TABLE OF CONTENTS

Chapter 23
Resource and Patient Management System Network

8-23.1 INTRODUCTION

A. Purpose. This chapter establishes Indian Health Service (IHS) policies and procedures that govern use of the IHS Resource and Patient Management System (RPMS) Network, hereafter referenced as the "Network." It includes guidance for IHS, Tribal, and Urban (I/T/U) health programs participating in the Master Patient Index (MPI), Health Information Exchange (HIE), Personal Health Record (PHR), RPMS DIRECT Messaging, and access to the eHealth Exchange (Exchange).

B. Background. The IHS is launching these new technologies and services to introduce a new era of patient engagement and HIE across the Indian health system through the Network, a suite of tools that enable I/T/U health programs to work cooperatively to improve the quality of patient care. The new features will improve access to essential health information at the point of patient care and provide new options for promoting health communications for patients and healthcare providers.

These tools address the requirements established by the Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) detailed in the 2014 Certified Electronic Health Record (EHR) rules that enable eligible healthcare providers and hospitals to achieve meaningful use. The Network enables actions such as: access to patient health information through the HIE for permitted purposes, patient access to their RPMS data through the PHR, and the ability for patients to send secure and encrypted emails to their healthcare team using the RPMS DIRECT email system. These services can improve the quality of patient care and increase patient satisfaction.

The Network is organized to facilitate Protected Health Information (PHI) access and sharing for treatment and related disclosures in a manner that complies with all applicable laws and regulations, including without limitation, those protecting the privacy and security of PHI.

C. Scope. This chapter applies to all IHS organizational components including but not limited to Headquarters, Area Offices, and service units conducting business for and on behalf of the IHS through contractual relationships when using IHS Information Technology (IT) resources. The policies contained in this chapter apply to all IHS IT activities including the equipment, procedures, and technologies that are employed in managing these activities. The policy includes teleworking, travel, other off-site locations, and all IHS office locations. Agency officials will apply this chapter to contractor personnel, interns, externs, students, and other non-Government employees by incorporating such reference in contracts or memorandums of agreement as conditions for using Government-provided IT resources.

D. Authorities.

(1) Federal Information Security Management Act of 2002, Public Law (Pub. L.) 107-347

(2) Health Information Technology for Economic and Clinical Health Act (HITECH), Title XIII of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5

(3) Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. 104-191, 45 Code of Federal Regulations (CFR) Parts 160 and 164

(4) Indian Health Care Improvement Act of the Patient Protection and Affordable Care Act of 2010, 25 United States Code (U.S.C.) Section 1662

(5) National Institute of Standards and Technology (NIST) Special Publication 800-73-3, "Interfaces for Personal Identity Verification – Part 1: End-Point Personal Identity Verification (PIV) Card Application Namespace, Data Model and Representation," February 2010

(6) Office of Management and Budget Circular A-130, "Management of Federal Information Resources"

(7) Privacy Act of 1974, as amended, Title 5 U.S.C. 552a, implemented by Title 5 CFR Part 5b

(8) REAL ID Act of 2005, Division B, Pub. L. 109-13

(9) X.509 Certificate Policy for The Federal Bridge Certification Authority (FBCA), Version 2.27, December 2, 2013

E. Acronyms.

(1) CA Certificate Authority

(2) CCD Continuity of Care Document

(3) CCDA Consolidated Clinical Document Architecture

(4) CEO Chief Executive Officer

(5) CFR Code of Federal Regulations

(6) CIO Chief Information Officer

(7) DPP Designated Primary Provider

(8) DQM Data Quality Manager

(9) EHR Electronic Health Record

(10) Exchange eHealth Exchange

(11) FBCA Federal Bridge Certification Authority

(12) HIE Health Information Exchange

(13) HIM Health Information Management

(14) HIPAA Health Insurance Portability and Accountability Act

(15) HISP Health Information Service Provider

(16) ITECH Health Information Technology for Economic and Clinical Health Act

(17) ID Identification

(18) IHS Indian Health Service

(19) IRT Incident Response Team

(20) ISSO Information Systems Security Officer

(21) IT Information Technology

(22) ITAC Information Technology Access Control

(23) I/T/U IHS/Tribal/Urban

(24) LoA Level of Assurance

(25) LoA 3 Level of Assurance 3

(26) MPA Multi-Purpose Agreement

(27) MPI Master Patient Index

(28) NIST National Institute of Standards and Technology

(29) OIT Office of Information Technology

(30) PHI Protected Health Information

(31) PHR Personal Health Record

(32) PII Personally Identifiable Information

(33) PIV Personal Identity Verification

(34) Pub. L. Public Law

(35) RA Registration Authority

(36) RPMS Resource and Patient Management System

(37) SU/FA Service Unit/Facility Administrator

(38) T/U Tribal/Urban

(39) U.S.C. United States Code

F. Definitions.

(1) Access Manager. A web-based MPI administrative application that allows MPI administrators to manage the application, user access, and user profiles based on their designated roles within the application.

(2) Breach. The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information.

(3) Continuity of Care Document. A document form that contains the clinical content using the Health Level 7 American National Standards

Institute's standard format for the transmission and exchange of clinical content. The Continuity of Care Document (CCD) and successor formats are based on the Consolidated Clinical Document Architecture (CCDA).

(4) Consolidated Clinical Document Architecture. A standard that provides a common architecture, coding, semantic framework, and markup language for the creation of electronic clinical documents.

(5) Data Quality Manager. A web-based MPI user application that allows users to view patient demographic data, and definitive and potential duplicates between patient records. Once duplicates are identified, the Data Quality Manager (DQM) allows users to merge or resolve the duplicate records and/or make corrections and enhancements based on designated roles within the application.

(6) eHealth Exchange. A set of standards, services, and policies that enables secure HIE over the Internet. The IHS HIE will provide a foundation for the exchange of health information between participating Indian health programs. The Exchange will broaden access across diverse entities across the country, helping to achieve the goals of the HITECH Act.

(7) Electronic Protected Health Information. Protected Health Information that is transmitted by "electronic media" or that is maintained in any form of electronic media (as that term is defined at 45 CFR § 160.103).

(8) Health Information Service Provider. An organization that provides services on the Internet to facilitate use of DIRECT messaging among

Providers. A Health Information Service Provider (HISP) is a logical concept that encompasses certain services that are required for DIRECT-mediated exchange, such as the management of trust between senders and receivers. A user typically agrees to allow the HISP to maintain a digital certificate on their behalf. Using this digital certificate, the HISP can securely send or receive DIRECT messages for the entity. The user initiates outgoing messages, and accesses incoming messages through the systems provided by the HISP, often through a secure e-mail web portal or a secure e-mail client software application.

(9) Health Insurance Portability and Accountability Act Privacy and Security Rules. Standards for Privacy and Security of Individually Identifiable Health Information at 45 CFR Parts 160, 162 and 164, as amended. The Privacy Rule provides Federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic PHI.

(10) Indian Health Service Active Directory. A collection of hosts and routers, and the interconnecting network(s), managed by a single administrative authority including the Federal D1 domain of IHS.

(11) Indian Health Service Health Information Exchange. A system that provides a service to collect, store, query, and retrieve patient health

summary information in the form of a CCD or successor format, exported from the IHS RPMS facilities or other healthcare systems meeting the interface requirements. The IHS HIE provides user access to summary medical record information from multiple Indian Health facilities utilizing RPMS databases and other eHealth Exchange communities from across the country.

(12) Indian Health System. The IHS and participating Tribal and Urban (T/U) programs.

(13) Level of Assurance. One's ability to determine, with some level of certainty that the electronic credential representing an entity (machine or human); can be trusted to belong to the entity. The NIST and FBCA outlines four Levels of Assurance (LoA) ranging in confidence level from low to very high, which is measured by the strength and rigor of the identity proofing process conducted by the Registration Authority (RA).

(14) Level of Assurance 3. One of the four identity authentication assurance levels used for e-government transactions. Individual vetted at LoA 3 provides high confidence in the asserted identity's validity. Credentials required are one Federal Government issued Picture Identification (ID), one REAL ID Act compliant picture ID, or two Non-Federal Government IDs, one of which shall be a photo ID (e.g., Non-REAL ID Act compliant Driver's License). Any credentials presented must be unexpired. REAL ID Act compliant IDs are identified by the presence of the Department of Homeland Security REAL ID star. See "X.509 Certificate Policy for the FBCA."

(15) Master Patient Index. Contains records for all the patients from all of the Indian health system facilities participating in the MPI. Each facility record belongs to an MPI record, which is created by the MPI. Two facility records that represent the same real-life person belong to the same MPI record. An MPI record contains its own set of patient demographics called the Single Best Record, which is calculated from the demographics data of its facility records. The MPI generates a unique patient ID for each MPI record. The MPI enables the HIE.

(16) Personal Health Record. A secure web application that enables verified patients to view their clinical information and use this information to interact with their medical team.

(17) Proactive Audit. An audit conducted on a regular basis for possible inappropriate use or activity. As an example, audit monitoring identifies user patterns and allows for access monitoring to evaluate and update user access accordingly.

(18) Protected Health Information. The term "Protected Health Information" and the abbreviation "PHI" shall have the same meaning as the term "protected health information" in 45 CFR § 160.103, limited to the individually identifiable health information received by a Business Associate from or on behalf of a Covered Entity. This term shall include Electronic PHI.

(19) Reactive Audit. An audit conducted in response to a request or to a triggered event, such as a complaint or breach in privacy or security.

(20) Retention of Audit Records. The required period that audit records are retained by a covered entity. Six years is the minimum period that

audit logs must be retained. Records retained for legal action or as otherwise needed for compliance activity may be retained longer than six years.

(21) Patient Auditing. Patients can view their PHR and secure messaging activities on the My Health Records (Home) page, according to the "Personal Health Record Web Portal User Manual."

(22) Resource and Patient Management System. Decentralized, integrated system for management of both clinical and administrative information in healthcare facilities that is managed and maintained by the IHS.

(23) RPMS DIRECT Messaging. A secure web-based messaging service intended for the exchange of patients' health information among healthcare providers and their patients and/or patients' personal representatives. RPMS DIRECT Messaging is HIPAA compliant and integrated with applicable systems, such as EHR and PHR, to provide an easy way for registered healthcare providers, healthcare organizations, patients, and patients' personal representatives to securely share Personally Identifiable Information (PII) and PHI electronically.

(24) Trusted Agent. An individual appointed on behalf of the RA to complete an in-person identity verification of the RPMS DIRECT users. The RPMS DIRECT Administrators and PHR Registrars will serve as Trusted Agents.

8-23.2 MASTER PATIENT INDEX DATA ACCESS AND SHARING

This section establishes the process for the Indian health system to participate in accessing and sharing data through the MPI application. The Indian health system

includes IHS and participating T/U programs. The MPI was designed to facilitate data exchange across the IHS enterprise thereby helping to improve patient access to care and provider access to patient information. Patient demographic data from RPMS systems across the country are interfaced to the central MPI database and will serve to link information for individual patients who receive care from multiple locations within the Indian health system. The MPI serves as the core infrastructure for HIE capabilities in IHS which integrates with other services such as the PHR, the National Data Warehouse, and the Exchange.

A. Policy. It is IHS policy that all patient data contained in the central MPI database will be accessible only by authorized users of the MPI and HIE. All MPI access and sharing of data shall comply with the HIPAA Privacy and Security Rules, Privacy Act, and all IHS policies related to privacy, security and data use:

(1) All IHS facilities are required to upload their patient demographic information into the central MPI database.

(2) All organizations that participate in the MPI will do so with the understanding that all patient data will be included in the central MPI database.

(3) There is no ability to exclude individual patient records from a given site whose data has been uploaded to the central MPI database.

B. Procedures. These procedures must be followed by all participating sites:

(1) All authorized MPI users will be required to complete orientation and training, and sign the IHS Rules of Behavior prior to using the MPI application.

(2) Participating T/U organizations will be required to enter into a Multi-Purpose Agreement (MPA) and agree to all terms. The MPA policies and procedures are not covered in this chapter.

(3) Access will not be granted until an approved/processed request to access the MPI has been submitted by the user's supervisor through:

a. The Information Technology Access Control (ITAC) System for users within an IHS facility; or

b. An IHS Help Desk ticket for users within T/U facilities.

(4) Authorized users are granted specific roles within the MPI by their supervisor/administrator at their local site. See Section 8-23.3, "Master Patient Index Users."

(5) All inappropriate or suspicious activity, such as incorrectly linked accounts (breaches), must be reported as follows:

a. All IHS facilities shall use the Incident Response Team (IRT) procedures for reporting contained in Part 8, Chapter 9, "Establishing an Incident Response Capability," *Indian Health Manual* (IHM), and local facility procedures.

b. The T/U facilities shall use their local breach procedures:

i. The local policies and procedures for audit must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and Information Systems Security Officer (ISSO) of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

8-23.3 MASTER PATIENT INDEX USERS - PROCEDURES

A. Scope. This section establishes the process for MPI administrators and users to access and manage the MPI application to establish unique identifiers to identify patients throughout the Indian health system. This system includes IHS and participating T/U health programs. The MPI contains records for all the patients from all of the Indian health system facilities participating in the MPI. Each facility record belongs to an MPI record, which is created by the MPI. Two facility records that represent the same real-life person belong to the same MPI record. An MPI record contains its own set of patient demographics called the Single Best Record, which is calculated from the demographics data of its facility records. The MPI generates a unique patient ID for each MPI record. The MPI enables the HIE.

B. Training. All of the participating Indian health system facilities are required to train MPI users prior to using the software. Staff responsible for managing multiple patient records shall have a thorough understanding prior to using the MPI application.

C. Procedures. The MPI application will be used to identify and verify potential duplicates and to link patient records using patient demographic data. The Health Information Management (HIM) and Patient Registration staff, where applicable, must be trained in the use of the application. It is important for sites to understand

the criticality of completing training and development of specific procedures to ensure accuracy in identifying, verifying, and linking electronic data. These procedures must be followed by all authorized users that have access to the MPI application:

(1) All authorized MPI users will be required to complete orientation and training, and sign the IHS Rules of Behavior prior to using the MPI.

(2) The MPI local administrator will authorize MPI application access within local facilities. See the "Master Patient Index User Manual."

(3) The MPI user shall query and verify potential duplicate patient records, and link patient records using patient demographic data.

(4) The MPI user shall also unlink patient records for potential wrong patient linkage. See Section 8-23.2.C(5) above for reporting potential breaches.

(5) The MPI user shall review and reconcile periodic duplicate patient reports.

(6) View Only users have query capability to identify potential multiple patient records and notify MPI users to reconcile the multiple records.

(7) It is highly recommended that HIM and Patient Registration staff, where applicable, be appointed as MPI users and MPI View Only users.

(8) Each participating Indian health system facility shall develop policies and procedures to ensure accuracy in identifying, verifying, linking, and unlinking electronic data.

8-23.4 ADMINISTRATOR ACCESS TO THE MASTER PATIENT INDEX SYSTEM

A. Scope. This section establishes the process for administrators' access to the IHS MPI system. For system and user management, MPI Administrators will be designated at three levels: National, Area, and Service Unit. These authorized administrators will manage system related functions, such as user management and audits, using the MPI system

B. Responsibilities. Authorized MPI Administrators shall manage and provide user access to the MPI system following the procedures contained in this chapter to ensure appropriate user access and monitoring of the MPI system. The IHM, Part 8, Chapter 12, "Information Technology Security," describes a full set of roles and responsibilities to which staff must adhere. This policy describes additional roles and responsibilities that are required for MPI.

(1) Chief Information Officer. The IHS Chief Information Officer (CIO) is the MPI system owner. The CIO will appoint the National Administrator(s) for the IHS MPI.

(2) MPI National Administrator will:

a. Be responsible for the MPI system, ongoing operation and maintenance, auditing, and assisting with MPI Area Administrators' onboarding, training, and support.

b. Have privileges to manage MPI Groups, Roles, and the Access Functions and Access Details for each role using the MPI Administrative application.

c. Be able to approve, deny, and update administrators' accounts.

(3) Area Directors. Each Area Director shall appoint an Area MPI Administrator.

(4) Area MPI Administrators will:

a. Work with the National Administrator and local Service Unit/Facility Administrators (SU/FA) to facilitate MPI onboarding for facilities within the Area Office.

b. Manage access, provide training, support, and perform required audits for SU/FA.

(5) Chief Executive Officer. The Chief Executive Officer (CEO) will appoint the local SU/FA.

(6) Service Unit/Facility Administrators will:

a. Work with their designated Area MPI Administrator to complete their facility MPI onboarding.

b. Manage user access, complete identity verification and provide role based access, conduct audits, and provide training for their local facility MPI Users, View Only Users, and administrators.

(7) MPI Users. MPI Users will have full user access to the MPI DQM tool to manage patient records and generate audit reports. Full access allows them to search and view patient records; to search and view potential duplicates; to compare patient data; to merge valid duplicate patient records; to un-merge patient records; to resolve or permanently resolve patient records; and to view audit history.

(8) MPI View Only Users. The MPI View Only Users will have limited DQM access to search and view patient records; to search and view potential duplicates; to compare patient data; and to view audit history.

C. Procedures. Authorized MPI Administrators must comply with appropriate MPI requirements, privacy and security laws, and the following MPI Administrator procedures:

(1) All T/U organizations will be required to enter into an MPA and agree to all terms, in order to have access to the MPI. The MPA policies and procedures are not covered in this chapter.

(2) All authorized MPI Administrators will be required to complete training and sign the IHS Rules of Behavior prior to using the MPI system. (See the "Master Patient Index Administrator Manual."

(3) The MPI Administrator access shall be requested, tracked, and updated using:

a. The ITAC System for administrators within an IHS facility; or

b. An IHS Help Desk ticket for administrators within T/U facilities.

(4) Only authorized MPI Administrators shall grant access to users and additional administrators for purposes defined under this policy and in accordance with Section 8-23.3, "Master Patient Index Users," above.

(5) The National MPI Administrator or designee shall facilitate Area Office onboarding.

(6) The Area MPI Administrators shall work with the National MPI Administrator and Area facilities to coordinate facility onboarding.

Area MPI Administrators shall manage access and training for the alternate Area MPI Administrator and local SU/FAs.

(7) The SU/FA shall:

a. Collaborate with the Area MPI Administrator for facility onboarding.

b. Work with the appropriate clinical manager to delegate MPI User and MPI View Only User role for the local facility.

c. Collaborate with local staff, such as the Clinical Application Coordinator, HIM Supervisor, or other appropriate staff to provide required training to MPI Users and View Only Users.

d. Grant and manage MPI access to local users, such as MPI User and MPI View Only User.

e. Provide support, to their local MPI Users and View Only Users.

(8) All MPI Administrators and users must have their identity verified before a unique username and default password is assigned.

(9) All designated MPI Administrators must utilize the appropriate method as stated below to manage and track assigning, reassigning, or terminating MPI user access:

a. Federal facilities must utilize the ITAC System.

b. The T/U administrators must develop and utilize internal policies and procedures to manage and track MPI account access for their MPI users.

(10) All supervisors must contact their MPI Administrator immediately, based on local policy, to update user access when a user resigns, is reassigned, or is terminated.

(11) The MPI Administrators must add, remove, or modify users' access in appropriate MPI applications and Active Directory (AD) groups according to valid requests.

(12) The MPI Administrators shall routinely monitor system activities by using audit functionality within the MPI application (see the "Master Patient Index Administrator Manual."

a. These audits may be reactive audits as requested by the local CEO, HIM staff, Privacy Officer, Security Officer, Compliance Officer, or other individuals that have legitimate need for the information to respond to patients' requests for accounting of disclosure, inquiries, breaches, and/or events.

b. Routine proactive audit reports that are recommended for user groups, include but are not limited to:

i. Type of activities performed by users.

ii. User status.

iii. Annual re-authorization evaluation for MPI administrators and users.

(13) Retention of audit records shall be maintained as follows:

a. Audit logs shall be stored for 90 days at the IHS Office of Information Technology (OIT).

b. Audit reports must be retained for a minimum of 6 years at each site.

(14) Administrators must report inappropriate or suspicious activities, such as misuse of the MPI system and PII as follows:

a. The IHS facilities shall use the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures.

b. The T/U facilities shall use their local breach procedures:

i. The local policies and procedures for auditing must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(15) Local facility MPI policies must be in place and enforced by management responsible for enforcement of privacy, security, and access to PHI. As an example, the Governing Body, CEO, HIM Supervisor, Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific MPI policies in their training, compliance and/or administrative policies. Any facility seeking designation of a SU/FA attests to having local policies that are subject

to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled to MPI.

8-23.5 ACCESS TO THE HEALTH INFORMATION EXCHANGE

A. Scope. Authorized users of the IHS HIE shall follow procedures for PHI though the use of the HIE web-based application. All data in the central IHS HIE database will be accessible by authorized users of the MPI and IHS HIE. This section establishes the procedures for Indian health system participation in accessing and sharing data over the IHS HIE and national Exchange provided by HealtheWay. The IHS HIE service will facilitate access to the Exchange through the IHS CONNECT gateway. The IHS HIE and Exchange will enable health information to follow the patient, be available for clinical decision-making, and support appropriate use of healthcare information to improve population health.

B. Central IHS HIE Database Procedures. All IHS facilities are required to upload their patients' CCDA information into the central IHS HIE database.

(1) All organizations that elect to participate in the IHS HIE will do so with the understanding that all patients will be included in the central IHS HIE database. There is no ability to exclude patient records from a given organization whose data has been uploaded to the central IHS HIE database. This means that within the Indian health system, data from all patients will be accessible to authorized users anywhere else in the System.

(2) Transmission of patient data outside the Indian health system via the Exchange is governed by patient choice. By default, patients are not included in the Exchange; however, patients may change their option at any time. Through the IHS HIE Patient Consent Module, patient

may elect to “opt-in” or “opt-out” of data sharing over the Exchange. IHS HIE authorized users will assist patients to “opt-in” or “opt-out” by using the Consumer Preference Module.

C. HIE Site Procedures. The following procedures must be followed by all sites participating in the HIE:

(1) The local CEO will designate an HIE SU/FA.

(2) Access will not be granted until an approved and processed request has been submitted by the user's supervisor through:

a. The ITAC System for HIE users within an IHS facility; or

b. An IHS Help Desk ticket for HIE users within T/U facilities.

(3) All authorized IHS HIE users will be required to complete orientation and training, and sign the IHS Rules of Behavior prior to using the IHS HIE.

(4) Healthcare providers, including physicians, dentists, nurse practitioners, physician assistants, medical assistants, and other healthcare professionals who access the IHS HIE are responsible for adhering to the “Agreement to Health Information Exchange Terms and Conditions” (see Exhibit 8-23-A).

(5) All participating I/T/U sites and their HIE users that access patient data through the Exchange must comply with the Exchange’s Data Use and Reciprocal Support Agreement.

(6) Federal sites are required to have the patient's authorization to use or to revoke the use of their information across the Exchange, by signing the IHS-810 Form, “Authorization for Use or Disclosure of Protected

Health Information" or other valid request. The form and guidance on its use can be found in the IHM, Part 2, Chapter 7, "HIPAA Privacy Rule and the Privacy Act," Section 2-7.7, "Procedure for Use or Disclosure of Health Information Pursuant to Authorization or Valid Written Request." An example of a completed IHS 810-Form is contained in the "Health Information Exchange User Manual."

(7) Tribal and Urban facilities will be required to enter into the MPA and agree to all terms. The MPA policies and procedures are not covered in this chapter.

(8) The SU/FA and users must report inappropriate or suspicious activities, such as misuse of the IHS HIE system and PHI/PII, as follows:

a. The IHS facilities shall use the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

b. The T/U facilities must notify IHS IRT in the event of an IHS HIE breach by e-mail at OITIncidentResponseTeam@ihs.gov in the event of a breach.

(9) Local facility HIE policies must be in place and enforced by management responsible for privacy, security, and access to PHI. As an example, the Governing Body, CEO, HIM Supervisor,

Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific IHS HIE access process policies in their training, compliance and/or administrative policies. Any facility seeking designation of a SU/FA attests to having local policies that are subject to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled from using the IHS HIE.

8-23.6 SECURITY AUDITING OF THE HEALTH INFORMATION EXCHANGE

A. Purpose. This section establishes the security auditing process for participants of the IHS HIE. All IHS HIE data will be accessible by authorized users of the IHS HIE. All HIE Administrators will follow procedures to regularly audit the IHS HIE to ensure appropriate use of the system.

B. Procedures. Authorized users that have access to the IHS HIE audit web application must follow these procedures:

(1) Only authorized users may be granted access to audit records through the IHS HIE audit web application.

(2) Administrator access to the IHS HIE audit web application will not be granted until an approved/processed request has been submitted by the user's supervisor through:

a. The ITAC System for administrators within an IHS facility; or

b. An IHS Help Desk ticket for administrators within T/U facilities.

(3) The HIE National Administrator or designee shall be granted the national audit administrator privileges with access to audit reports across all facilities participating in the HIE. This role is limited to

individuals that are IHS employees or their designees. These individuals will respond to audit report requests from the HIM Supervisor, Privacy Officer, Security Officer, Compliance Officer, and/or other appropriate staff.

(4) The Area HIE Administrator:

a. Shall be granted the national audit administrator privileges with access to audit logs across all facilities participating in the HIE.

b. Must query and run audits for facilities within their Area Office only.

(5) Facility CEOs will designate the HIE SU/FA

(6) Facility HIE SU/FAs:

a. Shall monitor system activities of local users.

b. Will request audit reports from the Area HIE Administrator via an IHS Help Desk ticket.

(7) All HIE Administrators must monitor system activities routinely using appropriate audit reports available within the IHS HIE audit web application. See the IHS "Health Information Exchange Administrator Manual." Routine proactive audit reports that must be executed or requested, but are not limited to, are listed below:

Table 8-23-A: Health Information Exchange Administrator Audit Reports

Report	**Headquarters**	**Area**	**Facility**	**Frequency (based on tier and activity)**
Type of records viewed by the user		X	X	Monthly
Type of Activity	X	X	X	Bi-Weekly; depends on tier and activity
Successful or failed authentication attempts	X	X	X	Weekly
User's status: Active, inactive, locked account	X	X	X	Daily
Monitor activity of staff for access to family records		X	X	Weekly
Access attempts, unauthorized attempts, compare current access vs. disabled access	X	X	X	Weekly
Monitor activities of Service Unit/Facility for compliance to audit policy	X	X	X	At least Annually
Monitor Administrators access to ensure disabled accounts for terminated and retired staff within 24 hours	X	X		Weekly
Locked out users report			X	Bi-weekly
Annual access review	X	X	X	Annually

(8) Area HIE Administrators shall provide reactive audit reports as requested by the SU/FA, CEO, HIM Supervisor, Privacy Officer, Security Officer, Compliance Officer or other individuals who have a legitimate need for the information for accounting of disclosure, inquiries, breaches, and/or other events.

(9) Retention of audit records shall be as follows:

a. Audit logs shall be stored for 90 days at IHS OIT.

b. Audit reports must be retained for a minimum of six (6) years at each site.

(10) All HIE Administrators must report inappropriate or suspicious activities, such as misuse of the IHS HIE system and PHI/PII, using the IHS IRT process and local facility procedures:

a. IHS facilities (IHS D1/AD Domain users) shall use the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures.

b. T/U facilities shall use their local breach procedures:

i. The local policies and procedures for audit must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(11) Local facility HIE policies must be in place and enforced by management responsible for enforcement of privacy, security, and access to PHI. As an example, the Governing Body, CEO, HIM Supervisor, Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific IHS HIE security audit

policies in their trainings, compliance and/or administrative policies. Any facility seeking designation of an HIE Administrator(s) attests to having local policies that are subject to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled to the IHS HIE.

8-23.7 PROCESSING PATIENT ACCESS TO THEIR PERSONAL HEALTH RECORD

A. Scope. This section establishes the process for patients to access and interact with their health information through a secure Internet IHS PHR application. The IHS PHR is intended to improve the overall health of patients by improving patient and provider collaboration, allowing patient self-management, and increasing patient access to health information. The IHS PHR provides a secure web-based application where patients can interact with their healthcare information from all medical facilities that utilize the RPMS and associated EHR. Additionally, patients will have access to health education, health assessments, and electronic services online. The IHS PHR registration process may be initiated at the patient's request at a facility that utilizes RPMS.

B. Procedures. Authorized users (PHR registrars and administrators) must follow procedures for validation of patient identity and grant or revoke access to the patient's PHI though the use of the PHR web-based application. The following procedures must be followed by all authorized users who have access to the PHR application:

(1) Only individuals who are authorized to administer access to the PHR application or to register patients may use the IHS PHR Administration application.

(2) All authorized IHS PHR users will be required to complete orientation and training, and to sign the IHS Rules of Behavior prior to using the IHS PHR.

(3) Access will not be granted until an approved/processed request has been submitted by the user's supervisor through:

a. The ITAC System for administrators within an IHS facility; or

b. An IHS Help Desk ticket for administrators within T/U facilities.

(4) All PHR users will be granted access based on their level of Administrator or Registrar responsibilities (see the "Personal Health Record Web Portal Administrator Manual") as follows:

a. The PHR National Administrator or designee shall be granted the PHR national administrator privileges to approve, deny, and update administrator accounts.

b. Each Area or respective Tribe will designate a PHR Administrator who will be granted privileges to approve, deny, and update SU/FA accounts.

c. Each Service Unit/Facility CEO will designate a PHR Administrator who will be granted local facility administrator privileges to approve, deny, and update local administrator and PHR registrar accounts.

d. Service Unit/Facility level PHR Registrars will be identified and assigned PHR privileges to perform the registrar functions. It is highly recommended that Registrars be identified from the

HIM Department due to their familiarity with release of information and role as custodian of the patient health record.

e. The PHR Registrar will perform the following key functions:

i. Work directly with patients in their request for a PHR account and registration process.

ii. Provide the patient with a copy of the Notice of Privacy Practices, as amended, which includes the PHR language.

iii. Link and unlink the patient PHR account to their patient health records.

iv. Verify identity of patients.

v. Create reports as requested by the Service Unit/Facility managers or supervisor.

vi. Update the patient's PHR access status field in the RPMS Patient Registration module. This is an important step that ensures Meaningful Use performance measures are met.

(5) All PHR Administrators and Registrars will be responsible for the following:

a. Responding to patient requests to reset their PHR password.

b. Disabling a patient's PHR account (See the "Personal Health Record Web Portal Administrator Manual"). In-person requests at the facility shall be in writing using the IHS-810 Form, "Authorization for Use or Disclosure of Protected Health

Information" [see Section 8-23.5C(5) above] or other written request. An example of a completed IHS-810 Form is contained in the "Personal Health Record Web Portal Administrator Manual" referenced above.

c. Providing a copy of the request with the disabled date to the patient. Once the account is disabled update the PHR access status field in the Patient Registration module.

d. Providing access to an un-emancipated minor's PHR account by following the IHM, Part 2, Chapter 7, "HIPAA Privacy Rule and the Privacy Act,"" Section 2.7-23, "Procedure for Access to or Disclosure of Protected Health Information of Unemancipated Minors."

e. Generating PHR reports to respond to queries, audits, incidents, investigations, and utilization. See "Auditing Process of the Personal Health Record," Section 8-23.8 below.

f. Disconnecting the patient's RPMS health record that is linked to an incorrect PHR account. The inappropriate linkage should be disconnected immediately by the local PHR registrar. Disassociation of the appropriate account in a timely fashion is of utmost importance. If the local PHR registrar is not available, the local PHR Administrator may perform the unlinking. If the local PHR Administrator is not available the Area PHR Administrator may perform the unlinking and if not available, the National PHR Administrator may perform this task. Further, the inappropriate linking of a PHR account to the wrong patient is considered a breach of confidentiality if the

PHR account has been viewed by the patient. These breaches shall be reported to the IRT and the immediate supervisor.

(6) All inappropriate or suspicious activity, such as incorrect linked accounts (breaches), must be reported as follows:

a. IHS facilities shall use the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures.

b. T/U facilities shall use their local breach procedures:

i. The local policies and procedures for audit must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(7) Facilities are strongly encouraged to work with their Area or local HIM consultants to develop specific procedures to ensure the accurate linking of patient records and to support the roles and responsibilities of PHR Administrators and Registrars.

8-23.8 AUDITING PROCESS OF THE PERSONAL HEALTH RECORD

A. Purpose. This section establishes the audit process for authorized users of the IHS PHR. Authorized PHR Administrators shall conduct audits and run reports on use of the IHS PHR through the PHR Administrator portal.

B. Procedures. All authorized PHR Administrators must follow procedures defined herein and in the "Personal Health Record Web Portal Administrator Manual" and in Section 8-23.7, "Processing Patient Access to their Personal Health Record," above.

(1) Only authorized PHR Administrators shall have access to "Create Reports" in the PHR Administrator portal for monitoring and auditing.

(2) The PHR Administrator portal access shall be requested, tracked, and updated using:

a. The ITAC System for administrators within an IHS facility; or

b. An IHS Help Desk ticket for the administrators within T/U facilities.

(3) The PHR National Administrator shall have privileges to run reports on all the users of the PHR portal and PHR Administrator portal. This role is limited to individuals who are IHS employees or their designees who have IHS-wide security responsibilities.

(4) Each Area Office shall designate an Administrator who shall monitor system level activities for their Area service units and facilities.

(5) The local CEO shall designate a SU/FA who shall monitor local facility system activities.

(6) Based on their level of privileges, the administrators shall monitor system activities using the audit function within the PHR Administrator portal (see the "Personal Health Record Web Portal Administrator Manual"). Routine audit reports include, but are not limited to the following:

Table 8-23-B: Personal Health Record Administrator Audit Reports

Report Type	Reports	National Admin	Area Office Admin	Service Unit/ Facility Admin	Frequency
PHR System Event Type	Successful or failed login attempts	X	X	X	Weekly
	User and facility record failure	X	X	X	Daily
	Successful and failed system event logging	X			Daily
	Service Problem: Master Patient Index (MPI) and Health Information Exchange (HIE)	X			Daily
Administrator Application Event Type	Monitor Administrator's access (i.e., Admin account creation, update, inactivation)	X	X	X	Monthly
	Patient Application process status (i.e. failed or successful)	X	X	X	Daily
	Patient unlink status (i.e. failed or successful)		X	X	Weekly
	Annual access review	X	X	X	Annually
Patient Application Event Type	Patient successful and failed activities (i.e., registration, information update, navigation, etc.)			X	Monthly
	Patient status: Active, inactive, locked account	X		X	Monthly

(7) Administrators shall provide reactive audit reports as requested by the local CEO, HIM Supervisor, Privacy Officer, Security Officer, Compliance Officer or other individuals who have a legitimate need

for the information for an accounting of disclosure, inquiries, breaches, and/or other events.

(8) Retention of audit records shall be maintained as follows:

a. Audit data shall be stored for six years by the OIT, IHS.

b. Audit records must be readily available for 90 days.

(9) Administrators must report inappropriate or suspicious activities, such as misuse of the PHI/PII under PHR, as follows:

a. IHS facilities shall use the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures.

b. The T/U facilities shall use their local breach procedures:

i. The local policies and procedures for audit must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(10) Local facility PHR policies must be in place and enforced by management responsible for enforcement of privacy, security, and access to the PHI. As an example, the Governing Body, CEO, HIM

Supervisor, Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific PHR audit process policies in their training, compliance and/or administrative policies. Any facility seeking designation of a SU/FA attests to having local policies that are subject to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled to PHR.

8-23.9 END USER ACCESS TO THE RPMS DIRECT MESSAGING SYSTEM.

This section establishes the process for healthcare providers, patients, and/or their personal representatives, within the Indian health system, to exchange PHI/PII in a secure, encrypted manner using the secure email messaging system known as the RPMS DIRECT. For additional responsibilities, see Section 8-23-10, "Administrator Access to the RPMS DIRECT Messaging System.

The IHS RPMS DIRECT is a secure, web-based messaging service, intended for the exchange of patients' health information between healthcare providers and their patients and/or their personal representatives. It is intended to eliminate and reduce the use of fax services or postal mail that involves the inherent risks of information being misplaced, compromised, or accessed by unauthorized users. The RPMS DIRECT is HIPAA compliant and integrated with applicable systems, such as EHR and PHR, to provide an easy way for registered healthcare providers, healthcare organizations, patients, and patients' personal representatives to securely share PHI/PII electronically.

The Indian health system healthcare providers must register for an RPMS DIRECT account at each facility where they provide care. For patients and/or their personal representatives, the PHR registration process will allow creation of an RPMS DIRECT account.

A. RPMS Direct Messaging System. The RPMS DIRECT will be utilized as a secure email system for various healthcare related communications, such as the following:

(1) To transition care.

(2) To ask medical questions.

(3) To make appointments.

(4) To request medication refill.

(5) To upload and send information.

B. Policy. The RPMS DIRECT is dedicated solely for the purpose of healthcare related exchanges among DIRECT participants only. All users of RPMS DIRECT must follow these requirements and standards when using the RPMS DIRECT. Tribal and Urban organizations must enter into the MPA to access RPMS DIRECT. The MPA policies and procedures are not covered in this chapter.

C. Responsibilities. The IHM, Part 8, Chapter 12, "Information Technology Security," describes a full set of rules and responsibilities to which staff must adhere. This section provides additional roles and responsibilities for implementation of RPMS DIRECT.

(1) Service Unit/Facility Administrator. The SU/FA is an individual(s) at a local facility responsible for granting access and performing responsibilities, as defined in the "Administrator Access to the RPMS DIRECT Messaging System," Section 8-23.10, related to identity vetting and making changes to authorized users RPMS DIRECT access.

(2) Message Agent. A Message Agent is an individual assigned to a patient or patient group to receive, distribute, and respond to secure messages on behalf of healthcare providers based on local policies and standards of patient care. The SU/FA will grant access to the Message Agent. Message Agents can be assigned to the patient or patient groups using the RPMS Designated Primary Provider (DPP) Package.

(3) Healthcare Provider. Healthcare providers include physicians, dentists, nurse practitioners, physician assistants, medical assistants, and other healthcare professionals who need to transmit and/or receive PHI/PII. Participating healthcare providers are responsible for adhering to the Agreement to RPMS Direct Messaging Terms and Conditions" (see Manual Exhibit 8-23-B).

(4) Patient. Participating patients are responsible for adhering to the "Agreement to the Personal Health Record Terms and Conditions," (See Manual Exhibit 8-23-C).

(5) Personal Representative. An individual authorized by the patient to access their PHI pursuant to an authorization or authorized by applicable law. Patients' personal representatives are also responsible for adhering to the "Agreement to the Personal Health Record Terms and Conditions" (see Manual Exhibit 8-23-C). For more information, see the IHM, Part 2, Chapter 7, "HIPAA Privacy Rule and the Privacy Act," Section 2.7-25, "Procedure for the Use and Disclosure of PHI for Emancipated Minors and Adults with Personal Representatives or Legal Guardians."

D. Procedures. All authorized users that have access to the RPMS DIRECT system must comply with appropriate IHS HISP requirements, privacy, and security laws, and the following RPMS DIRECT access procedures:

(1) All authorized RPMS DIRECT users will be required to complete orientation and training, and sign the IHS Rules of Behavior prior to using the RPMS DIRECT.

(2) Users must complete the RPMS DIRECT registration process by verification of identity being completed in person by the designated Trusted Agent. Provided are the security assurance levels required for the following users:

a. Healthcare providers and Message Agents must contact their local SU/FA and follow local procedures to complete the registration process. Healthcare providers and Message Agents require assurance at LoA 3.

i. Access will not be granted for IHS users until an approved/processed ITAC request has been submitted by the user's supervisor.

ii. Tribal and Urban healthcare providers and Message Agents must open an IHS Help Desk ticket to initiate access for RPMS DIRECT.

iii. Healthcare providers must provide a current, federally issued PIV card or two forms of valid ID, where at least one is a Government issued picture ID and the other is REAL ID Act compliant picture ID, such as a State driver's license, or State or Tribal ID card.

iv. Failure to complete identify vetting requirements will result in access not being granted to the RPMS DIRECT system. The designated SU/FA must verify identity information before granting a RPMS DIRECT account to healthcare providers and Message Agents.

b. Patients and/or their personal representative will have to complete the PHR registration process to gain access to RPMS DIRECT. See Section 8-23.7, "Processing Patient Access to their Personal Health Record."

(3) The SU/FA will assign a unique user name to each healthcare provider and Message Agent. The SU/FA must transmit passwords separate from the usernames when providing this information electronically. Healthcare providers and Message Agents must follow the RPMS DIRECT password and login requirements defined in the "RPMS DIRECT Messaging User Manual."

(4) Supervisors must submit ITAC requests and contact the SU/FA to remove the employee from RPMS DIRECT immediately when the user resigns, is reassigned or is terminated. See Section 8-23.10, "Administrator Access to the RPMS DIRECT Messaging System."

(5) Tribal and Urban SU/FAs must open an IHS Help Desk ticket to update and track RPMS DIRECT access for their healthcare providers and Message Agents.

(6) Users or their supervisors must notify the SU/FA to setup message forwarding during the user's absence.

(7) Activities of RPMS DIRECT users may be monitored, recorded, and subjected to auditing.

(8) The SU/FA must provide reactive audit reports as requested by the local CIO, HIM Supervisor, Privacy Officer, Security Officer, Compliance Officer or other individuals that have a legitimate need for the information to respond to patient's request for an accounting of disclosure, inquiries, breaches, and/or events.

(9) These reports may capture user level activities and data including but not limited to, username, user's full name, successful and failed login and log-out attempts, date and time of each activities, and origin of the activity.

(10) The SU/FA and users must report inappropriate or suspicious activities, such as misuse of the RPMS DIRECT system and PHI/PII, using the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(11) Local facility RPMS DIRECT policies must be in place and enforced by management responsible for enforcement of privacy, security, and access to PHI.

(12) The Supervisor, Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific RPMS DIRECT Audit Process policies in their training, compliance, and/or administrative

policies. Any facility seeking designation of a SU/FA attests to having local policies that are subject to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled to RPMS DIRECT.

(13) A request must be submitted to the SU/FA to establish a trust relationship to exchange secure messages with external healthcare organizations. See Section 8-23.10, "Administrator Access to the RPMS DIRECT Messaging System," for more information.

8-23.10 ADMINISTRATOR ACCESS TO THE RPMS DIRECT MESSAGING SYSTEM

A. Purpose. This section establishes the process for IHS RPMS DIRECT Messaging administrators within the Indian health system to manage the RPMS DIRECT system. The RPMS DIRECT is a secure, web-based messaging service, intended for the exchange of patients' health information between healthcare providers and their patients and/or their personal representatives, and among healthcare providers. The RPMS DIRECT administrator portal is a secure, web-based portal, designed to support administrative functions such as managing domains and user accounts, and for performing audits. The authorized administrative users include the National Administrators, Area Administrators, and SU/FAs. Authorized users of RPMS DIRECT may include Message Agents, healthcare providers, patients, and/or their personal representatives. Note that additional responsibilities are defined in Section 8-23.9, "End User Access to the RPMS DIRECT Messaging System." Authorized administrative users of RPMS DIRECT must adhere to the policies and procedures defined in this chapter, the "X.509 Certificate Policy for the Federal Bridge Certification Authority," and the "DigiCert "Certification Practices Statement."

B. Responsibilities. The IHM, Part 8 Chapter 12, "Information Technology Security," describes a full set of roles and responsibilities to which staff must adhere. This section describes additional roles and responsibilities that are required for RPMS DIRECT.

(1) Certificate Authority. An authority trusted by the IHS HISP for issuance and management of certificates. The Certificate Authority (CA) will be responsible for performing the following general functions:

a. Binding identities to cryptographic keys

b. Creating and signing both organizational and address bound certificates

c. Distributing certificates appropriately

d. Revoking certificates

e. Distributing certificate status information in the form of Certificate Revocation Lists

f. Providing a repository where certificates and certificate status information is stored and made available

(2) Registration Authority. The RA is an authority trusted by the IHS HISP that works in collaboration with the IHS trusted CA to collect and verify information of the certificate subjects, such as, RPMS DIRECT Administrators and PHR Registrars, and will evaluate to either approve or reject subscriber certificate management transactions including certificate renewal, re-key, and revocation requests.

(3) Chief Information Officer. The IHS CIO is designated as the RPMS DIRECT Messaging system owner. The IHS CIO shall approve the DirectTrust Framework and appoint the National Administrator(s) for the IHS HISP.

(4) National Administrator. The IHS National Administrator will:

a. Be responsible for the RPMS DIRECT system and system compliance.

b. Facilitate onboarding of the IHS HISP, I/T/U facilities and issuance of their certificates.

c. Be responsible for management and mapping of the organizational certificates and public and private keys.

d. Be a Trusted Agent appointed on behalf of the RA to complete identity vetting of Area Administrators and additional National Administrators.

e. Grant and manage RPMS DIRECT system access for Area Administrators and additional National Administrators.

f. Perform audits and manage maintenance, upgrades, accreditation, and re-accreditation of the RPMS DIRECT system.

(5) Area Administrator. The Area Administrator will:

a. Work directly with the CA to facilitate onboarding of I/T/U facilities and issuance of their organizational certificates.

b. Appoint local SU/FAs, grant access, and perform their identity vetting at LoA 3.

c. Manage domain names, Area audits, and RPMS DIRECT system access and trainings for SU/FA.

(6) Tribes. Tribes that have assumed Tier Two (Area level) support will have an individual assigned to an equivalent role as the Area Administrator.

(7) Service Unit/Facility Administrator. The SU/FAs shall appoint facility Message Agents. Local SU/FAs shall manage system access and complete identity vetting at LoA 3 for Message Agents, PHR Registrars, and healthcare providers. They shall manage message forwarding, run audits, and provide trainings for their local facility RPMS DIRECT users and local administrators. The SU/FAs shall work directly with the facility supervisors to update access for the local RPMS DIRECT users.

(8) PHR Registrar. The PHR Registrar shall manage RPMS DIRECT access for patients and/or their personal representatives. The PHR Registrars shall complete the identity vetting of the patients and/or their personal representatives in accordance with Section 8-23.7, "Processing Patient Access to their Personal Health Record."

(9) Message Agent. The Message Agent shall be a facilitator of the secure messages. They shall receive, distribute, and respond to secure messages on behalf of healthcare providers based on local policies and standards of patient care. Message Agents can be assigned to the patient or patient groups using the DPP package in the RPMS.

C. Procedures. Authorized users of the RPMS DIRECT system must comply with appropriate IHS HISP requirements, privacy and security laws, and the following RPMS DIRECT access procedures:

(1) Tribal and Urban organizations will be required to enter into the MPA and agree to all terms, in order to have access to the RPMS DIRECT. The MPA policies and procedures are not covered in this chapter.

(2) All authorized RPMS DIRECT users will be required to complete orientation, training, and sign the IHS Rules of Behavior prior to using the RPMS DIRECT.

(3) The RPMS DIRECT usage must be dedicated solely to the purposes of health related exchanges between authorized Federal and non-Federal healthcare providers, patients, patients' personal representatives, legal guardians, and other trusted external healthcare organizations. Under the IHS HISP, only authorized individuals shall have access to the RPMS DIRECT system. Only authorized administrators shall grant this access for purposes defined under the HIPAA policy and procedure at IHM, Part 2, Chapter 7, "Health Insurance Portability and Accountability Act - Privacy Rule and the Privacy Act."

(4) The National Administrator shall provide RPMS DIRECT system access and training and work directly with the CA and RA to do the following:

a. Facilitate onboarding

b. Work with facilities to determine implementation

c. Validate facility and domain

d. Issue the X.509 digital certificates for each facility, Area Administrators, SU/FA, and PHR Registrar

(5) The Area Administrators shall work with the CA, RA, National Administrator, and Area facilities to coordinate facility onboarding, such as sub-domain setup, issuance of the organizational certificates, and access and trainings for the alternate Area Administrator and SU/FAs within their Area.

(6) The SU/FA shall collaborate with Area Administrator for facility onboarding and:

a. Work with the appropriate clinical manager to delegate Message Agents and alternate Message Agents for the local facility.

b. Grant RPMS DIRECT access to local users, such as Message Agents and healthcare providers.

c. Collaborate with local staff, such as the Clinical Application Coordinator, HIM Supervisor, or other appropriate staff to provide required trainings to Message Agents, PHR Registrar, and healthcare providers.

d. Work with the appropriate clinical manager who will ensure that the Message Agent is assigned to the patient or group of patients using the DPP package in the RPMS.

e. Setup message forwarding for users during their absence.

(7) All RPMS DIRECT users must have their identity vetted at LoA 3 and be assigned a default password during initial registration. Users are

advised of the password reset process and required to change their password upon login. Passwords must meet password requirements defined in the "RPMS DIRECT Messaging User Manual."

(8) All designated RPMS DIRECT administrators must utilize the appropriate method below to manage and track assigning, reassigning, or resigning of the RPMS DIRECT account access:

a. The Federal facilities must utilize the ITAC system. More guidance can be found in the "IHS General User Security Handbook."

b. Tribal and Urban administrators must develop and utilize internal policies and procedures to manage and track RPMS DIRECT account access for their RPMS DIRECT users.

(9) All supervisors must contact RPMS DIRECT administrators immediately when the user resigns, is reassigned, or is terminated using local policies and procedures in place.

(10) All RPMS DIRECT administrators must add, delete, or modify users' access based upon requests submitted by supervisors.

(11) All RPMS DIRECT administrators shall routinely run and monitor system activities using appropriate audit reports or fields available within the RPMS DIRECT Messaging Administrator Application (see the "RPMS DIRECT Messaging Administrator Manual").

a. These audits may be reactive audits as requested by the local CEO, HIM Supervisor, Privacy Officer, Security Officer, Compliance Officer or other individuals that have legitimate

need for the information to respond to patient requests for accounting of disclosure, inquiries, breaches, and/or events.

b. Administrators may customize audit reports based on local needs.

c. Routine proactive audit reports that are recommended for administrators, but not limited to include:

Table 8-23-C: Routine RPMS DIRECT Administrator Audit Reports

Report	**National**	**Area**	**Facility**	**Frequency** (based on tier and activity)
Type of Activity				
Successful or failed authentication attempts	X	X	X	Weekly
User's status: Active, inactive, locked account	X	X	X	Weekly
Access attempts, unauthorized attempts, compare current access vs. disabled access	X	X	X	Weekly
Monitor activities of Area Service Unit/Facility for compliance to audit policy	X	X		At least Annually
Monitor Administrators access to ensure accounts disabled for terminated and retired staff within 24 hours	X	X	X	Weekly
Locked out users report			X	Bi-weekly
RPMS DIRECT users under each domain	X	X	X	Annually
Annual Re-authorization evaluation	X	X	X	Annually

(12) Retention of audit records shall be maintained as follows:

a. Audit logs shall be stored for 90 days at the OIT, IHS.

b. Audit reports must be retained for a minimum of 6 years at each site.

(13) All Administrators must report inappropriate or suspicious activities, such as misuse of the RPMS DIRECT and PHI/PII as follows:

a. IHS facilities shall use the IRT procedures for reporting contained in the IHM, Part 8, Chapter 9, "Establishing an Incident Response Capability," and local facility procedures.

b. T/U facilities shall use their local breach procedures.

i. The local policies and procedures for audit must comply with policies herein and HIPAA procedures for breach notification.

ii. The T/U facilities must notify the IHS IRT in case of a suspected breach by e-mail at OITIncidentResponseTeam@ihs.gov.

c. Additionally, local administrators shall advise the Area and/or local Privacy Officer and ISSO of the incident(s) and include them in the investigation, response, and any subsequent notification that is required by law.

(14) The IHS HISP must establish a trust relationship with external healthcare organizations to enable secure exchanges using DIRECT. To establish a trust relationship, designated administrators shall follow

procedures defined in all RPMS DIRECT policies and procedures including the following:

a. The SU/FA must open an IHS Help Desk ticket to notify Area and National Administrators to begin discussion with potential external DIRECT healthcare organizations and their HISP.

b. The external healthcare organization's HISP shall work with the National Administrator for onboarding with the same Trust Framework and Trust Bundle with which IHS is established.

c. Upon successful onboarding with the IHS established Trust Bundle, the National Administrator shall ensure secure exchange is enabled and the Trusted Community Partner (Healthcare Organization) list is updated.

(15) The SU/FA and PHR Registrar shall provide support, as appropriate, to their local healthcare providers and patients and/or their personal representatives, respectively.

(16) Local facility RPMS DIRECT policies must be in place and enforced by management responsible for enforcement of privacy, security, and access to PHI. As an example, the Governing Body, CEO, HIM Supervisor, Privacy/Security Officers and/or Compliance Officer will have established or incorporated specific RPMS DIRECT policies in their training, compliance and/or administrative policies. Any facility seeking designation of a SU/FA attests to having local policies that are subject to audit, and accepts responsibility for enforcing these policies, at risk of access being disabled to RPMS DIRECT.

Health Information Exchange Terms and Conditions

ALL Users of the Indian Health Service (IHS) Health Information Exchange (HIE) must agree to the following Terms and Conditions for participation:

(1) You are accessing the IHS HIE, a United States (U.S.) Government information system that contains sensitive patient health related information. This system includes (1) this computer, (2) related hardware, (3) software, (4) all computers connected to this network, (5) network services (including internet access), and (6) all devices and storage media attached to this network or to a computer on this network. This information system is provided for the use of authorized IHS HIE users only.

(2) All patient information viewed through the IHS HIE is strictly confidential and is subject to the protection of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and is subject to the Privacy Act of 1974, as amended (5 *United States Code* § 552a) and the security regulations promulgated pursuant to HIPAA.

(3) You may choose to print, save, or download information from your IHS HIE account to upload to the patients' medical record. You are advised to take actions to protect your patients' health information. When downloading and/or saving Protected Health Information/Personally Identifiable Information (PHI/PII) make sure action is performed on work computers only where the environment is secure and its hard-drive or other storage media is encrypted to HIPAA standards. Storage of the data must comply with applicable Federal law, Federal regulations, including HIPAA, and organizational security, privacy and Health Information Management (HIM) policies.

(4) Any computer used to access IHS HIE must have hard drive and other storage media encrypted to HIPAA standards. Make sure IHS HIE is accessed on work computers only where the environment is secure and its hard-drive is encrypted to HIPAA standards. Downloading and/or saving a Continuity of Care Document creates a file on this computer that other people may be able to see. Use caution if you are using a shared computer.

(5) THERE IS NO RIGHT OF PRIVACY IN THIS SYSTEM. Activities performed within the IHS HIE may be monitored, recorded, captured, and disclosed in any manner, by authorized personnel to facilitate protection against unauthorized access and to verify security procedures and operational security. Any unauthorized or improper use of the system and contained information is prohibited and subject to criminal and civil penalties, and revocation of IHS HIE access.

(6) By accessing the IHS HIE, you consent to the IHS HIE Terms and Conditions defined herein and in all applicable IHS HIE policies and procedures, and verify that you are authorized to access the IHS HIE using the unique user ID assigned to you.

Personal Health Record Terms and Conditions

ALL Users of the Indian Health Service (IHS) Personal Health Record (PHR) must agree to the following terms and conditions for participation:

(1) Summary. The IHS created an online website called the PHR. The PHR website is where you can view your health information. You can use it to send secure email messages to your health care team.

a. To access the PHR, you will need to create a username and password. You will enter your username and password every time you want to look at your PHR. You will have five chances to enter the correct username and password or you will be locked out. When you are done using the PHR you must log out. This prevents someone from getting into your account. You will be logged out of the PHR after 10 minutes of no activity.

b. The information in the PHR is to help you make better healthcare decisions. It is NOT intended to replace the advice of your doctor. Contact your medical facility if you see errors in your PHR.

c. The PHR account may be made on a patient's behalf (such as by a parent or guardian). You must read and click "accept" for the patient.

d. The IHS makes every effort to protect your privacy. Anyone who misuses your information may face criminal and civil penalties. The IHS does not sell or trade your personal information. The IHS may contact you regarding surveys, questionnaires, and polls, however you can choose not to participate and still use the PHR. You can also to close your PHR account at any time.

(2) Indian Health Service Privacy Policy. The PHR application is a computer system of the IHS. The computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized uses. The IHS computer systems may be monitored for all lawful purposes, such as ensuring that their use is authorized; managing the system; protecting against unauthorized access; and verifying security procedures; survivability; and operational security. During monitoring, information may be examined, recorded, copied, and used for authorized purposes.

(3) Privacy Act Warning.

a. You do not have to provide the personal information requested for IHS PHR registration, but if you do not, IHS will be unable to establish a PHR account for you. Your decision not to provide this information will not have any effect on any other benefits to which you may be entitled.

b. The IHS makes every effort to protect your privacy. Certain demographic information, such as your name, PHR username, date of birth, health record number or "Chart Number," gender, and zip code are collected to provide you access to the IHS PHR and is subject to the Privacy Act of 1974, as amended [5 *United States Code* (U.S.C.) § 552a]. Only authorized persons may use your information contained in the IHS PHR. Any unauthorized disclosure or misuse of your information may result in criminal and/or civil penalties. Any individual may file a civil action in a Federal District Court against IHS if the individual believes that IHS violated the Privacy Act.

c. For site management, information is collected for statistical and management purposes. The IHS PHR uses software programs to create anonymous, summary statistics, which are used for such purposes as assessing what IHS PHR information and services are useful to you and other users, determining technical design specifications, and identifying system performance or problem areas. For security purposes and to ensure that this service remains available to all users, IHS PHR employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement requests or investigations, no attempts are made to identify individual users, to link an individual user to data entered in IHS PHR, or to track an individual user's usage habits. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under Federal law.

(4) The Use of Cookies. The IHS PHR application does not use "persistent cookies" to retain information about users of the IHS PHR. The IHS prohibits the use of "persistent cookies," a type of web technology that collects user-identifying information over time and across different websites.

(5) Personal Health Records My Messaging. You may send and receive secure messages within your PHR. This account can only be used to communicate with your Indian

Health System health care team through the My Messaging Menu. You can download a log that has your message activity with your health care team through My Messaging.

(6) Personal E-mail Address. The IHS reserves the right to contact you via the e-mail address you provide regarding important system or account information, major changes planned for the IHS PHR or for other system-related needs. The IHS will only use your e-mail address to forward you materials on the information in which you have indicated interest. Your e-mail address may also be used to send you reminders for forgotten usernames. If you no longer wish to receive these emails you always have the ability at any time to opt out of the IHS PHR.

(7) Security of Information. At all times, security maintenance and administration is an essential element of website operation and maintenance. The IHS PHR has several levels of security to protect your information. When you type in your personal information, IHS PHR establishes a secure connection with your browser so your information is encrypted or scrambled for transmission and storage. In addition, these security levels comply with the Privacy Act of 1974 as amended (5 U.S.C. § 552a); the Health Insurance Portability and Accountability Act of 1996 Public Law (Pub. L.) 104-191, Aug 21, 1996,110 Stat.1936, 45 *Code of Federal Regulations* (CFR), Parts 160 and 164; and the Health Information Technology for Economic and Clinical Health Act (Pub. L. 111-5, Feb 17, 2009).

(8) Secure Socket Layer/Transport Layer Security. The Secure Socket Layer/Transport Layer Security (SSL/TLS) is a security protocol which provides a transmission level of encryption between the user's browser and the IHS PHR server machines. The SSL/TLS is a method for protecting an IHS PHR user's identification and password.

(9) Personal Responsibility for Personal Information. You have access to the information contained in your IHS PHR account and as such, have the ability to disclose information in this account to other individuals.

(10) Registration and Log In. To provide certain services such as enabling you to enter personal information, The IHS will require your username and password for identification. To view any medical information you have in the IHS system, the IHS will require verification of your identity.

(11) Password Protection. Your PHR account is password protected. You will have five chances to enter the correct password before you are locked out of the system. We strongly recommend that you do not share your password with anyone and that you

change your password on a regular basis. Exercise caution by securing your password. The IHS will never ask for your password in an unsolicited phone call, unsolicited e-mail, or by any other means.

(12) Logging Out. You must log out when you are finished accessing the password protected PHR. This prevents someone else from accessing your account if you leave or share the computer. If ten minutes of non-activity pass, the session will expire.

(13) Exit Site Notice. The IHS PHR has links to other organization's websites such as the National Library of Medicine to provide you with additional health information. Once you link to another site, you are subject to the privacy and security policy of the new site. The IHS is not responsible for content on other websites.

(14) Saving of Passwords by Browser on Public Computers. Many Internet browsers (such as Internet Explorer, Apple Safari, or Google Chrome) allow users to save username and passwords. When prompted by a browser to save your IHS PHR username and password, it is recommended that you decline this option. Saving username and passwords could potentially enable persons to gain access to your personal information.

(15) Surveys, Questionnaires, and Polls. The IHS PHR may use surveys, questionnaires and polls to facilitate feedback and input from our users. When you respond to surveys, questionnaires or polls related to our site, this information is collected only as anonymous, aggregated information and is used for statistical purposes. No survey, questionnaire or poll will ever ask you for your social security number or PHR password.

(16) Agreement and Disclaimers.

a. General Disclaimer.

i. The IHS provides this web portal subject to the following Terms and Conditions. You must agree to these Terms and Conditions to access the IHS PHR.

ii. The IHS PHR is an IHS web portal intended for use by the Indian Health System patients for viewing, retrieving, and storing personal health records. Establishing an IHS PHR account is intended for eligible Indian Health System beneficiaries, including American Indians and Alaskan Natives of the United States and their advocates. All site information resides on and transmits through protected Federal computer systems and networks. The IHS PHR has links to other organization's' websites to

provide you with additional health information or information services. Once you link to another site, you are subject to the privacy and security policy of the new site. The IHS is not responsible for content on other websites.

iii. IHS use and disclosure of your health information is limited as required by Federal law. The IHS only uses the specified information you provide as agreed to in these Terms and Conditions. The IHS does not sell, trade, or rent users' personal information. The IHS reserves the right to perform statistical analyses of user behavior and characteristics to measure interest in and use of the various areas of the site. The IHS may at times share aggregate information (i.e., anonymous, statistical data) about our users within the IHS for quality assurance audits and IHS PHR program administrative needs.

iv. The IHS acknowledges that privacy and security of your information matter to you. The IHS respects your privacy and has taken measures to provide appropriate levels of security to protect your personal information. Certain information about your account may be shared with authorized personnel to administer the IHS PHR program. The IHS protects the information you provide with security technology based on current computer industry standards, and applicable Federal guidelines.

b. Indian Health Service PHR and Your IHS Health Records. Any address or contact information you enter is used for system troubleshooting and related correspondence. Any updates you make to your contact information on the IHS PHR will not be submitted to IHS or updated in your IHS health records. To make corrections in your health record, you must contact the medical facility where you receive care to update your official health record. The IHS health record displayed in your PHR is an electronic copy of your official health record. Your health record that is stored at IHS health facilities remains the official, legal, and authoritative IHS health record.

c. The IHS PHR and Any Claim for Payment with the IHS. The PHR may not be used to notify IHS for purposes of Purchased and Referred Care (formerly Contract Health Service) eligibility, referrals, or questions. If you wish to file a claim or change your information for any reason, you must contact your local IHS health care facility.

d. Medical Disclaimer.

i. The information provided by the IHS PHR is based on your official health record at the time it was last updated from the facility. The health-related information and resources available through the IHS PHR are NOT intended to be used for or replace the advice of your doctor, your current medical diagnosis, or your current treatment. Seek advice from your physician or other qualified health care provider before starting new treatment, modifying your current treatment, or to ask questions about a medical condition or disease. The information provided by the IHS PHR is intended to help you and others make better healthcare decisions and take greater responsibility for your own health.

ii. Health care recommendations may change over time. Therefore, resources contained on the IHS PHR may become outdated and not current with accepted medical standards. Always consult a qualified healthcare professional with any questions or concerns you may have regarding your medical condition.

e. Your Obligations.

i. The IHS PHR is an IHS web portal intended for use by the Indian Health System patients to allow for the creation of accounts for viewing, retrieving, and storing information only, except as otherwise explicitly authorized. Your health information resides on and transmits through protected Federal computer systems and networks.

ii. Your use of the IHS PHR means you understand, accept and grant your unconditional consent for authorized IHS personnel to review and take action including, but not limited to, monitoring, auditing, inspecting, investigating, restricting access, tracking, sharing with authorized personnel, or any other authorized actions by authorized IHS and law enforcement personnel.

iii. If your PHR account reflects incorrect patient information you must contact your local facility.

iv. Threats, attempts, or actions to modify this system, deny access to the system, gain unauthorized access to data, breach system security or otherwise damage the system or data contained within is strictly

prohibited. These actions may result in criminal, civil, or administrative penalties resulting from violations of Federal laws including, but not limited to, 18 U.S.C. § 1030 (Fraud and Related Activity in Connection with Computers) and 18 U.S.C.§ 2701 (Unlawful Access to Stored Communications).

f. Printing. You may choose to print information from your PHR. If you do, you are advised to take actions to protect your health information. Once you print your personal information, the security of that information is your responsibility. Remember to check for documents on printers and destroy all health information you do not need.

g. Inactivating Your Account. You may choose to inactivate your IHS PHR account at any time. To do so you may send a secure PHR message or go to your local Indian Health System facility to inactivate your account. If you go to an IHS facility you will be asked to put your request in writing. Be aware that once inactivated, information from the account becomes immediately inaccessible and cannot be retrieved.

h. Agreement. By clicking "Accept" below, you acknowledge that you have read and agree to all of the terms and conditions above. If the PHR account is being created for an unemancipated minor, a parent, guardian, or individual acting in loco parentis must read and click "accept" on behalf of the unemancipated minor. You expressly acknowledge and agree that neither IHS or their suppliers are responsible for the results of your decisions resulting from the use of the service, including, but not limited to, your choosing to seek or not to seek professional medical care, or your choosing or not choosing to modify or terminate specific treatment based on the information provided by this online service. Further, you expressly acknowledge and agree that representatives from the IHS PHR program and the IHS may contact you regarding surveys, questionnaires, and polls. Your participation in questionnaires and polls is voluntary and not required in order for you to participate in IHS PHR.

i. Changes to PHR Terms and Conditions. The PHR Terms and Conditions may be revised. When IHS makes a change that affects the collection and use of your personal information, IHS will update and post the revised Terms and Conditions on the IHS PHR home page. Upon log-in you will be prompted to read and accept the new Terms and Conditions. You must accept the revised Terms and

Conditions to continue using your IHS PHR account. With regard to the PHR account of an unemancipated minor, a parent, guardian, or individual acting in loco parentis must accept the revised Terms and Conditions on behalf of the unemancipated minor. If you choose not to accept the Terms and Conditions you will not be allowed to complete your login.

RPMS DIRECT Messaging Terms and Conditions

ALL Users of the Indian Health Service (IHS) Resource Patient and Management System (RPMS) DIRECT Messaging System must agree to the following terms and conditions for participation:

(1) Indian Health Service Privacy Policy. The RPMS DIRECT is a secure email system of the IHS. This system, including all related equipment, networks, and network devices (specifically including Internet access) is available only for authorized use. The IHS may monitor this system for all lawful purposes, such as ensuring authorized use; managing the system; protecting against unauthorized access; verifying security procedures; survivability; and operational security. This information may be monitored, recorded, copied, and used for authorized purposes.

(2) Privacy Act Warning. The RPMS DIRECT registration and account setup requires collection of your personal information. The IHS will be unable to establish a RPMS DIRECT account without your personal information.

The IHS makes every effort to protect your privacy. For registration purposes: two (2) valid government picture IDs are required, and some demographic information may be collected in the system, such as your name, date of birth, credentials, zip code, and RPMS DIRECT username to provide you access to RPMS DIRECT. Collection of this information is subject to the Privacy Act of 1974, as amended [5 *United States Code* (U.S.C.) § 552a]. Only authorized persons may use your information contained in the RPMS DIRECT. Any unauthorized disclosure or misuse of your information may result in criminal and/or civil penalties. Any individual may file a civil action in a Federal District Court against IHS if the individual believes that IHS violated the Privacy Act.

For site management, information is collected for statistical and management purposes. RPMS DIRECT uses software programs to create anonymous, summary statistics, which are used for such purposes as assessing what RPMS DIRECT information and functions are useful to you and other users and identifying system performance or problem areas. For security purposes and to ensure that this service remains available to all users, IHS RPMS DIRECT employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigations and required audits, no other attempts are made to identify individual users or to track an individual user's usage habits. Unauthorized attempts to upload information or change information on or from this system are strictly prohibited and may be punishable under Federal law.

(3) The Use of Cookies. The RPMS DIRECT does not use "persistent cookies" to retain information about users of the RPMS DIRECT. The IHS prohibits the use of "persistent cookies," a type of web technology that collects user-identifying information over time and across different websites.

(4) RPMS DIRECT Messaging. You may send and/or receive secure messages using the RPMS DIRECT through your RPMS Electronic Health Record (EHR) or RPMS DIRECT web system. RPMS DIRECT will only send and receive messages from trusted DIRECT accounts. Your RPMS DIRECT account shall be used to exchange health related information with other healthcare providers, patients, and/or patients' personal representatives only.

Message Agents will monitor and respond to messages on behalf of healthcare providers, patients, and patients' personal representatives as appropriate.

(5) Alternate Email Address (Non-DIRECT email address). The IHS RPMS DIRECT reserves the right to contact you via the alternate email address regarding important system or account information, major changes planned for RPMS DIRECT, or for other system-related needs. The RPMS DIRECT is not responsible for any consequences resulting from RPMS DIRECT emails being blocked by your Internet service provider, spam-blocking software, or similar.

(6) Security of Information. Security maintenance and administration is an essential element of RPMS DIRECT system operation and maintenance. RPMS DIRECT has several levels of security to protect your information. When you type in your message, RPMS DIRECT establishes a secure connection with your browser so information is encrypted or scrambled for transmission and storage. In addition these security levels comply with the Privacy Act of 1974 as amended (5 U.S.C. § 552a); Health Insurance Portability and Accountability Act (HIIPAA) of 1996 Public Law (Pub. L.) 104-191, Aug 21, 1996,110 Stat.1936; 45 *Code of Federal Regulations*, Parts 160 and 164; and (2) Health Information Technology for Economic and Clinical Health Act (Pub. L. 111-5, Feb 17, 2009).

(7) Secure Socket Layer/Transport Layer Security. The Secure Socket Layer/Transport Layer Security (SSL/TLS) is a security protocol, which provides a transmission level of encryption between the user's browser and RPMS DIRECT server machines. The SSL/TLS is a method for protecting RPMS DIRECT user's identification and password.

(8) Personal Responsibilities. As an RPMS DIRECT user, you must handle and respond to the information received in the RPMS DIRECT account timely and appropriately in accordance with healthcare industry standards of patient care and your local policies.

Based on your professional judgment, significant health information exchanges will be shared and incorporated into the patient's RPMS EHR record. You take full responsibility for disclosing information in this account to other individuals as needed.

(9) Registration and Log In. To meet Meaningful Use performance measures, and to send and receive secure messages to other healthcare providers, patients, and patients' personal representatives, registration is required. To access RPMS DIRECT, the IHS will require identity verification during registration and login.

(10) Password Protection. Your RPMS DIRECT account is password protected. You will have four (4) chances to enter the correct password before the system locks your account. You will need to contact your system administrator for assistance to unlock your account. Your password will expire every sixty (60) days. You shall not share your password with anyone and must exercise caution by securing your password. The IHS will never ask for your password.

(11) Logging Out. You must log out when you are finished accessing the password protected RPMS DIRECT. This prevents someone else from accessing your account if you leave or share the computer. If ten minutes of non-activity pass, the session will expire.

(12) Saving of Passwords by Browser on all Computers. Many internet browsers (such as Internet Explorer, Apple Safari, or Google Chrome) allow users to save their usernames and passwords. When prompted by a browser to save your RPMS DIRECT username and password, you must decline this option. Saving your username and password could potentially enable anyone to gain unauthorized access to your account and your patients' health information.

(13) Surveys, Questionnaires, and Polls. The IHS may use surveys, questionnaires, and polls to facilitate feedback and input from RPMS DIRECT users. When you respond to surveys, questionnaires, or polls related to RPMS DIRECT, this information is collected anonymously. This aggregated information is used only for statistical purposes. No surveys, questionnaires, or polls will ever ask you for your personal information or RPMS DIRECT password.

(14) Agreement and Disclaimers to RPMS DIRECT Messaging Terms and Conditions.

a. General Disclaimer.

i. The IHS RPMS DIRECT is subject to the following Terms and Conditions and the RPMS DIRECT Messaging Privacy Policy. You must agree to these Terms and Conditions and the RPMS DIRECT Messaging Privacy Policy to access RPMS DIRECT.

ii. RPMS DIRECT is a secure email system. It is available for the Indian Health System healthcare providers, patients, and patients' personal representatives to send and receive healthcare related information between its participants and other trusted DIRECT partners. The Indian Health System is made up of the IHS, which is a Federal agency, and participating Tribal/Urban programs. Your RPMS DIRECT account is dedicated solely for healthcare related communications and must not be used for any other purposes. All information resides on and transmits through protected Federal computer systems and networks.

iii. Use and disclosure of your information is limited, as required by Federal law. The IHS only uses the specified information you provide as agreed to in these Terms and Conditions. The IHS does not sell, trade, or rent users personal information. The IHS reserves the right to perform statistical analyses and profiling of user behavior and characteristics to measure interest in and use of the various functions of the system. The IHS may at times share this aggregated information (i.e. anonymous statistical data) about our users within the Indian Health System for quality assurance audits and RPMS DIRECT administrative needs.

iv. The IHS acknowledges that privacy and security of your and your patients' information matters to you. The IHS has taken measures to provide appropriate levels of security to protect the information exchanged within the RPMS DIRECT. Certain information about your account may be shared with authorized personnel to administer RPMS DIRECT. The IHS protects the information you provide with security technology based on current computer industry standards, and applicable Federal guidelines.

b. Medical Disclaimer.

i. The RPMS DIRECT provides an additional method of communication between RPMS DIRECT users, patients, patient's personal representatives and other trusted partners. RPMS DIRECT does not replace face-to-face patient care communications. The information provided by RPMS DIRECT is to help you and patients with healthcare decisions. RPMS DIRECT is not used in the event of a medical emergency.

ii. The health-related information exchanged through the RPMS DIRECT is not part of the patients' RPMS EHR medical record unless incorporated into the RPMS EHR chart by the health care provider.

c. Your Obligations.

i. RPMS DIRECT is an IHS web system for Indian Health System participants to send and receive health-related information to other healthcare providers and to patients and/or their personal representatives. As a user, you must verify the DIRECT address of the recipient of your message. Your use of RPMS DIRECT means you understand, accept, and grant your consent to review and take action related to your system usage including, but not limited to monitoring, auditing, inspecting, investigating, restricting access, tracking, sharing with authorized personnel, or any other authorized actions by authorized Indian Health System and law enforcement personnel.

ii. Threats, attempts, or actions to modify this system, attempt to inappropriately share the data, deny access to the system, gain unauthorized access to data, breach system security, or otherwise damage the system or data contained within are strictly prohibited. These actions may result in criminal, civil, or administrative penalties resulting from violations of Federal laws including, but not limited to, 18 U.S.C. § 1030 (Fraud and Related Activity in Connection with Computers) and 18 U.S.C.§ 2701 (Unlawful Access to Stored Communications).

d. Printing, Saving, or Downloading Information. Documents containing Protected Health Information may only be viewed or stored on authorized, encrypted and secure devices, and must be deleted when no longer required. Storage of the data must comply with applicable Federal law, Federal regulations, including HIPAA,

and organizational security, privacy and Health Information Management policies.

e. Inactivating Your Account. To inactivate your RPMS DIRECT account, you must contact your supervisor and provide a written request. Be aware that once inactivated, information from the account becomes immediately inaccessible and cannot be retrieved by you.

f. Agreement. By logging in to RPMS DIRECT, you acknowledge that you have read and agreed to all of the Terms and Conditions stated herein. You expressly acknowledge and agree to take actions as defined in your local policies and in accordance with the industry standards of patient care. Further, you expressly acknowledge and agree that representatives from the RPMS DIRECT and the IHS may contact you regarding surveys, questionnaires, and polls. Your participation in questionnaires and polls is voluntary and not required in order for you to access RPMS DIRECT.

g. Changes to RPMS DIRECT Messaging Terms and Conditions and Privacy Policy. The RPMS DIRECT Terms and Conditions and Privacy Policy may be revised. When IHS makes a change that affects the information collected and use of the system, IHS will update and post the revised Terms and Conditions and Privacy Policy on the RPMS DIRECT login screen and on the RPMS DIRECT informational website. By logging in to the RPMS DIRECT system, you accept that you have read and acknowledged the new Terms and Conditions and Privacy Policy.