning to attribute special sensitivity to any and all health information. [Kunitz and Associates, Inc., 1995] (2) A label representing the security level of an object and describing the sensitivity of the data in the object. The label consists of two parts a hierarchical classification and a set of non-hierarchical categories or compartments. In systems supporting mandatory access controls, sensitivity labels determine whether a particular subject will be allowed to access a particular object. [O’Reilly, 1992]

**SERIAL:** Pertaining to data or instructions that are processed in sequence, one bit at a time, rather than in parallel (several bits at a time).

**SERIAL LINE INTERNET PROTOCOL (SLIP):** A means to operate IP over telephone lines or cables. It expands the connections of computers to network environments.

**SERVER:** A computer on a network that shares its resources, such as printers and files with other computers on the network. A component of a distributed computing system that provides a service in response to requests from clients. (See also CLIENT/SERVER).

**SHIELDED TWISTED-PAIR (STP) WIRE:** A type of wire that has a pair of wires twisted together and coated with an aluminum wrap for protection from external interference; depending on the intended use, STP can provide long-distance connections of up to 1,000 feet.

**SIMPLE MAIL TRANSFER PROTOCOL (SMTP):** The Internet standard protocol for transferring electronic mail messages from one computer to another.

**SMALL COMPUTER SYSTEM INTERFACE (SCSI):** A mechanical, electrical, and functional standard for connecting small computers with intelligent peripherals such as hard disks and CD-ROMS.

**SMART CARD:** An access card containing encoded information and sometimes a microprocessor and a user interface. The information on the code, or the information generated by the processor, is used to gain access to a facility or a computer system. [O'Reilly, 1992]

**SOFTWARE:** Instructions, or programs, that enable a computer to do useful work; contrasted with hardware, or the actual computer apparatus.

**SOFTWARE REENGINEERING:** The transformation from one level of abstraction to another; a process based on a usual design methodology, proceeding from requirements to a final product.

**SPECIAL INTEREST GROUP (SIG):** A subgroup of an organization or a computer networking systems consisting of members who share a common interest.

**SPOOF:** A trick that causes an authorized user to perform an action that violates system security or that gives away information to an intruder. [O'Reilly, 1992]

**SQL ACCESS GROUP (SAG):** A consortium of 42 leading systems and suppliers that include most suppliers in the relational database market. The group's mission is to solve the SQL RDBMS interoperability problems by developing a technical specification to enable multiple RDBMSs and application tools to work together.

**STANDARD GENERALIZED MARKUP LANGUAGE (SGML):** A standard that defines a language for document representation that formalizes markup and frees it of system and processing dependencies. It provides a coherent and unambiguous syntax for describing whatever a user chooses to identify within a document.

**STRONG AUTHENTICATION:** Authentication by means of cryptographically derived credentials. [ISO/IEC 9594- 8]

**STRUCTURED QUERY LANGUAGE (SQL):** A language set that defines a way of organizing and calling data in a computer database. SQL is becoming the standard for use in client/server databases.

**SWITCHED MULTIMEGABIT DATA SERVICE (SMDS):** A high-speed (up to 34Mbps), connectionless, packet switched MAN data service. It is considered a wideband/broadband data service and is designed to be easily integrated into user's existing local data communications and computing environments while having minimal impact on user's existing hardware and software.

**SYMMETRIC ENCRYPTION:** A form of crypto system in which encryption and decryption are performed using the same key. Also known as conventional encryption. [Stallings, 1995]

**SYMMETRIC KEY:** The key used in a symmetric ("secret-key") encryption system. In such systems, the same key is used for encryption and decryption. [CORBA Security Services, 1997]

**SYMMETRIC MULTI-PROCESSING (SMP):** A type of multiprocessing in which all CPUs are identical and in which any CPU can execute both user and kernel instructions.

**SYNCHRONOUS DATA LINK CONTROL (SDLC):** A data communications method, also known as digital.

**SYNCHRONOUS OPTICAL NETWORK (SONET):** A US high-speed fiber optic transport standard for a fiber optic digital hierarchy. It can operate at speeds ranging from 51.48Mbps to 2.5Gbps.

**SYSTEM SECURITY:** The result of all safeguards including hardware, software, personnel policies, information practice policies, disaster preparedness, and oversight of these components. [Institute of Medicine, 1994]

**SYSTEM SECURITY ADMINISTRATOR:** The person who controls access to computer systems by entering commands to perform such functions as assigning user access codes and privileges, revoking user access privileges, and setting file protection parameters. [CPRI, 1996c]

**SYSTEMS:** An interrelated set of entities which function in relation to each other, as in software systems, hardware systems, information systems, etc.

**SYSTEMS MANAGEMENT:** A set of processes that facilitates the use of and change to technical resources that deliver information services. These processes are performed by a combination of manual procedures and automated tools.

**SYSTEMS NETWORK ARCHITECTURE (SNA):** An architecture based on the use of microprocessors in each major device in a hardware configuration and the use of SDLC protocol.

---

*T*

---

**TAG IMAGE FILE FORMAT (TIFF):** A defacto standard format for image files.

**TASK:** A specific step or single item of work to be performed in the process of completing a project.

**TECHNICAL REFERENCE MODEL (TRM):** The document that provides a framework and common vocabulary to describe the information systems domain.

**TELECOMMUNICATIONS:** Systems of hardware and software used to carry voice, video, and/or data between locations. Includes telephone wires, satellite signals, cellular links, coaxial cable, etc., and related devices.

**TELECOMMUTING:** Use of electronic facilities to allow a worker to "commute" to work through communications networks rather than to physically travel to and from an office or work place.

**TELEPROCESSING:** Work completed on the computer via terminals or other remote devices through the use of telecommunications.

**TELNET:** The Internet standard protocol for remote terminal connection service. Telnet allows a user at one site to interact with a remote timesharing system at another site as if the user's terminal were connected directly to the remote computer.

**TERMINAL:** A device composed of a keyboard for putting data into a computer and a video screen or printer for receiving data from the computer.

**TERMINAL EMULATION:** Hardware and software that enables a PC or other intelligent device to act as a host terminal.

**TERMINAL SERVER:** A small, specialized, networked computer that connects many terminals to a LAN through one network connection. Any user on the network can then connect to various network hosts.

**THIN CLIENT TECHNOLOGY:** A networking environment in which dumb terminal workstations are set up, and a minicomputer or mainframe server controls many network functions. It is the opposite of fat client networking in which personal computers are used in a decentralized network environment.

**THREAT:** (1) An action or event that might prejudice security. [ITSEC] (2) A possible danger to a computer system. [O'Reilly, 1992] (3) The potential for exploitation of a vulnerability. [National Research Council, 1991]

**TOKEN:** (1) When used in the context of authentication, a physical device necessary for user identification. [National Research Council, 1991] (2) A physical item that's used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to gain access. [O'Reilly, 1992]

**TRANSMISSION CONTROL PROTOCOL/INTERNET PROTOCOL (TCP/IP):** The most common communication protocol for regional and national networks that links computers together on the Internet. The combination of a network and transport protocol developed by ARPANET for inter-networking IP-based networks.

## *U*

---

**UNIFIED MEDICAL LANGUAGE SYSTEM® (UMLS®):** UMLS helps health professionals and researchers retrieve and integrate electronic biomedical information from a variety of sources. It can be used to overcome variations in the way similar concepts are expressed in different sources. This makes it easier for users to link information from patient record systems, bibliographic databases, factual databases, expert systems, etc. The UMLS Metathesaurus contains mappings to MeSH (Medical Subject Headings at the National Library of Medicine), ICD-9-CM, SNOMED, CPT, and a number of other coding systems. The UMLS is not itself a standard; it is a cross-referenced collection of standards and other data and knowledge sources.

**UNIFIED MODELING LANGUAGE (UML):** A general-purpose notational language for specifying and visualizing complex software, especially large, object-oriented projects. UML builds on previous notational methods such as Booch, OMT, and OOSE. It is being developed under the auspices of the Open Management Group (OMG).

**UNIX:** A multi-tasking, multi-user operating system developed by AT&T Bell Laboratories in the 1960's that runs on a number of computing platforms. It consists of the kernel, the shell or interface, and the file system.

**UPLOAD:** The transferring of files, which reside on one computer to another computer via electronic communications.

**USER:** (1) A human being using the system to issue requests to objects in order to get them to perform functions in the system on his behalf. [CORBA Security Services, 1997] (2) A person or a process who accesses a computer system. [O'Reilly, 1992]

**USER NETWORK (USENET):** News groups distributed to computers and users over the Internet.

**UUCP:** An International, cooperative wide-area network that links thousands of UNIX computers in the United States, Europe, and Asia.

## V

---

### **VETERANS HEALTH INFORMATION SYSTEMS AND TECHNOLOGY**

**ARCHITECTURE (VistA):** A term used to describe the VA's health care information system. It encompasses in-house developed applications developed by VA staff (see Decentralized Hospital Computer Program), office automation applications, locally developed applications and commercial-off-the-shelf applications.

**VIDEO CONFERENCING:** In America, the term is fast becoming defined as any use of television to join people in some live interaction. However, the term is actually applied to a wide range of situations from live video lecturing to large audiences, to a point-to-point, individual-to-individual desktop PC chats. One possible categorization is into large scale and small scale. The majority of large-scale set-ups are currently satellite-based in the form of "interactive television," i.e., one-way video and two-way audio. This allows for broadcast from a central point to many different locations regardless of distance. Small scale refers to compressed video for meetings between relatively few points for

small meetings. A technology used for this function is ISDN. ISDN promises to make two-way video equally as cost effective, with potential for greater interactivity.

**VIRTUAL PRIVATE NETWORK (VPN):** A network that utilizes a public data network or the Internet as if it were a dedicated point-to-point network by implementing encryption and other security mechanisms across the network.

**VULNERABILITY:** (1) A security weakness due to failures in analysis, design, implementation or operation. [ITSEC] (2) A weakness in a system that can be exploited to violate the system's intended behavior. There may be security, integrity, availability, and other vulnerabilities. The act of exploiting a vulnerability represents a threat, which has an associated risk of being exploited. [National Research Council, 1991]

## W

---

**WEB BROWSER:** See Browser.

**WEB PAGE:** A set of data, image and text, written in HTML, and available on the World Wide Web via a web browser.

**WIDE AREA NETWORK (WAN):** A computer network which covers a geographically large area in which the transmission exchange is carried over telecommunication channels (e.g. telephone lines, satellites) provided by common carriers.

**WINDOWS:** GUI (Graphical User Interface): Developed by Microsoft Corporation for IBM compatible PCs.

**WORKFLOW:** The automation of work among users where the system is intelligent enough to act based on definition of work types, users, tasks and the recognition of dynamic processing conditions.

**WORKSTATION:** A powerful personal computer used in a client/server environment.

**WORLD WIDE WEB (WWW):** A hypertext-based system for finding and accessing Internet resources.

## X

---

**X3:** See National Committee for Information Technology Standards.

**X3L8:** A technical committee of X3 (X3 is now referred to as the National Committee for Information Technology Standards) responsible for developing standards on data representation. X3L8 is now referred to as NCITS L8.

**X12:** The ANSI X12 standards specify the format and data content of electronic business transactions.

**X.25:** An international standard for connecting computers or terminals to a network that operates by means of packet switching. This standard defines the interconnection of packet switching networks and their associated computers or terminals. These types of networks make efficient use of the telecommunications networks by taking the data generated by a computer or a remote terminal and chopping it up into small identified packets and then looking for the most efficient way of sending this information to its destination.

**X.75:** An international standard that provides for interconnections between data networks of different nations.

**X.400:** An electronic mail addressing and address directory control system established by the IEEE, designed to facilitate electronic mailing between otherwise independent data networks.

**X500:** a standard for distributed directory services. The standard encompasses both the structure of the X.500 database and also the protocol used in querying the database. X.500 can be used for different types of directories. Its most notable implementation is a global White Pages service containing in excess of a million names contributed to by X.500 servers in dozens of countries. X.500 provides a hierarchical database structure (e.g. country/organization/organizational unit/person). The database consists of entries (one per object) which may describe persons, network resources, organizations, etc., each with its own set of attributes.

**X.509:** An ITU-T recommendation that specifies a framework for the use of public key certificates and the authentication service for X.500 directories. The initial version of X.509 was published in 1988, version 2 was published in 1993, and version 3 was proposed in 1994 and considered for approval in 1995. Version 3 addresses some of the security concerns and limited flexibility that were issues in versions 1 and 2. X.509 also defines a syntax for certificate revocation lists (CRLs).

**APPENDIX C-ACRONYMS**

Acronym	Definition
<b>A/R</b>	Accounts Receivable
<b>AHCCCS</b>	Arizona Health Care Cost Containment System
<b>AI/AN</b>	American Indian/Alaska Native
<b>ANSI</b>	American National Standards Institute
<b>APA</b>	American Psychiatric Association
<b>API</b>	Application Program Interface
<b>ARMS</b>	Administrative Resource Management System
<b>ASC</b>	Accredited Standards Committee
<b>ASTM</b>	American Society for Testing and Materials
<b>ATHFNET</b>	Area to Health Facility Network
<b>ATM</b>	Asynchronous Transfer Mode
<b>B2B</b>	Business to Business
<b>BC/BS</b>	Blue Cross/Blue Shield
<b>CA</b>	Certificate Authority
<b>CAP</b>	College Of American Pathologists
<b>CBSE</b>	Component Based Software Engineering
<b>CCM</b>	CORBA Component Model
<b>CCOW</b>	Clinical Context Object Working Group
<b>CDC</b>	Center for Disease Control
<b>CDR</b>	Clinical Data Repository
<b>CFO</b>	Chief Financial Officer
<b>CHS</b>	Contract Health Services
<b>CIO</b>	Chief Information Officer

<b>CIRN</b>	Clinical Information Resource Network
<b>CIT</b>	Center for Information Technology
<b>CM</b>	Configuration Management
<b>CMM</b>	Capability Maturity Model
<b>COAS</b>	Clinical Observation Access Service
<b>COM</b>	Component Object Model
<b>COM+</b>	Component Object Model
<b>CORBA</b>	Common Object Request Broker Architecture
<b>COTS</b>	Commercial-Off-The-Shelf
<b>CPR</b>	Computerized Patient Record
<b>CPT</b>	Current Procedural Terminology
<b>CPRI</b>	Computerized Patient Record Institute
<b>CPRS</b>	Computer-based Patient Record System
<b>CPT</b>	Current Procedural Terminology
<b>CRIHB</b>	California Rural Indian Health Board
<b>CSA</b>	Common Service Architecture
<b>DBMS</b>	Database Management Systems
<b>DC</b>	Digital Certificate
<b>DCOM</b>	Distributed Component Object Model
<b>DCP</b>	Distributed CACHE Protocol
<b>DDP</b>	Distributed Data Protocol
<b>DES</b>	Digital Encryption Standard
<b>DHCP</b>	Decentralized Hospital Computer Program
<b>DHHS</b>	Department of Health and Human Services
<b>DICOM</b>	Digital Imaging and Communication in Medicine
<b>DIR</b>	Division of Information Resources

<b>DNS</b>	Domain Name Service
<b>DOD</b>	Department of Defense
<b>DSS</b>	Decision Support System
<b>DTD</b>	Document Type Definition
<b>DVA</b>	Department Veterans Affairs
<b>EBT</b>	Electronic Benefits Transfer
<b>EDI</b>	Electronic Data Interchange
<b>EDW</b>	Enterprise Data Warehouse
<b>EES</b>	Escrowed Encryption Standard
<b>EFT</b>	Electronic Funds Transfer
<b>EJB</b>	Enterprise Java Beans
<b>EMR</b>	Electronic Medical Record
<b>ERP</b>	Enterprise Resource Planning
<b>FASA</b>	Federal Streamlining Act
<b>FARA</b>	Federal Acquisition Reform Act
<b>FDMS</b>	Financial Data Management System
<b>FI</b>	Fiscal Intermediary
<b>FTP</b>	File Transfer Protocol
<b>GB</b>	Gigabyte
<b>GCPR</b>	Government Computer-based Patient Record
<b>GIOP</b>	General Inter-ORB Protocol
<b>GMRA</b>	Government Management Reform Act
<b>GOTS</b>	Government-Off-The-Shelf
<b>GPEA</b>	Government Paperwork Elimination Act
<b>GPRA</b>	Government Performance and Results Act
<b>GUI</b>	Graphical User Interface

<b>HCF</b>	Health Care Facility
<b>HCFA</b>	Health Care Financing Administration
<b>HEC</b>	Health Eligibility Center
<b>HHS</b>	Health and Human Services
<b>HII</b>	Health care Information Infrastructure
<b>HIPAA</b>	Health Insurance Portability and Accountability Act
<b>HL7</b>	Health Level 7
<b>HQ</b>	Headquarters
<b>HTML</b>	HyperText Markup Language
<b>HTTP</b>	HyperText Transfer Protocol
<b>HVHF</b>	High Volume Health Care Facility
<b>ICD</b>	International Classification of Diseases
<b>ICDR</b>	Interactive Clinical Data Repository
<b>ICMP</b>	Internet Control Message Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>IHDT</b>	Indian Health Design Team
<b>IHS</b>	Indian Health Services
<b>IHSNET</b>	IHS Network
<b>IIOP</b>	Internet Inter-ORB Protocol
<b>IOM</b>	Institute of Medicine
<b>IP</b>	Internet Protocol
<b>IRM</b>	Information Resource Management
<b>ISDN</b>	Integrated Services Digital Network
<b>ISO</b>	International Standards Organization
<b>IT</b>	Information Technology
<b>EA</b>	Enterprise Architecture

<b>ITMRA</b>	IT Management Reform Act of 1996
<b>ITSC</b>	Information Technology Support Center
<b>I/T/U</b>	IHS/Tribal/Urban
<b>JAD</b>	Joint Application Design
<b>LAN</b>	Local Area Network
<b>LAT</b>	Local Area Transport
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>LOINC</b>	Logical Observation Identifiers, Names, and Codes
<b>LVHF</b>	Low Volume Health Care Facility
<b>MDCA</b>	Microsoft's Distributed Component Architecture
<b>MFI</b>	Multi-Facility Integration
<b>MOF</b>	Meta Object Facility
<b>MOM</b>	Message Oriented Middleware
<b>MPI</b>	Master Person Index
<b>MS</b>	Microsoft
<b>MSCS</b>	Microsoft Cluster Server
<b>MS IE</b>	Microsoft Internet Explorer
<b>MS IE3</b>	Microsoft Internet Explorer (version 3)
<b>MS IIS</b>	Microsoft Internet Information Server
<b>MSMQ</b>	Microsoft Message Queuing
<b>MTS</b>	Microsoft Transaction Server
<b>MUMPS</b>	Massachusetts Utility Multi-Programming System
<b>MVR</b>	Master Veteran Record
<b>NCC</b>	Network Control Center
<b>NCHS</b>	National Center of Health Statistics
<b>NCITS</b>	National Committee on Information Technology Standards

<b>NDC</b>	National Drug Codes
<b>NIH</b>	National Institutes of Health
<b>NP</b>	National Program
<b>NPAD</b>	National Patient Administration Database
<b>NPCDB</b>	National Patient Care Database
<b>NPI</b>	National Provider Index
<b>NPIRS</b>	National Patient Information Reporting System
<b>NPS</b>	National Provider System
<b>O&amp;M</b>	Operations and Maintenance
<b>ODS</b>	Operational Data Store
<b>OIRA</b>	Office of Information and Regulatory Affairs
<b>OIRM</b>	Office of Information Resource Management
<b>OLAP</b>	On-line Analytical Processing
<b>OMB</b>	Office of Management and Budget
<b>OMG</b>	Object Management Group
<b>ORB</b>	Object Request Broker
<b>ORDBMS</b>	Object Relational Database Management System
<b>OS</b>	Operating System
<b>PCC</b>	Patient Care Component
<b>PDA</b>	Personal Digital Assistant
<b>PDD</b>	Presidential Decision Directive
<b>PIDS</b>	Patient Identification Service
<b>PKI</b>	Public Key Infrastructure
<b>PL</b>	Public Law
<b>PPP</b>	Point to Point Protocol
<b>PRA</b>	Patient Record Architecture

<b>PRA</b>	Paperwork Reduction Act
<b>RAD</b>	Rapid Application Development
<b>RAM</b>	Random Access Memory
<b>RDBMS</b>	Relational Database Management System
<b>RIM</b>	Reference Information Model
<b>RMON</b>	Remote Network Monitoring
<b>RPMS</b>	Resource Patient Management System
<b>RSA</b>	Rivest - Shamir - Adleman (encryption algorithm)
<b>RTF</b>	Rich Text Format
<b>SAF</b>	Security Architecture Framework
<b>SAMS</b>	Supply Administration Management System
<b>SAN</b>	Storage Area Network
<b>SCSI</b>	Small Computer System Interface
<b>SDLC</b>	Synchronous Data Link Control
<b>SEI</b>	Software Engineering Institute
<b>SGML</b>	Standard Generalized Markup Language
<b>SIG</b>	Special Interest Group
<b>SIGOBT</b>	Special Interest Group Object Brokering Technologies
<b>SLIP</b>	Serial Line Internet Protocol
<b>SMS</b>	Systems Management Servers
<b>SMTP</b>	Simple Mail Transfer Protocol
<b>SNA</b>	System Network Architecture
<b>SNMP</b>	Simple Network Management Protocol
<b>SQL</b>	Structured Query Language
<b>SSA</b>	Social Security Administration
<b>SSL</b>	Secure Socket Layer

<b>SSO</b>	Single Sign On
<b>TCP/IP</b>	Transfer Control Protocol/Internet Protocol
<b>TPB</b>	Third Party Billing
<b>TRM</b>	Technical Reference Model
<b>UML</b>	Unified Modeling Language
<b>UMLS</b>	Universal Medical Language System
<b>USDP</b>	United Software Development Process
<b>USHIK</b>	U.S. Health Information Knowledgebase
<b>VA</b>	Department of Veterans Affairs
<b>VBA</b>	Veterans Benefits Administration
<b>VHA</b>	Veterans Health Administration
<b>VISN</b>	Veterans Integrated Service Network
<b>VistA</b>	Veterans Health Administration Information Systems Technology Architecture
<b>VPN</b>	Virtual Private Network
<b>VTC</b>	Video Teleconferencing
<b>WAN</b>	Wide Area Network
<b>WAP</b>	Wireless Application Protocol
<b>WEB</b>	World Wide Web
<b>WML</b>	Wireless Markup Language
<b>WWW</b>	World Wide Web
<b>X12</b>	Identification number for ANSI standard specification for business data interchange
<b>XMI</b>	Extensible Metadata Interchange
<b>XML</b>	Extensible Markup Language
<b>KPA</b>	Key process area