MU Meaningful Use

INDIAN HEALTH SERVICE

Improving the Quality of and Access to Care

Policies for Meaningful Use Data Sharing

March 19, 2014

Janice Chase, Acting Lead
HIM National Program, OIT/HQ

Agenda

- Patient Merge – On HOLD Status
- Master Patient Index (MPI)
- Health Information Exchange (HIE)
- National HealtheWay Network
- Personal Health Record
- RPMS DIRECT Messaging System
- Auditing Policy Requirements

Patient Merge

Patient Merge (PM) on HOLD as of 11-18-2013

- Dr. Hays, acting director and chief information officer, sent out a memo on 11-18-2013 to **halt** use of **Patient Merge** (BPM).
- Identified issue: the BPM can **merge Problem Lists improperly.**
- Identified issue: **Laboratory** data can be **merged improperly.**
- Impact for merging patient data will be evaluated with new version latter half of 2014.

MU Policy Workgroup Meeting

2/25-27/2014 Reviewed 12 DRAFT policies and related documents:

- PHR Terms and Conditions
- DIRECT Terms and Conditions
- Agreements

Master Patient Index User Policy

- Purpose: To establish a process for Master Patient Index (MPI) administrators and users to access and manage MPI applications to establish **unique ID** to identify patients throughout IHS and participating Tribal/Urban health programs (**Indian Health System).**
- Policy: All **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.

Master Patient Index User Policy (cont.)

- Procedure:
  - Local administrator will delegate MPI access.
  - MPI application user to **identify, verify, and link** potential duplicate patient records using patient demographic data.
  - Recommended that Health Information Management (**HIM**) and **Patient Registration** staff be **trained.**
    - Sites need to **understand the criticality** of completing training and **development** of specific **procedures** to ensure accuracy in identifying, verifying, and linking electronic data.
  - HIM supervisor is the custodian of patient records; it is highly recommended that HIM supervisors be accountable for MPI processes within facilities.

Policy for MPI Data Access/Sharing

- Purpose: To establish a process for the Indian Health System to participate in accessing and sharing data through the MPI.
- Policy: **All** data in the MPI database will be shared with authorized users of the MPI and HIE. **No** ability to **exclude** (“opt out”) patient **records** from a given site. This includes tribal and urban facilities that elect to participate.

Policy for MPI Data Access/Sharing (cont.)

- Procedure:
  - All sites **must** provide orientation and training prior to use.
  - Tribal and Urban organizations will be required to sign or amend an existing **I**nterconnection **S**ervice **A**greement, **B**usiness **A**ssociate **A**greement, and **End User** Agreement.
    - Sites not on D1/Active Directory must initiate user access through Area or HQ Help Desk ticket.
  - Federal user access granted through Information Technology Access Control (ITAC) request.

Policy for Access to the Health Information Exchange (HIE)

- HIE definition: The Indian Health Service (IHS) **HIE** is an application that provides a **service** to collect and store **patient health summary** information in the form of a Continuity of Care Document (CCD). The HIE provides user access to summary health record information from **multiple** Indian health **facilities** utilizing RPMS databases from across the country.

Policy for Access to the HIE

- HIE application: The HIE Consumer Preferences provides system users with a mechanism to update individual patient preference specifying “opt-in” or “opt-out” of having their data shared over the “Exchange.”
  - HIE service allows access to the “Exchange.” The 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**.

Policy for Access to the HIE (cont.)

- Policy: It is IHS policy that all data in the HIE database will be shared with authorized users who will follow procedures for protected health information (**PHI**).
  - IHS facilities are **required** to **upload** their patient **CCD** information.
  - **Tribal** and **Urban** facilities **participate** understanding that **all patients** will be included in the HIE database.
  - HIE users **help** patients "**opt-in**" or "opt-out" of data sharing over the "Exchange" via the Patient Consent module. By **default,** patients **are not** in the "Exchange."
  - **IHS** patients must sign the **IHS-810** form, Authorization for Use or Disclosure of Protected Health Information.

Policy for Access to the HIE (more)

Procedures:

- **Federal** users need to **complete** the Information Technology Access Control (**ITAC**) access request.
- Tribal and Urban facilities must sign or amend an existing **I**nterconnection **S**ervice **A**greement, **B**usiness **A**ssociate **A**greement, and HIE **End-User Agreement.**
  - Initiate access through Area or HQ Help Desk ticket.
- Provide orientation and training.
- Comply with the Indian Health Service DURSA.
- Report all inappropriate or suspicious activity using the Incident Response Team (IRT) procedures.

What is the DURSA?

"The **D**ata **U**se and **R**eciprocal **S**upport **A**greement is the legal, multi-party trust agreement that is entered voluntarily by all **entities**, organizations and federal agencies that desire **to engage** in electronic **h**ealth **i**nformation **e**xchange with each other using an **agreed** upon set of national **standards**, **services** and **policies** developed in coordination with the Office of the National Coordinator for Health IT (ONC)," U.S. Department of Health and Human Services.

For more information: http://www.nationalehealth.org/dursa

What is the DURSA? (cont.)

The DURSA is based upon:

- Existing federal, state, and local laws applicable to the **privacy** and **security** of health information.
- Current policy framework for health information exchange.

The DURSA is intended to be a legally enforceable contract that represents a framework for broad-based information exchange among a set of **trusted** entities.

Indian Health Service has a **signed DURSA** with the national eHealth **Exchange**.

Policy for Access to the eHealth Exchange Connect Gateway

Background: The Nationwide Health Information Network, now the eHealth **Exchange**, advances health information exchange between **federal** agencies and **non-federal** entities to **support** quality and efficient health care, required by Executive Order 13410:

> "Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs."

IHS HIE will interface with the Exchange which includes the MPI and Patient Consumer Preferences for consent.

Policy for Access to the eHealth Exchange Connect Gateway (cont.)

- Purpose: To establish a policy on the process for Tribal health programs and Urban Indian organizations to participate in accessing and sharing data over the eHealth Exchange Connect Gateway.
- Policy: Authorized users of the Exchange must **follow procedures** for protected health information (PHI). Data in the HIE database can be queried and shared with authorized users.

Policy for Access to the eHealth Exchange Connect Gateway (cont.)

Procedures:

- Required to sign or amend an existing **I**nterconnection **S**ervice **A**greement, **B**usiness **A**ssociate **A**greement, and **End-User Agreement.**
  - Initiate access through Area or HQ Help Desk ticket.
- Provide orientation and training prior to use.
- Report inappropriate or suspicious activity to the Incident Response Team (IRT).
- Sign a participant agreement.

Policy for Access to the eHealth Exchange Connect Gateway (cont.)

Procedures:

- Under the DURSA, signed by the Indian Health Service (IHS), each participant executes a valid and enforceable agreement with each of its participant users in order to access the eHealth Exchange "Exchange" Connect Gateway.
- Requirements for Participant Users:
  - Comply with all applicable federal and state laws.

Policy for Access to the eHealth Exchange Connect Gateway (cont.)

Requirements for Participant Users (cont.)

- Comply with all applicable provisions of the **DURSA.**
- Submit a Message through the "Exchange" only for **Permitted Purposes.**
- Use Message Content received through the "Exchange" in accordance with the **terms and conditions** of the DURSA.
- As soon as reasonably practicable after determining that a breach occurred, **report** such **breach** to the participant.
- **Refrain** from disclosing to **any** other person any **passwords** or other **security measures** issued to the participant user by the participant.

Policy for Processing Patient Access to their Personal Health Record

IHS Personal Health Record (PHR):

- A secure web-based application for patients to interact with their healthcare information and providers.
- The IHS PHR is accessible to any patient who receives care at a facility that utilizes Resource and Patient Management System (RPMS).
- IHS PHR registration process will be initiated at the patient's request.

Policy for Processing Patient Access to their Personal Health Record (cont.)

POLICY: It is IHS policy that authorized users, (PHR registrars and administrators) follow procedures for **validation** of **patient identity** and to grant or revoke access to their protected health information (PHI) though the use of the PHR web-based application.

Policy for Processing Patient Access to their Personal Health Record (cont.)

PROCEDURES for authorized users:

- Only individuals who are authorized to administer access to the PHR application or to register patients may use the IHS PHR Administration application.
- **Federal** user access is granted by completing the ITAC access request.
- **Tribal and Urban sites** *not* on D1/Active Directory must initiate user access through Area or HQ Help Desk ticket.

Policy for Processing Patient Access to their Personal Health Record

PROCEDURES for authorized users continued:

- PHR user access is based on level of administrator or registrar responsibilities:
  - The national PHR administrator privileges include approving, denying, and updating administrator accounts.
- Designate area PHR administrator for privileges to approve, deny, and update area, service unit and facility administrator accounts.
  - Tribes providing tier two services will designate a tier two PHR administrator.

Policy for Processing Patient Access to their Personal Health Record (cont.)

PROCEDURES for authorized users (continued):

- Each facility chief executive officer will designate a PHR administrator who will be granted **local** facility-level administrator privileges to approve, deny, and update local administrator accounts.
- **Facility**-level PHR registrars identified will be assigned PHR privileges to perform registration. It is highly recommended that registrars be identified from the **H**ealth **I**nformation **M**anagement department due to their release of information and custodian of the health record roles.

Policy for Processing Patient Access to their Personal Health Record (cont.)

PROCEDURES for authorized users continued:

- The PHR registrar will perform the following key functions:
  - Work directly with patients in their request for a PHR account and registration process.
  - Provide the patient with a copy of the Notice of Privacy Practices (NPP), as amended, which includes the PHR.
  - 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.

Policy for Processing Patient Access to their Personal Health Record (cont.)

PROCEDURES for authorized users (continued):

- The PHR registrar will perform the following key functions:
  - Verify identity of patients.
  - Link and unlink patient PHR accounts to their health records.
  - Create reports as requested by the service unit/facility managers or supervisor.

Policy for Processing Patient Access to their Personal Health Record (cont.)

Procedures for all users:

- All inappropriate or suspicious activity, such as incorrect linked accounts (breaches), will be reported using the IRT procedures.
- Additionally, the area and/or local privacy officer shall be advised of the incident and included in the investigation, response, and any subsequent notification that is required by law.
- Facilities are strongly encouraged to work with their area HIM consultants to develop **specific procedures** to ensure the accurate linking of patient records and support the role and responsibility of PHR administrators and registrars.

Policy for End User Access to the RPMS DIRECT Messaging System

- Background: **RPMS DIRECT** is a secure, web-based messaging service for the **exchange** of patients' **health** information between healthcare providers and their patients.
- RPMS DIRECT is **HIPAA-compliant** and **integrated** with the **EHR** and **PHR** to provide an easy way for registered providers, healthcare organizations, patients, and their representatives to **share PHI** securely and electronically.

Policy for End User Access to the RPMS DIRECT Messaging System (cont.)

- Policy: RPMS DIRECT is **solely** for the purpose of **healthcare**-related **exchanges** among **DIRECT participants** only. All users must follow these requirements and standards when using RPMS DIRECT. Tribal and Urban organizations **must** have the appropriate **agreements** in place to have access to the RPMS DIRECT.

Policy for End User Access to the RPMS DIRECT Messaging System (cont.)

Definitions:

- Health Information Service Provider (HISP) – An organization that provides services on the internet to facilitate use of DIRECT messaging among providers.
- Level of Assurance (LoA) – Ability to determine, with some level of certainty, that the electronic credential representing an entity (the HISP) can be trusted to belong to the entity.
- Trusted Agent – An individual appointed on behalf of the Registration Authority to complete an in-person identity verification of RPMS DIRECT users. RPMS DIRECT national administrators, area office administrators, service unit/facility administrators (SU/FAs) and/or PHR registrars will serve as a Trusted Agent.

Policy for End User Access to the RPMS DIRECT Messaging System (cont.)

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

- Users must complete the RPMS DIRECT registration process by in-person verification of identity by contacting their local SU/FA.
- Providers and message agents require assurance at LoA 3 (two forms of ID or PIV card).

Policy for End User Access to the RPMS DIRECT Messaging System (cont.)

- Access will not be granted until an approved/ processed ITAC request has been submitted by the user's supervisor.
- Tribal and Urban healthcare providers and message agents must open a helpdesk ticket based on either area or HQ tiered customer support to initiate access for RPMS DIRECT.
- Patients will have to complete the PHR registration process to gain access (PHR Patient Access Policy).

Policy for End Use Access to the RPMS DIRECT Messaging System (cont.)

- SU/FA will provide passwords to providers and message agents.
- SU/FA will remove a user from RPMS DIRECT immediately when a user resigns, is reassigned or is terminated.
- SU/FA will set up message forward.
- User RPMS activity may be monitored, recorded, and subject to audit.

Policy for End User Access to the RPMS DIRECT Messaging System (cont.)

- Local I/T/U facility RPMS DIRECT policies must be in place and acknowledged by the management responsible for the enforcement of privacy, security, and access to PHI.
- A request must be submitted to SU/FA to establish a trust relationship to exchange secure messages with external healthcare organizations.

Policies for Auditing

- HIE Audit Policy – HIE administrators will follow procedures to audit the IHS HIE regularly to ensure appropriate use of the system.
- Definitions:
  - Proactive Audit: an audit conducted on a regular basis for possible inappropriate use or activity.
  - Reactive Audit: an audit in response to a request or triggered event, such as an accounting of disclosure, complaints, incident or breach.
- Access per ITAC request or help desk ticket.

Policies for Auditing (cont.)

- National administrator role
- Area offices will designate area administrators to monitor activity.
- I/T/U sites (CEO) will designate a SU/FA who will be granted local facility-level administrator privileges to monitor system activity.

Policies for Auditing (cont.)

- Based on level of privileges, administrators must monitor system activities routinely. Routine proactive audit reports include:
  - Type of records viewed by the user.
  - Successful or failed authentication attempts.
  - Monitored activity of staff for access to family records.
  - Locked out user reports.
  - Annual access review.

Policies for Auditing (more)

- Administrators provide reactive audit reports as requested by the I/T/U CEO, HIM, privacy officer, security officer, compliance officer or other individuals who have a legitimate need for the information.
- Administrators must report inappropriate or suspicious activities.

Other Audit Policies

- PHR Audit Policy
- RPMS DIRECT Administrator and Audit Policy

Questions

Thank you!

Janice.Chase@ihs.gov

(505) 274-4854