



RESOURCE AND PATIENT MANAGEMENT SYSTEM

e-Prescribing Productions

(BEPR)

Security Manual

Version 2.0
December 2013

Office of Information Technology (OIT)
Division of Information Resource Management
Albuquerque, New Mexico

Table of Contents

1.0	Introduction.....	1
2.0	Package Security.....	2
2.1	AC - Access Control	2
2.2	AT - Awareness and Training	2
2.3	AU - Audit and Accountability	3
2.4	CA - Certification, Accreditation, and Security Assessment.....	3
2.5	CM - Configuration Management.....	4
2.6	CP - Contingency Planning.....	5
2.7	IA - Identification and Authentication	5
2.8	IR - Incident Response	6
2.9	MA - System Maintenance.....	6
2.10	MP - Media Protection	6
2.11	PE - Physical and Environmental Protection	6
2.12	PL - Planning and Rules of Behavior.....	7
2.13	PS - Personnel Security.....	7
2.14	RA - Risk Assessment.....	7
2.15	SA - System and Services Acquisition.....	7
2.16	SC - System and Communications Protection.....	8
2.17	SI - System and Information Integrity.....	8
	Glossary.....	9
	Acronym List	10
	Contact Information	11

Preface

The purpose of this document is to provide technical security information about the IHS e-Prescribing (BEPR) package. The BEPR package is designed to pass HL7 messages from RPMS to a commercial pharmacy by way of the Surescripts® network. The package is used to facilitate the download of a file containing a listing of participating pharmacies. This is known as the Directory Download. The package is used to send and receive requests for an SPI (Surescripts® Provider Identifier) number from Surescripts,

Further definition of these terms is included in the Glossary.

1.0 Introduction

The Security categorization for this application is HIGH in accordance with FIPS 199. Security controls used in this application adhere to those outlined in the System Security Plan for RPMS (SSP 06-02) with specific details as follows in this document.

IHS e-Prescribing (BEPR) software is a component of the Indian Health Service (IHS) Resource and Patient Management System (RPMS). It provides facilities a mechanism for transmitting prescriptions electronically to third parties using HL7 messages routed through the IHS Central server and Surescripts®. See the main Technical Manual for package overview.

2.0 Package Security

This manual provides a package security plan detailing the specific security controls in place in this national software package. This section will not be included in any Freedom of Information Act (FOIA) request releases. Distribution of this section is limited to the ISC and OIT personnel. Since certain keys and authorizations must be delegated for proper management of the system, non-authorized personnel may find information about these items elsewhere in the technical and user manuals.

The Security categorization for this application is HIGH in accordance with FIPS 199. Security controls used in this application adhere to those outlined in the System Security Plan for RPMS (SSP 06-02) with specific details in the following subsections of this document.

2.1 AC - Access Control

RPMS end users do not have direct access to the BEPR application. The messages that are transported by this application may be viewed by IT personnel in the process of troubleshooting. The message content will ultimately be viewed indirectly by third party pharmacy staff including pharmacists, pharmacy technicians and clerks .

Site managers may have access to the Ensemble Management Portal which can be used to directly view message content. Access to Ensemble will be determinate on job duties and level of access should limit the user to a level needed to perform said duties.

Network communications between RPMS and outside applications are provided by Ensemble Web Services. This includes communicating with Surescripts and off site commercial pharmacies (only when the site is a part of the IHS HIE) and communicating with the Electronic Health Record (EHR) Graphical User Interface (GUI) if EHR version 1.1 Patch 9 is installed). All Web Services use SOAP 1.1/1.2 over HTTP with MTOM 1.0 as the communications protocols. The security of the BEPR HTTP-based WS traffic is ensured at the network level and is outside of the scope of this manual.

2.2 AT - Awareness and Training

The BEPR application contains patient healthcare data that is covered by Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), and other applicable privacy and confidentiality rules and regulations.

The only functionality for direct user access to HL7 messages that is provided is the Message Viewer available to site managers within the Ensemble Management Portal. Site managers who access the Ensemble Management Portal and view HL7 messages must be familiar with national, IHS, and local facility standard policies and procedures for handling confidential patient data both on screen and on related printed and saved materials. For users at federal facilities, this awareness is provided through annual Information Technology (IT) security, Privacy Act, and HIPAA training that is mandatory for all individuals with access to sensitive patient data.

2.3 AU - Audit and Accountability

The Ensemble Management Portal allows site managers to retrieve information about specific requests for BEPR data that come from the EHR GUI. The data elements available in the BEPR HL7 message are include the Encoding Characters, Sending Application, Sending Facility, Receiving Application, Receiving Facility, Date/Time Of Message, Message Type, Message Control ID, Processing ID, Version ID, Accept Acknowledgment Type, Application Acknowledgment Type, Patient Identifier List, Patient Name, Date/Time of Birth, Patient Address, SSN Number, Order Control, Placer Order Number, Quantity/Timing, Date/Time of Transaction, Entered By, Ordering Provider, Enterer's Location, Order Control Code Reason, Ordering Facility Name, Ordering Facility Phone Number, Ordering Provider Address, Requested Give Code, Requested Dosage Form, Provider's Pharmacy/Treatment Instructions, Provider's Administration Instructions, Allow Substitutions, Requested Dispense Code, Requested Dispense Amount, Requested Dispense Units, Number Of Refills, Pharmacy Name and Address, Pharmacy Phone Number, Route, Diagnosis Code, and Diagnosis Type,

HL7 message segments are stored in the ^Ens.MessageHeaderD, ^Ens.MessageHeaderI, ^EnsLib.H.MessageD, ^EnsHL7.Segment globals. These messages include new prescriptions, SPI requests, and Surescripts and pharmacy responses.

2.4 CA - Certification, Accreditation, and Security Assessment

IHS e-Prescribing has been certified as part of the RPMS NIST Meaningful Use certification. The package was also certified with EHR by Surescripts®.

IHS e-Prescribing is a component of the RPMS, and is therefore covered under the RPMS Certification and Accreditation (CA) and security assessments.

2.5 CM - Configuration Management

The IHS OIT RPMS program has formal Configuration Management (CM) and testing policies and procedures, as documented in the OIT Integrated Configuration Management Plan, November 2007 and in the draft RPMS Test Plan (April 2007). The CM Plan is included within the IHS Enterprise Performance Life Cycle to establish a consistent method for formally identifying and controlling project configuration items.

The e-Prescribing project adhered to the goals of the OIT CM Plan: (1) work products were identified, controlled, and available; (2) changes to configuration items were controlled; (3) selected work products that compose baselines at given points in time were identified; (4) integrity of baselines was maintained; (5) artifacts and deliverables (e.g., charter, concept, Project Management Plan [PMP], requirements, etc.) were tracked; and (6) accurate status and current specification data were provided to developers.

The RPMS program manager has identified Sharepoint (<http://workgroups.ihs.gov/sites/RPMS/default.aspx>) as the controlled repository for key artifacts of the RPMS software development process, including the project charter, PMP, and the baseline requirements report generated from the Serena® database tools.

The industry-standard tools identified by the Chief Information Officer (CIO) to document and manage RPMS requirements, including the problem report process and the change request process, are Serena® TeamTrack® and Serena® Dimensions® RM (see <http://www.serena.com/US/products/> for detailed information about the functions of these products). The e-Prescribing Project Team uses these tools to document all original functional and nonfunctional requirements; iterate requirements between the functional and development teams to resolve issues and baseline the requirements; document problem reports (PRs) to the development team during testing and subsequently document approval; and document change requests (CRs) and subsequently identify completed items.

Members of the OIT test team, two points of contact (POCs) from the development team, and one POC from the Software Quality Assurance (SQA) staff have access to the Serena® tools at various levels appropriate to their role in the CM process.

The processes for development testing at the unit, integration, and system levels are defined internally by the developers (Vangent, Inc.). The project Test Plan details the process to follow once the first software build is delivered to IHS for internal testing. Tracking of development tasks and Quality Assurance (QA) test process management for the developers was managed through an internal Issue Tracking system at Vangent, Inc. In addition, Vangent utilizes a source code control system to maintain a history of all changes related to the e-Prescribing software since its inception, including comments describing the change and a time-date-user stamp identifying the person making the change. The functional testers communicate PRs and CRs to the developers via Serena® tools, and the developers document their internal Issue Tracking system IDs for complete traceability. Changes to the e-Prescribing software will be released to IHS for testing in iterative builds that will be each independently tested and verified to ensure they addressed reported issues and that changes did not introduce new problems. See Section 2.15. The e-Prescribing test team will perform complete regression testing on all requirements at key stages in the testing process, including prior to the final release to SQA for final review and deployment.

2.6 CP - Contingency Planning

The e-Prescribing application is primarily a tool to transmit patient data stored within existing RPMS databases. It stores its configuration settings and the e-Prescribing production information in the RPMS database and does not require any special contingency planning (CP) outside of the normal backup/recovery strategies that are currently in place to protect RPMS data files.

As part of the e-Prescribing installation process, new Cache/Ensemble databases and namespaces are defined. The site manager will need to disable journaling for these new databases and add them to the list of databases that the facility backs up on a regular basis.

The e-Prescribing application does not store any data files on the client workstation computers.

It is recommended that in the event of transmission failures that the site reverts to written, telephoned or faxed prescriptions.

2.7 IA - Identification and Authentication

e-Prescribing orders coming from the EHR GUI are transmitted via asynchronous WS. These requests specify the patient identifiers and which Station Number the requested response message should be sent back to.

The site must have the site number registered with the National e-Prescribing Team and have that number added to the e-Prescribing site listing. The site must adhere to all rules and regulations for IHS e-Prescribing to remain active on this list.

The Provider is identified by the Surescripts Provider Identifier (SPI) after the site Credentialing Officer has confirmed and submitted the appropriate information to Surescripts. The SPI is a unique 13 digit number. A root of 10 digits is assigned to the Provider with an additional 3 digits delineating the location.

2.8 IR - Incident Response

In an incident response (IR) situation, RPMS site managers will be able to use messages stored in the Ensemble Message Viewer and Event Log to retrieve message information about specific requests for e-Prescribing messages coming from the EHR GUI.

In case of an IR situation involving e-Prescribing messages previously transmitted to the IHS HIE or that the site manager cannot locate, the site manager will contact the Help Desk, which will then access this information in the appropriate e-Prescribing messages.

2.9 MA - System Maintenance

There is no additional system maintenance (MA) required for this package.

2.10 MP - Media Protection

Local controls will be put in place according to IHS policy and the IHS General User Security Handbook.

The risk of exposing e-Prescribing related source control is not regarded as severe. The e-Prescribing software does not have any secret or confidential information embedded in it. *Any encrypted information is encrypted using industry standard encryption techniques.*

If the site manager chooses to print or save Windows screenshots of the HL7 message, this information should be considered in the same regard as other applications that allow displayed or printed access to patient information, e.g., Health Summary.

2.11 PE - Physical and Environmental Protection

Local controls are to be put in place according to IHS policy and the *IHS General User Security Handbook*.

2.12 PL - Planning and Rules of Behavior

This security manual is the System Security Plan for this application. The Rules of Behavior are to be found in this application's User Manual. For additional details, see the *RPMS Programming Standards and Conventions*, Section 8.2.6.7, "Rules of Behavior."

2.13 PS - Personnel Security

In accordance to the local security plan, controls are in place prior to allowing access to this application.

2.14 RA - Risk Assessment

The greatest risk to the e-Prescribing application is the same as any other RPMS components that display, print, or transmit patient data: the potential exposure of patient data to unauthorized or inappropriate user access. The following risks have been identified:

- Incorrect assignment of access to Ensemble Message Viewer, which will allow unauthorized personnel to access and view the HL7 messages that contain confidential patient data.
- Insecure network setup, which may allow unauthorized entities to request, receive, or intercept HL7 messages with confidential patient data.
- Failure to follow procedures for handling confidential patient data (e.g. leaving a printout of a HL7 message unattended) by the site manager with access to the Ensemble Message Viewer.

2.15 SA - System and Services Acquisition

The Software Development Life Cycle used to develop the e-Prescribing interface was the Enterprise Performance Cycle Framework (EPLC). All functional requirements for the e-Prescribing interface were reviewed and approved by IHS Subject Matter Experts (SMEs). All nonfunctional requirements were reviewed and approved by IHS OIT. Each software build was tested and reviewed by a Vangent, Inc. internal SQA team. Module-specific requirements, test cases and results of unit testing were delivered by Vangent, Inc. to IHS OIT at the end of the development cycle. The RPMS CM process, including the RPMS Test Plan, is more fully documented in Section 2.5 of this document.

2.16 SC - System and Communications Protection

Communication between the RPMS and the Local Ensemble production is done by placing and retrieving HL7 messages from the HLA and HLB global nodes. A TCP connection between the Local Ensemble production and the Central Ensemble production is made for delivery and receipt of HL7 messages. The Local Ensemble production retrieves a Directory Download file from the Central Ensemble production via Web Services, which are described in Section 2.1 in greater detail.

2.17 SI - System and Information Integrity

The e-Prescribing interface retrieves RPMS data, but doesn't add, edit, or delete records in the RPMS database. The e-Prescribing interface stores copies of HL7 messages generated in response to EHR GUI electronic prescription orders in the database for audit purposes. However, once these documents have been created, the e-Prescribing interface does not modify them.

Glossary

Health Level Seven (HL7)

HL7 specifies a number of flexible standards, guidelines, and methodologies by which various healthcare systems can communicate with each other. Such guidelines or data standards are a set of rules that allow information to be shared and processed in a uniform and consistent manner. These data standards are meant to allow healthcare organizations to easily share clinical information.

Acronym List

IHS

Indian Health Service

RPMS

Resource and Patient Management System

Contact Information

If you have any questions or comments regarding this distribution, please contact the OIT Help Desk (IHS).

Phone: (505) 248-4371 or (888) 830-7280 (toll free)

Fax: (505) 248-4363

Web: <http://www.ihs.gov/GeneralWeb/HelpCenter/Helpdesk/index.cfm>

Email: support@ihs.gov