THE INDIAN HEALTH SERVICE

HIPAA Audits and Investigations

Resource and Patient Management System

EHR for HIM

Superior Health Information Management
Now and for the Future

Presenters

Ruth Hawkins

- Elko Facility Privacy Liaison
- HIM Director

Maria Strom

- Phoenix Area Privacy Coordinator

Heather McClane

- IHS Privacy Officer

Objectives

At the end of this session participants should be able to:

- Examine the RPMS EHR Tools of Sensitive Patient Tracking (SPT) and Indian Health Service (IHS) Security Audit (BUSA) Applications
- Conduct Privacy Audits and User Activity using SPT and BUSA
- Best practices with violations and investigations
- Questions and Answers

Sensitive Patient Tracking and Reports (SPTR)

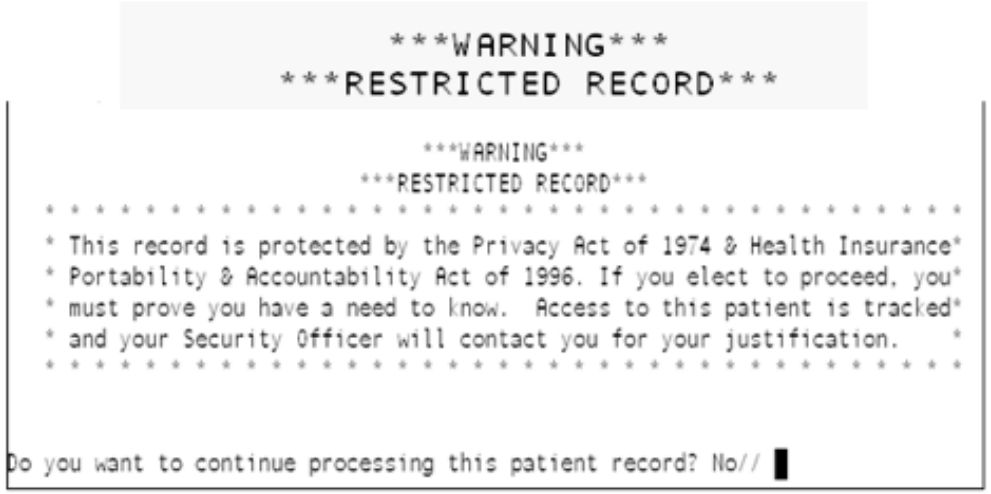
- What is Sensitive Patient Tracking (SPT)?
- Why Use Sensitive Patient Tracking?
- Who Should have Access to Run Sensitive Patient Tracking?
- When to Run Sensitive Patient Tracking Reports?
- Monitoring the Use of Sensitive Patient Tracking…
  - Don’t lose sight of the purpose for this function
- https://www.ihs.gov/RPMS/PackageDocs/PIMS/pims053i.pdf

Sensitive Patient Tracking and Reports (2)

SPT allows a facility to track who accesses patient records marked as sensitive.

When a marked record is accessed a warning message displays.

Note: If the site parameter "Track All Patient Access" is turned on, then all patients not already classified as Sensitive will be tracked and no warning message is displayed, but a tracking log is maintained in the system.



Sensitive Patient Tracking and Reports (3)

Who has access to run SPTR?

- The Sensitive Patient Tracking Menu contains the security options for assigning, displaying, and purging information related to sensitive patient records. Only holders of the DG SECURITY OFFICER key have access to this menu; most users will never see the Sensitive Patient Tracking menu.

```
SPTR    Sensitive Patient Tracking Reports ... [BZLBDG SECURITY MENU]
           **> Locked with BZLBDG SECURITY
```

Sensitive Patient Tracking and Reports (4)

Using Sensitive Patient Tracking

System Audits, Investigations of reported incidents/violations.

SPTR Sensitive Patient Tracking Reports ... [BZLBDG SECURITY MENU]
DUA Display User Access to Patient Record
PAU Display All Patients Accessed by a User

Sensitive Patient Tracking and Reports (Additional Options with BDG Security)

```
Sensitive Patient Tracking (BDG SECURITY MENU)
|
|__DUA Display User Access to Patient Record [BDG SECURITY DISPLAY LOG]
|
|__EPL Enter/Edit Patient Security Level [BDG SECURITY ENTER/EDIT]
|
|__LSP List Sensitive Patients [BDG SECURITY LIST]
|
|__PLOG Purge Record of User Access from Security Log [BDG SECURITY PURGE
|       LOG]
|
|__PPAT Purge Non-sensitive Patients from Security Log [BDG SECURITY PURGE
|       PATIENTS]
|
|__USP Update Security Parameters [BDG SECURITY PARAMETER EDIT]
|
|__XSO Sensitive Patient Tutorial [BDG SECURITY HELP]
```

Sensitive Patient Tracking and Report Options

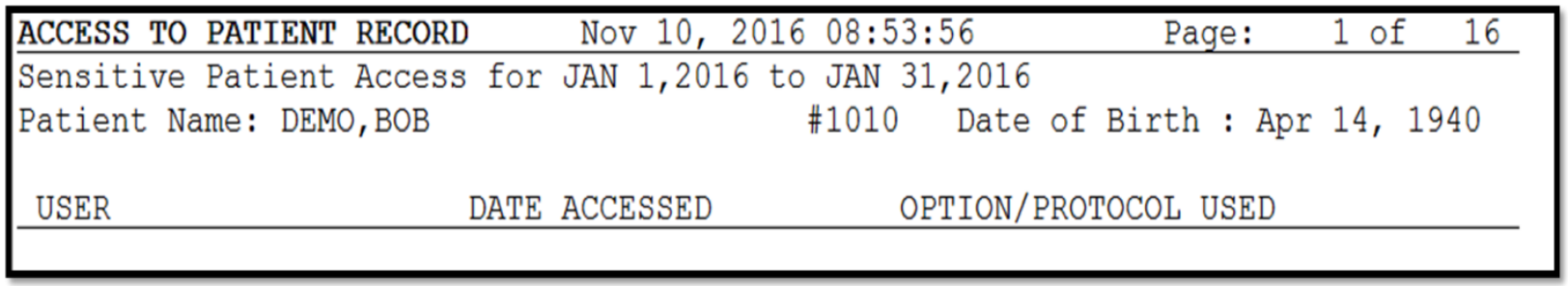
The two options listed here are used primarily by HIMs, Facility Privacy Liaisons, and Area Privacy Coordinators for monitoring, auditing, and investigative purposes.

- DUA Display User Access to Patient Record [BDG SECURITY DISPLAY LOG] **> Locked with DG SECURITY OFFICER
- PAU Display All Patients Accessed by a User [BDG SECURITY USER LIST] **> Locked with DG SECURITY OFFICER

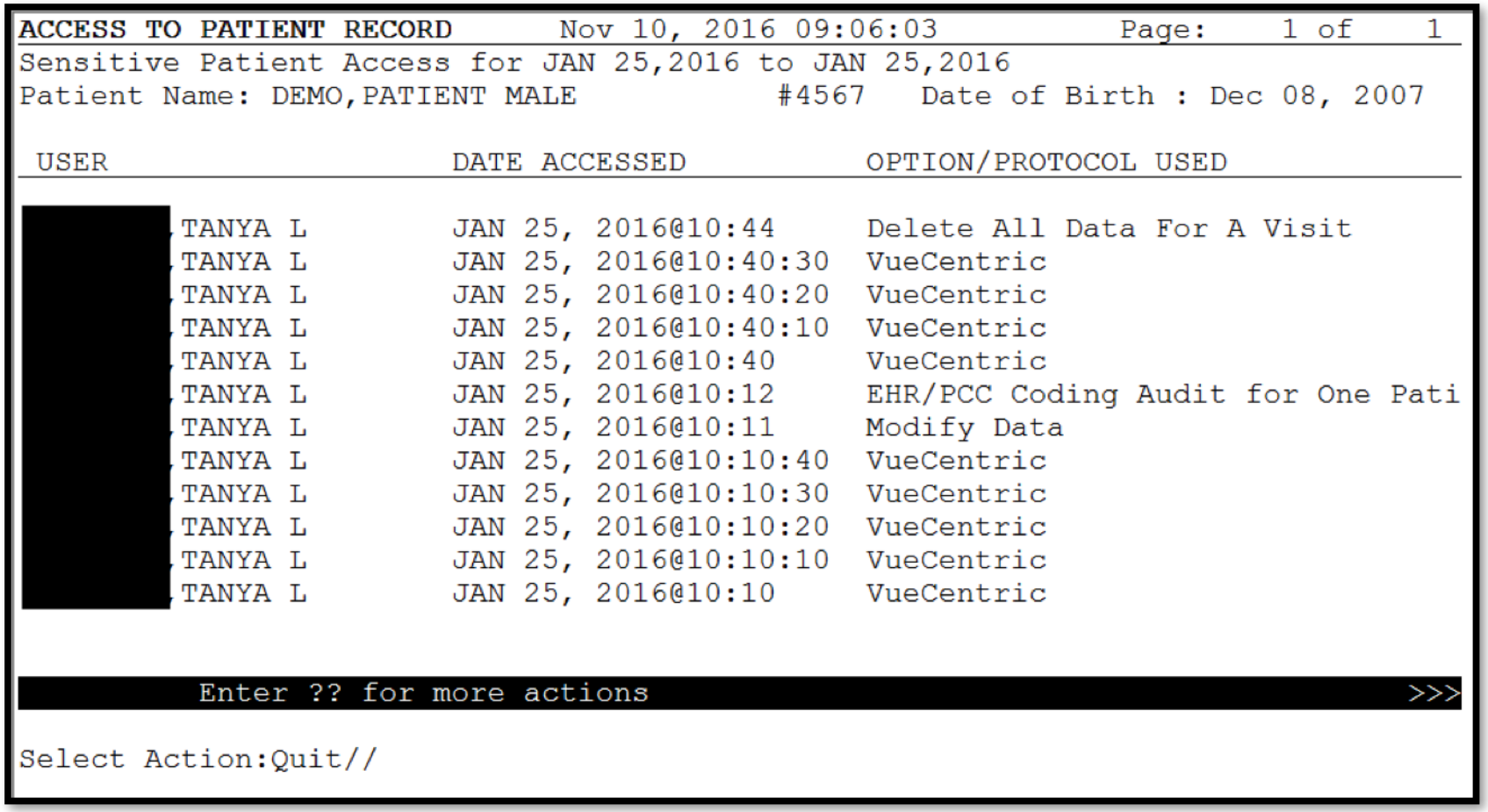
Display a User Access to Patient Record (DUA)

Holders of the DG SECURITY OFFICER key use this option to display users who accessed a particular patient record over a given date range. View one user's access or all users who accessed the record.

- Select Patient NAME:
- Beginning DATE:
- Ending DATE:
- Do you want to see when a select user accessed this record? No//



Display a User Access to Patient Record (DUA) (2)



```
ACCESS TO PATIENT RECORD      Nov 10, 2016 09:06:03          Page:    1 of    1
Sensitive Patient Access for JAN 25,2016 to JAN 25,2016
Patient Name: DEMO,PATIENT MALE            #4567   Date of Birth : Dec 08, 2007

 USER                          DATE ACCESSED           OPTION/PROTOCOL USED

[redacted],TANYA L             JAN 25, 2016@10:44      Delete All Data For A Visit
[redacted],TANYA L             JAN 25, 2016@10:40:30   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:40:20   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:40:10   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:40      VueCentric
[redacted],TANYA L             JAN 25, 2016@10:12      EHR/PCC Coding Audit for One Pati
[redacted],TANYA L             JAN 25, 2016@10:11      Modify Data
[redacted],TANYA L             JAN 25, 2016@10:10:40   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:10:30   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:10:20   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:10:10   VueCentric
[redacted],TANYA L             JAN 25, 2016@10:10      VueCentric


          Enter ?? for more actions                                      >>>

Select Action:Quit//
```

Display All Patients Accessed by a User (PAU)

Use this option to view all patients a particular user accessed within a date range. The list may be sorted by date, by patient name (alphabetically), or by the option accessed. The report lists the patient's sensitivity level, if known, at time of access.

SELECT USER:

SELECT EARLIEST DATE:

SELECT LATEST DATE:

Select one of the following:

1. BY DATE
2. BY PATIENT NAME
3. BY OPTION

Select How you Want the Report Sorted:

Display All Patients Accessed by a User (PAU) (2)

Access by Specific User Nov 10, 2016 09:01:04 Page: 1 of 7

User: [redacted],TANYA L

Date Range: Jan 01, 2016 to Jan 31, 2016

+Patient Name	Chart#	Access Date/Time	Option / Security Level	
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:50	INACTIVATE/ACTIVATE a	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:45	Modify Data	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:44	Delete All Data For A	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:40	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:31	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:16	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:15	VueCentric	/ N
DEMO,PATIENT ROSEBUD	456871	JAN 25, 2016@10:15	VueCentric	/ N
DEMO,PATIENT MALE	4567	JAN 25, 2016@10:12	EHR/PCC Coding Audit f	/ N

Sensitive Patient Tracking Report Tips

- Access Control is about who shall have access to which resources and how access is monitored.
- Implement Policies And Procedures for Electronic Information Systems audits.
- Designate a Facility Privacy Liaison or Area Privacy Coordinator .
- **Initiate Random User Access Reviews on a monthly basis.**

BUSA

- Enables tracking of user activity by OIT staff
- As a requirement for Meaningful Use (MU) stage two certification, all activity relating to patient data querying, adding, editing, copying, deleting, and printing must be logged.
- The manual recommends the local IT have the only access.

BUSA GUI Report

- **IHS User Security Audit**
- Web-enabled reporting interface
  - https://www.ihs.gov/RPMS/PackageDocs/BUSA/busa010u.pdf
- To review the information logged as part of the BUSA Auditing, use the address below but replace the IP address with the address of the RPMS server, the port with the proper port number, and replace namespace with the namespace of the RPMS live database. See the installation manual for further details on determining these values.
  - The IP address, port and namespace will need to be changed for your individual site.
  - Example: http://ip address:port/csp/namepace/BUSA.MainReportPage.cls

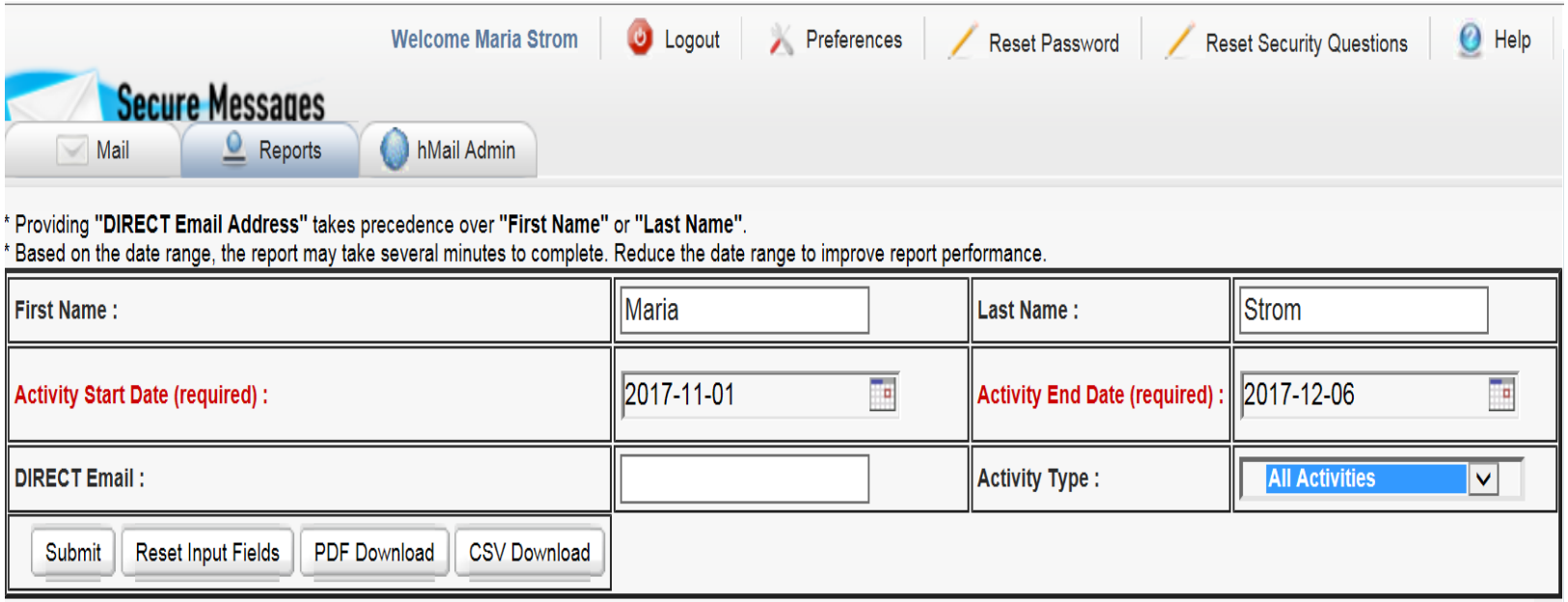
SECURITY AUDITING OF THE HEALTH INFORMATION EXCHANGE

- 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 Service Unit/Facility Administrators (SU/FA) will follow procedures to regularly audit the IHS HIE to ensure appropriate use of the system.
- Procedures are found in the IHS Manual Part 8 – Information Management – Chapter 23, Resource and Patient Management System Network Section 8-23.6
- (7) All HIE SU/FA shall monitor system activities routinely using appropriate audit reports available within the IHS HIE audit web application. Routine proactive audit reports that are recommended include, but are not limited to, the following:

Health Information Exchange Administrator Audit Reports

Report	Head-quarters	Area	Facility	Frequency (based on tier and activity)
Type of records viewed by the user		X	X	Monthly
Type of Activity	X	X	X	Biweekly: depends on tier and activity
Successful or failed authentication attempts	X	X	X	Weekly
Users' status: Active, inactive, and locked account	X	X	XX	Daily
Monitoer 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 Administratord access to ensure disabled accounts for terminated and retired staff within 24 hours	X	X		Weekly
Locked out users report			X	Bl-weekly
Annual access review	X	X	X	Annually

Health Information Exchange Administrator Audit Reports (2)



Health Information Exchange Administrator Audit Reports (3)

Activity Date and Time	DIRECT Email Address	Message	Activity Type	First Name
2017-11-06 09:40:49.287	maria.strom@directihs.net	Login Not Successful from 161.223.196.173 to webmail.	Invalid Login	Maria
2017-11-06 09:41:13.077	maria.strom@directihs.net	Login Not Successful from 161.223.196.173 to webmail.	Invalid Login	Maria
2017-11-06 09:41:53.7	maria.strom@directihs.net	Login Successful from 161.223.196.173 to webmail.	Log In	Maria
2017-11-06 09:43:12.0	maria.strom@directihs.net	Invalid Login from 161.223.196.173, 198.45.0.104	Invalid Login	Maria
2017-11-06 09:43:46.0	maria.strom@directihs.net	Login from 161.223.196.173, 198.45.0.104	Log In	Maria
2017-11-06 09:45:17.0	maria.strom@directihs.net	The following User profile values have been changed for loretta.ondelacy@hopi.directihs.net account from 161.223.196.173, 198.45.0.104 : Account is Enabled	User profile Update	Maria
2017-11-06 09:46:49.0	maria.strom@directihs.net	The following User profile values have been changed for loretta.ondelacy@hopi.directihs.net account from 161.223.196.173, 198.45.0.104 :	User profile Update	Maria
2017-11-06 09:59:48.737	maria.strom@directihs.net	maria.strom@directihs.net Logout from webmail from 161.223.196.173.	Log Out	Maria

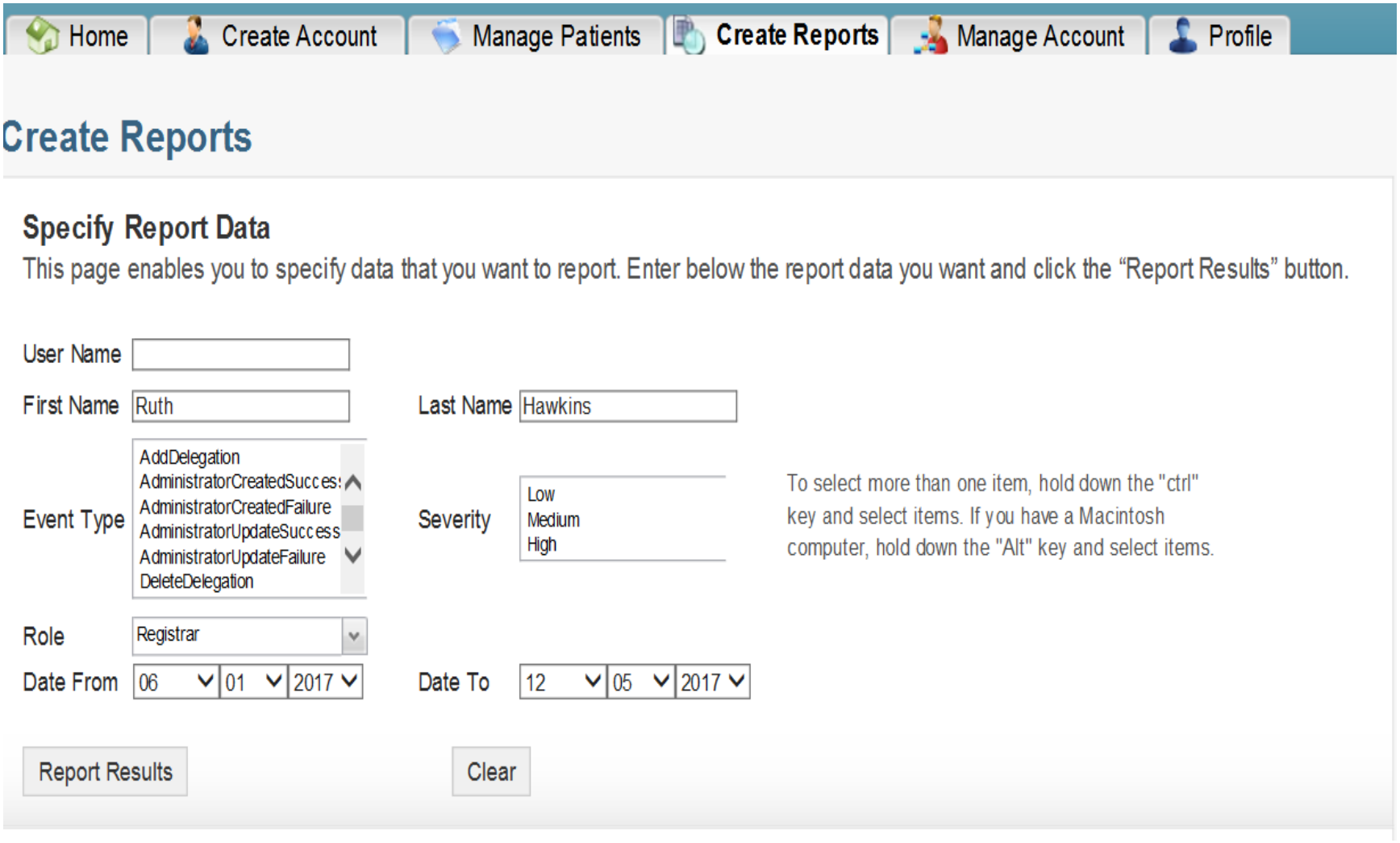
AUDITING PROCESS OF THE PERSONAL HEALTH RECORD

- Purpose. This section establishes the audit process for authorized users of the IHS PHR. Authorized PHR SU/FA shall conduct audits and run reports on use of the IHS PHR through the PHR Administrator portal.
- Procedures are found in the IHS Manual Part 8 – Information Management – Chapter 23, Resource and Patient Management System Network, Section 8-23.8
- The SU/FA shall monitor system activities using the audit function within the PHR Administrator portal. See the Personal Health Record Web Portal Administrator Manual at ftp://ftp.ihs.gov/pubs/PHR/bphr020a.pdf. Routine audit reports include, but are not limited to the following:

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, administrator and facility failures	X	X	X	Daily
	Successful and failed system event logging	X	X	X	Dailly
	Service Problem: Master Patient Index (MPI) and Health Information Exchange (HIE)	X			Dailly
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	Anually
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

PHR Administrator Portal



PHR Report Results

Report Results

Below are the report results. Click the "Generate Report" button to manage the results.

Results

Username	IP Address	Last Name	First Name	Event Type	Severity	Message	Time
[redacted]		Haw kins	Ruth	LoginSuccessful	Low	Successful login by administrator :: RKhaw k	08/11/201
		Haw kins	Ruth	ProcessPatientApplicationSu...	Medium	Patient :: Hepi15 application is successfully li...	08/11/201
		Haw kins	Ruth	Logout	Low	Administrator logged out :: rkhaw k	08/11/201
		Haw kins	Ruth	LoginSuccessful	Low	Successful login by administrator :: RKhaw k	06/23/201
		Haw kins	Ruth	AdministratorUpdateSucces...	Low	Successfully reset passw ord by :: rkhaw k	06/23/201
		Haw kins	Ruth	LoginSuccessful	Low	Successful login by administrator :: RKhaw k	06/23/201
		Haw kins	Ruth	Logout	Low	Administrator logged out :: rkhaw k	06/23/201
		Haw kins	Ruth	LoginSuccessful	Low	Successful login by administrator :: RKhaw k	06/23/201
		Haw kins	Ruth	Logout	Low	Administrator logged out :: rkhaw k	06/23/201
		Haw kins	Ruth	LoginSuccessful	Low	Successful login by administrator :: RKhaw k	07/25/201
		Haw kins	Ruth	Logout	Low	Administrator logged out :: rkhaw k	07/25/201

Incidents

- Lost PIV
- Lost computer
- Unattended PIV
- Lost Government Cell Phones
- Unauthorized Access to department (HIM), records, offices, etc.
- Unauthorized Disclosure
- Unattended Logged-In Computer
- Sending email containing PHI via Outlook – PKI Key is not appropriate
- Documents containing PHI left on a printer, fax machine, or copier

Steps for Any Investigation

A Privacy Liaison or Coordinator must:

- Recognize when an investigation is in order.
- Decide what the investigation should establish, such as whether a particular person accessed unauthorized PHI or whether privacy violation has been committed.
- Select appropriate investigators.
- Identify potential witnesses and documents for review.
- Plan the investigation (best to have a written plan).
- Organize a list of questions to ask witnesses.
- Establish security for files and records.
- Be prepared to modify and update the plan as needed, based on new information that might come in as the investigation progresses.

Written Complaint

- Before an investigation can be completed, we must receive a complaint in writing. Be sure this is a true complaint and not something like “see who was in my records.”
- Alternately, when we conduct our monthly monitoring of all staff access, including area office staff, under §164.308: If we as HIM Directors see suspicious activity, we can file an F07-02b form here: https://disirf.ihs.gov/, and **our filing of the IRF serves as written complaint.**

Check USP Under SPT/BDG

- Go into RPMS and enter ^spt or ^bdg (depending on how spt is set up at your service unit)
- Go to USP, then option 3. Print the list of DG security key holders.
- Go back to USP, option 1. Print the screen that opens.
- You want to show that your security parameters are set to purge after 365 days, not before.
- You also want to show that all staff are blocked from accessing their own records.

Important Reminder

- As Chief HIMS key holders, even though your SPT is set to block you, you will still have access to your own record.
  - The same applies to Chief MIS key holders.
  - To fix this, ask your Area HIM consultant or IT Site Manager to go to the EAR option in SPT and enter a restriction to block your ability to access your own chart.
  - Then be sure to go to EAR and enter restrictions for your IT staff as well.

Formulating Investigative Questions

- When you formulate your investigative questions, do not divulge PHI of the complainant or subject of the investigation.
- Keep it simple:
  - Example: On July 1, 2015 at 18:36 you accessed the record of Demo, Parent; Under what authority did you access the record?

Fact Finding

- Leave space for the employee to type in their responses,
- Give the employee enough time to answer the questions in writing, usually three to four business days.
- Make sure you have a statement such as: “Please be aware that you may be asked to answer further questions or provide further clarification of your responses.”
- Be sure to include 18 USC 1001 just before employee signature line
- **Do not** send these interview questions via Outlook; instead use Secure Data Transfer.

18 U.S.C. §1001

- I understand that Under 18 U.S.C. § 1001. Statements or entries generally (a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully— (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; (2) makes any materially false, fictitious, or fraudulent statement or representation; or (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title, imprisoned not more than 5 years.

HIPAA Disposition Schedule

- Under 45 CFR §164.530, we are required to maintain all records regarding HIPAA investigations, monitoring, and such for six years.
- Remember that SPT auto purges after 365 days; you don't want to set it for longer, as it will bog down and slow down your RPMS and EHR.
- This means that you will be unable to recreate an SPT report two years from now, so you wouldn't meet the six-year retention requirement electronically. You must print (or scan) your SPT report and retain for six years.
- The agency's disposition schedule provides for this and can be found here: http://www.archives.gov/records-mgmt/rcs/schedules/index.html?dir=/departments/department-of-health-and-human-services/rg-0513.

Making Recommendations

- We are required to make recommendations based on the Special General Memorandum 2015-01 and under 45 CFR §164.530.
- Keep in mind that regardless of what we recommend these are still federal employees who have rights and it is up to ER/LR and the employee's supervisor to determine, through Douglas Factors, what the actual disciplinary action is, if any.
- Our legal requirement is to make a recommendation for sanction. The supervisor's legal requirement is to work with ER/LR with Douglas Factors, which may or may not lesson the sanction. We have no need to know what disciplinary action, if any, was taken, (unless you have an OCR compliance review).
- Simply request the ER/LR Track It ticket from the supervisor for proof of compliance.

Due Process

- Keep in mind that it is extremely important that we ensure that both the agency and the employee are treated fairly, with respect and dignity.
- This means that we follow our policies and the letter of the law.
- All of our incidents are actually reported to OCR at the end of every calendar year.
- OCR can choose any of them and conduct a compliance review.

Questions and Discussion