

# The Health Insurance Portability and Accountability Act (HIPAA) of 1996

## OVERVIEW

*The Health Insurance Portability and Accountability Act (HIPAA) is a reality. The specifics of the standardized transaction sets and privacy have been completed and the formal regulations have been published with the other rules to soon follow. The regulations will impact healthcare in five major areas: standard transactions, standard code sets, uniform identifiers, security standards, and privacy standards. On the plus side, the required changes offer significant benefits through improved quality of claims, enhanced revenue collection, and reduced errors. To realize these benefits, the IHS must make a number of changes over the next two plus years.*

As passed by the United States Congress, HIPAA will institute administrative reforms that will be phased in over the period 2000—2003. Of major importance in the HIPAA legislation is the issue of data and transaction standardization- a mandate very few healthcare providers can sidestep.

There are five important aspects of HIPAA that healthcare providers must address to comply with the regulations and achieve the associated benefits.

- HIPAA mandates that all providers of healthcare and healthcare services adhere to standard electronic transaction formats for insurance eligibility, referrals, and claims billing in an effort to streamline electronic transactions and increase the portability of medical records.
- HIPAA requires the use of standardized code sets within the electronic transactions. These code sets, such as ICD-9 and CPT-4, are not new to healthcare; however, the requirement that all providers and payers use only standardized codes will simplify these transactions significantly.
- HIPAA will establish and require the use of unique identifiers for providers, plans, employers, and eventually individuals. These new identifiers will end the complete process where by each provider must maintain a table of ID numbers to process claims correctly. Under the new regulations, each provider, and each payer, will have one and only one unique identifier.
- HIPAA—along with NCQA and JCAHO—requires extensive security measures to be put in place to ensure the confidentiality of patient medical records. While applying only to information that is now or was previously in electronic format, the security standards dictate many changes in policies, procedures, and documentation, as well as requirements for security of desktop computers and networks.
- HIPAA establishes separate standards mandating the privacy of “individually identifiable patient information.” These standards limit the use of patient information, restrict its disclosure without a signed release, and establish a basic set of patient rights. These privacy standards establish a series of legal, contractual, and administrative challenges for healthcare organizations.

## Transactions Standards

Under the Transactions Standards, health plans must be able to reimburse providers, authorize services, certify referrals and coordinate benefits using a standard electronic format for each transaction. Providers should be able to check eligibility for coverage, verify claim status, request referrals or service authoriza-

tions and receive electronic remittance to post receivables. Coding standards for reporting diagnosis and procedures are included in the transaction standards. The transaction standards were published August 16, 2000 and the compliance date is October 16, 2002.

**Transactions Actions and Responsibilities**

Impact	Technical	Administrative	Program	When
RPMS 3 <sup>rd</sup> Party Billing	Transaction Standards		DIR	
Interfaces, Internal and External	Coding		DIR	
Compliance of Business Partners		Include compliance requirements in contracts	Contracting Office	
Business Process		Policy and Procedures	Business Office	
Recording diagnosis and treatment by clinical staff		Policy and Procedures	OPH/ Medical Records	
Awareness and Training		Training Programs	Personnel	

Note: Responsibilities lie at all levels of the program (HQ, Area and Facility).

Privacy Standards

The HIPAA Privacy Standards are intended to protect the privacy of all individually identifiable health information created or held by covered entities, regardless of whether it is or ever has been in electronic form. This includes paper records and oral communications. Covered entities (health plans, providers, clearinghouses) must maintain documentation of their policies and procedures for complying with the standards, and must include a statement of who has access to protected health information, how it is used within the covered entity, and when it would or would not be disclosed to other entities. Providers must obtain a patient’s consent for the disclosure or use of the patient’s health information, even for treatment, payment, and health care operations purposes. Covered entities must make a reasonable effort not to use or disclose more than the minimum amount of information necessary to accomplish the intended purpose of the use or disclosure, except when the information is used for purposes of treatment. An individual has a right of access to his or her protected health information, to request amending or correcting it, and to receive an accounting of all disclosures. The privacy standards were published December 28, 2000 and the compliance date is February 26, 2003.

## Privacy Actions and Responsibilities

Impact	Technical	Administrative	Program	When
RPMS and NPIRS	Restricted Use of Information, Disclosure History		DIR	
Authorization Controls		Authorization to Access Information	OPH	
Compliance of Business Partners		Chain of trust partner agreements	Contracting Office	
Business Process		Policy and Procedures	Business Office	
Determining minimum necessary information to disclose by clinical staff		Policy and Procedures	OPH/Medical Records	
Handling patient requests for restrictions or corrections		Policy and Procedures	OPH/Medical Records	
Awareness and Training		Training Programs	Personnel	

Note: Responsibilities lie at all levels of the program (HQ, Area and Facility).

## Security Standards

The HIPAA Security Standards must be applied by health plans, health care clearinghouses, and health care providers to all health information that is maintained or transmitted electronically. The standards are intended to protect both the system and the information it contains from unauthorized access and misuse. Each covered entity must assess its systems for potential risk and vulnerabilities to the health information it houses and develop, implement, and maintain appropriate security measures. The security requirements include:

- Administrative procedures – security measures to protect data and manage the conduct of personnel in protecting data
- Physical safeguards – protection of physical computer systems and related buildings from hazards and intrusion
- Technical security services – processes to protect, control, and monitor information access
- Technical security mechanisms – processes to prevent unauthorized access to data transmitted over a communications network

If an electronic signature is used for any transaction, the standards require that digital signature technology must be used.

### Security Actions and Responsibilities

Impact	Technical	Administrative	Program	When
Information Systems Security Controls (RPMS, NPIRS, other)	Access Controls, Encryption, Authentication and Audit		DIR	
Authorization Controls		Authorization to Access Information	OPH	
Compliance of Business Partners		Chain of trust partner agreements	Contracting Office	
Business Process		Policy and Procedures	Business Office	
Physical Security of Facilities		Policy and Procedures	OPH/ Facilities	
Physical Security of Computers and Communications		Policy and Procedures	DIR	
Personnel Security		Screening/Background Checks	Personnel	
Awareness and Training		Training Programs	Personnel	

Note: Responsibilities lie at all levels of the program (HQ, Area and Facility).

### Identifiers Standards

The HIPAA National Identifiers Standards will define standard national identifiers for employers, health care providers, health plans, and individuals to be used in certain electronic transactions (as defined in the HIPAA Transactions Standards). Covered entities (health plans, providers, and clearinghouses) must accept and transmit the standard identifiers when required in a standard electronic transaction. The national employer identifier proposed by HHS is the Employer Identification Number (EIN) issued by the Internal Revenue Service. The national health care provider identifier proposed by HHS is the National Provider Identifier (NPI), which is currently being developed and tested by HCFA. Standards for national health plan identifiers and individual identifiers have not yet been proposed by HHS.

## Identifiers Actions and Responsibilities

Impact	Technical	Administrative	Program	When
Information Systems (RPMS, NPIRS, others)	Implementing Identifiers Standards		DIR	
Interfaces, Internal and External	Coding		DIR	
Compliance of Business Partners		Include compliance requirements in contracts	Contracting Office	
Business Process		Policy and Procedures	Business Office	
Obtaining and Using Standard Identifiers		Policy and Procedures	OPH/ Medical Records	
Awareness and Training		Training Programs	Personnel	

Note: Responsibilities lie at all levels of the program (HQ, Area and Facility).

## COMPLIANCE COSTS VS. BENEFITS

Every Area Director should be concerned about the costs associated with HIPAA compliance, especially after the high cost of recent Year 2000 compliance efforts. While there will be significant costs associated with HIPAA, the good news is that there are also significant benefits to be achieved through implementation of the HIPAA reforms.

HIPAA is far more than just another series of government regulations to be satisfied. HIPAA is the catalyst that will propel healthcare into extensive use of electronic commerce. The benefits of these technologies have eluded the healthcare industry, due in no small part to a lack of industry wide standards. HIPAA resolves the standards issue and sets the stage for healthcare to move rapidly into e-commerce.

Electronic commerce and e-health are strategies that should continue to be rapidly implemented by the IHS. Much of the information transfer (most of healthcare is information transfer) will be subject to consolidation and or outsourcing over time. The IHS's ability to quickly seize upon e-health initiatives may be the difference between increasing third party collections or not being able to bill parties in the new Internet economy.

### Managing Costs

- Compliance with the new transaction standards, code sets, and identifiers may require upgrades to eligibility confirmation, coding, billing, and medical records applications. However these costs can be managed by taking a careful look at the organization's billing system.
- Meeting the new security standards will require a significant investment in policies, procedures, documentation, and training. **It is estimated that up to 80% of the impact on security will be**

**in these administrative areas, while only 20% will involve security technologies such as hardware or software.** The basic need for security has not changed. However, HIPAA requires healthcare organizations to invest extensively in security standards and technology. This emphasis may be new to many because the healthcare industry has often only paid lip service to security.

- The new privacy regulations will also impose a significant administrative burden on healthcare providers and payers. These regulations impose strict controls on what healthcare information can be released and to whom. Patients have new rights to limit access to their healthcare information. They also have rights to see their own records and challenge the accuracy of these records.

#### Achieving the Benefits

- A proactive approach to HIPAA compliance can provide ample opportunity to plan and systematically introduce the changes required by HIPAA.
- Using HIPAA to accelerate the adoption of e-health technologies offers significant benefits. Just as early adopters in most businesses and technologies accept risk, early adopters will share in rewards. The benefits or rewards that can be achieved through “first-in” status include incredible opportunities to increase third party collections.
- Business-to-business transactions will be more uniform and much easier to manage by the early adopter. Generating 3 to 5 second confirmations of insurance verifications via electronic transactions will significantly reduce the costs associated with inaccurate insurance information. Electronic submission of standardization claims to all payers will result in accelerated payments, reduced claims adjudication, and increased revenue.
- The move to electronic transactions also reduces the need to send paper copies of patient information via fax or mailed photocopies to physicians or payers. The use of this technology offers the potential for significant labor savings in medical records, clinical departments, and physician offices.

#### **APPROACH TO COMPLIANCE**

1. Build upon the experience and lessons learned from our success with Y2K.
2. Involve senior management from the beginning and appoint a senior management representative to coordinate the national HIPAA effort.
3. Use an interdisciplinary team approach
4. Determine what HIPAA means to the IHS and how much effort will be required to comply with it.
5. Start a nationwide awareness campaign at beginning of the compliance effort.
6. Consult with all stakeholders from the beginning to assure “buy in” at all levels of the I/T/U.
7. Use common sense when developing the strategy to comply with HIPAA.
8. To the extent possible use existing functional organizational structures and tools.

9. Develop a national compliance plan
10. Start the HIPAA compliance effort NOW and stay focused through routine progress briefings.

#### **NEXT STEPS**

1. The Team Leader must select key members of their HIPAA Compliance Team.
2. There needs to be a letter from the Director, IHS to the I/T/U informing them about what needs to be done to comply with HIPAA and what the IHS is doing in this arena.
3. There should be an Orientation meeting for the IHS HIPAA Compliance Team.
4. Involvement of the entire I/T/U needs to be accomplished.

## **Appendix**

1. Matrix HIPAA Rules and and program components responsible to carry them out.
2. Proposed HIPAA Compliance Team Members and gap analysis for HIPAA
3. Proposed methodology for the HIPAA compliance effort.

## **HIPAA Risk Assessment/Gap Analysis**

HIPAA-related changes will affect every information system and process that uses or collects patient data. To implement these significant changes in process, organization and staffing, service units should start now to educate all key stakeholders ramifications of the regulations and organize a HIPAA compliance program.

**I. Identify compliance leader and key staff to include in Task Force.** Consider the inherent HIPAA business opportunities as well as risk mitigation issues along with your organization's structure and culture. A well-structured compliance program can leverage HIPAA-related initiatives to achieve cost reductions through streamlined workflow, to improve cash flow and relationships with payors, and to advance an organization's e-business strategy. Recommendations for HIPAA steering committee membership are outlined below.

### **Executive Level Manager:**

Emerging HIPAA standards will have widespread implications for the entire healthcare organization. Although information technology is a major component of HIPAA compliance, HIPAA initiatives may be better managed as a strategic business issue rather than an IT issue. Engage a senior-level executive or manager to lead the HIPAA compliance effort. This should be a person who is well informed of the business issues and technology impacts associated with HIPAA compliance.

### **Chief Information Officer/Director IT Services:**

HIPAA will have a tremendous impact on existing technology, as well as require the consideration of new technology to effectively support a comprehensive compliance strategy. The involvement of the CIO is critical to successful HIPAA implementation efforts. However, keep in mind that HIPAA is not a technology issue any more than building a road is a bulldozer issue. The nature of the organization's business objectives should determine the appropriate set of tools chosen to support HIPAA and guide financial expenditures.

### **Health Information Management:**

HIM's involvement is essential to address the proposed standards on securing and maintaining the privacy of patient identifiable health information. Paper records as well as electronic media may well be covered in the final HIPAA rules.

### **Patient Financial Services:**

Patient financial management professionals must understand and guide the implementation of the new claims management-related transactions defined by HIPAA. These individuals can spearhead the redesign of their organization's revenue-cycle-processing, organizational, and customer-service models necessary to conform to HIPAA standards and to ensure productivity enhancements are achieved.

### **Human Resources:**

In crafting the HIPAA regulations, the Department of Health and Human Services recognized that organizations could simplify their administrative processes through the use of information technology and workflow changes. These changes will have far-reaching effects on employees in their job roles and job responsibilities. New HR policies and procedures will be required. HR

should play a significant role in guiding these changes to ensure employees understand compliance with HIPAA mandates.

**Risk Management:**

Underlying the standards is an intended set of actions. Risk identification, assessment and mitigation are imbedded in these actions. Results must be achieved and documented through policy and procedure development and implementation. For this reason, risk management should be a key player on the committee.

**Patient Registration:**

Patient registration professionals must understand and guide the implementation of processes to check eligibility of coverage and to gather an individual's personal information in a method that is confidential. These individuals can spearhead the redesign of their organization's patient entrance to the facility and customer-service models necessary to conform to HIPAA standards and to ensure productivity enhancements are achieved.

**Physician Representation:**

The privacy and confidentiality regulations, in particular, will drive changes in organizational culture with respect to the collection, transmittal, availability and storage of patient information. These changes may be especially challenging for healthcare providers to whom access to health information is highly valued and essential. Successful compliance with HIPAA regulations requires the cooperation and inclusion of physicians to address information accessibility and appropriateness.

**Clinical Departments:**

Many of the changes associated with HIPAA compliance will affect the day-to-day operations of major clinical departments and affiliates, including, but not limited to: nursing, pharmacy, radiology, surgery, respiratory, clinics, long-term care facilities and home health. It may be prohibitive to include representation from each area, but it's essential to the success of HIPAA initiatives to have key departments represented and/or individuals with the ability to articulate HIPAA implementation impacts on clinical operations.

**Facilities Management:**

HIPAA contains provisions for ensuring the physical safeguards of patient information. Facilities management (physical plant) representation is important within the committee composition to ensure compliance with these mandates.

**Education Department:**

Significant education—initially and ongoing—will be required to comply with HIPAA. Include a representative from the education department to ensure timely and accurate development of employee and patient education during implementation of HIPAA standards and ongoing. In addition to the above key committee membership, consider the following ad hoc representation.

**Chief Financial Officer:**

Consider having the CFO attend the committee meetings during times of key decision-making or when major milestones are approaching. This will help the CFO gain a better perspective of the financial realities associated with HIPAA compliance.

**Legal Counsel:**

Security and privacy regulations require numerous written policies, binding procedures, forms of agreements and contractual provisions. Legal counsel must be involved in developing these

documents. In addition, demonstrated compliance of legal counsel on the HIPAA team may mitigate penalties, if adverse events occur.

**Senior Executives/Board:**

Given the enterprise-wide impact of HIPAA, plus the potential personal liabilities in the event of an adverse event, regular status reporting to the board or an existing board committee should be encouraged.

**II. Identify information, business and clinical systems inventory**

- A. Inventory all information systems that contain or process healthcare information
- B. Designate staff member to report on each identified area(s).
- C. Identify all security/privacy policies, processes, procedures and practices

**III. Assess compliance levels, using the detailed inventory of all systems.** Verify and document all information, clinical, business and physical systems processes, policies, and procedures relative to:

- A. System security and functionality, and EDI, including:
  - Unique Identifiers
  - Electronic Signatures
  - Administrative Security processes and mechanisms
  - Physical Security processes and mechanisms
  - Technical Security processes and mechanisms.
- B. Third party transactions and relationships including:
  - Identifying all Standards Currently in Use
  - Potential Third Parties and current levels of HIPAA Compliance
  - Transaction Types
  - Details of Chain of Trust Agreements
- C. Code Set Standards for EDI, by
  - Medical data type and
  - Code sets now in use
- D. Contingency Planning for information systems
- E. Privacy, including
  - Use and disclosure of Health Data
  - Administrative requirements
  - Policies and procedures
  - Enforcement

**IV. Prepare final report, with details on specific areas of observed and potential risk.**

## **Proposed Approach to Complying to HIPAA Rules**

### **STEP 1 - AUDIT AND ASSESSMENT**

Determine current practices that must be changed to comply with HIPAA through analysis of current policies, procedures and IS technologies. This includes actual practices as they relate to day-to-day operations as demonstrated by the following *partial list* of areas covered.

#### Components of Initial Audit & Assessment

- Local and wide area networks security
- Data communications dial-up access
- Workstation access and controls
- Disaster recovery plan
- Audit procedures
- Current technical mechanisms
- IS security policy/procedures
- Internet/intranet access
- Physical access controls
- HR policy and procedures
- Data storage and disposal
- Training and awareness
- Current risk assessment of major applications and support system
- User security policy/procedures
- Contracts with business partners (chain of trust partner agreements)
- Internal business process
- Recording of diagnosis and treatment by clinical staff
- Billing procedures and codes used
- Privacy policy/procedures
- Physical security of computers and records
- Personnel security

### **STEP 2 - MANAGEMENT REVIEW**

Review the complete findings of the Audit and Risk Assessment with senior management, detail areas in need of remediation and determine priorities of remediation and implementation. Identify corporate goals and develop a project plan designed to attain those goals in an efficient and timely manner.

### **STEP 3 - DEVELOPMENT OF IHS HIPAA STRATEGY**

Design strategy to build HIPAA requirements into the day-to-day business practices of the organization. This includes the policies and procedures necessary to integrate controls of complex, cross functional departments such as IS, HR, Facility Management, Clinical Operations, Patient Care, Pharmacy, Billing Operations and Administrative Operations. Following is a *partial list* components covered..

#### Components of an Integrated IHS HIPAA Strategy

- Creating and updating policies
- Operating system controls

- Program change controls
- Disaster recovery planning
- Virus checking
- Disposal of information
- Single (Reduced) sign-on
- Employee education/awareness
- Asset and resource protection
- Documenting security/privacy standards
- Intrusion detection
- Network security/remote access
- Firewalls, encryption, active audit
- Termination procedures
- Unique user identification
- Web security
- Establish security committee
- Data Retention Policies (paper and electronic)
- Assure compliance of business partners
- Physical, personnel and network security

#### **STEP 4 -REMEDIAATION/IMPLEMENTATION**

Implementation consists of a project management team that works with senior management and staff to develop and implement the specific remediation appropriate for the organization and consistent with senior management business goals. A *partial list* of examples of policies that must be reviewed and modified to comply with HIPAA follows. The changes must be implemented.

##### Policy Development or revision

- Release of medical information
- Medical staff bylaws and procedures
- Alias policy
- Network access
- Deactivation of user id's
- Remote access
- Internet usage/e-mail
- Paper disposal-media controls
- AIDS and AIDS related conditions, etc.
- Physical access
- Employee education/awareness training
- Disciplinary action
- Departmental/operating system
- Non-employee access
- Intrusion detection
- Electronic signature
- Distribution of sign-on id's/passwords
- Software distribution - copying policy
- Disaster recovery planning
- Patient information access
- Physical security

- Personnel security
- Obtaining and use of standard identifiers
- Billing of third parties

#### Technology Implementation

- Access Controls - Designed to conform to corporate policy and direction, ranging from simple user id/password to role based definition, directory/file access, biometrics(fingerprint, retina, etc.) single sign on and others. All technology is implemented to ensure that people and systems have necessary access and utilize resources as they are authorized and intended to be used.
- Audit Controls - Provide controls, logs and regular reviews of how patient information is accessed and by whom. Audits must be at regular intervals and their findings must be documented.
- Physical Access - Area/environmental definition with installation of control mechanisms such as card entry systems and combination locks. All physical access controls are designed in conformance with organization policies developed to ensure that personnel have physical access to those areas of legitimate need, while preventing access to those without need.
- Internet/Intranet - Firewalls, encryption, digital certificates and other access mechanisms configured to support organization policies. Ensures that risk, access and delivery of Internet/Intranet content conform to senior management business directives.
- Intrusion Detection and On-Going Threat Analysis - Deployment of technology to ensure that attempts to circumvent security mechanisms are detected and to uncover any weaknesses prior to their exploitation. Provides continuing levels of risk, threat analysis and countermeasures.

#### **STEP 5 - PERIODIC FOLLOW-UP AUDIT & ASSESSMENT**

Follow-up audit and assessments are needed on a consistent basis to ensure that the IHS HIPAA Strategy is updated to accommodate changes in business process, industry standards and governmental regulations. This step ensures employee compliance to critical policies and procedures, provides a resource for on-going employee awareness training and provides methodology to accommodate technology changes. It also provides a continuing platform for maintenance and adjustment of policies and procedures to ensure practical conformance to business needs.