2019 Indian Health Service Partnership Conference

Spokane, Washington

STANDARDIZING PRIVACY OPERATIONS

HIM Track – Navajo Area Best Practices

Gary M. Russell-King, HIM Chief
Northern Navajo Medical Center
Acting Navajo Area HIM Consultant & Privacy Coordinator

LEARNING OBJECTIVES

1. Definition of Privacy Incident and Breach
2. Lessons learned from Shiprock Privacy Breach
3. Standardized Privacy forms and processes
4. Conduct a privacy investigation
5. Establishing privacy awareness

PRIVACY INCIDENT

An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

PRIVACY BREACH

The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose.

SHIPROCK PRIVACY BREACH

SHIPROCK PRIVACY BREACH

THURSDAY
APRIL 07
2016
Volume LV
Number 14

www.navajotimes.com
One Dollar

NAVAJO TIMES
DINÉ BI NAALTSOOS

Stolen documents – containing patient info – returned to Shiprock hospital

BY ALYSA LANDRY
SPECIAL TO THE TIMES

FARMINGTON, N.M. – Personal and medical data for about 7,500 patients at Northern Navajo Medical Center is at risk after a former employee walked off

health record numbers, Social Security numbers, dates of birth, insurance policy numbers and admitting diagnoses.

All the information has been retrieved and returned to the hospital, according to Jenny Notah, a spokeswoman for the

member discovered the warehouse and records for about 470 patients, Notah said. An investigation conducted by the U.S. Department of Health and Human Services' Office of Inspector General revealed records for about 7,000 addition-

has referred the matter to the U.S. Attorney's Office for possible prosecution.

There is no evidence that the data was used by or disclosed to unauthorized individuals, but the Indian Health Service sent letters to all 7,500 patients

on this incident to ensure the appropriate action is taken."

The letter also states that IHS has reviewed its processes and updated its policies to ensure similar incidents don't happen in the future. It also is providing face-to-face privacy train-

and regret that this situation occurred," the letter states. "The Indian Health Service is committed to providing quality care, which includes protecting your personal information. We want to assure you that we have policies and procedures in place

SHIPROCK PRIVACY BREACH 2016

- Former employee removed original patient update sheets from facility containing PII, copies of AOB, CIB, Social Security Card, drivers license.
- NNMC worked closely with IHS, HHS and OCR to address the breach and developed a corrective action, which was implemented at all Federal facilities on Navajo.

CORRECTIVE ACTION PLAN

- Identify key areas to address:
  1. Mandatory staff training
  2. Registration work flow and process
  3. Conducting privacy audits
  4. Education on Records Management

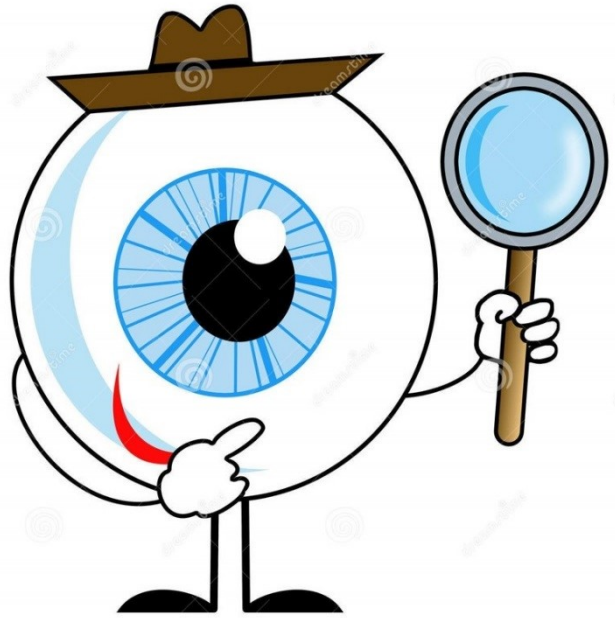
INVESTIGATION FINDINGS

- Hoarding of patient documents
- Inappropriate storage of PHI/PII (PMAP)
- Lack of staff knowledge on General Records Schedule
- Unnecessary collection of data/copies
- Untimely shredding

FINDINGS

Inappropriate use of electronic devices to transmit PHI/PII

a. Personal cell phones
b. Email
c. EHR broadcast
d. Social Media – Facebook



IMMEDIATE ACTION PLAN

- Stop copying extra documents
- Stop using clip boards for sign-in
- Updating face-to-face

CORRECTIVE ACTION

All findings uncovered during mini-privacy department sessions and on-site privacy reviews were incorporated into the updated privacy power point presentation and privacy test.

MANDATORY MINI-PRIVACY TRAINING

KEY POINTS TO REMEMBER FROM PRIVACY PRESENTATION:

1. **What is the difference between Privacy Act and HIPAA Privacy?**
   Privacy Act covers all Government record systems.

2. **What is the five (5) System of Records covered by the Privacy Act?**
   1. *Medical, Health and Billing Records*
   2. *Medical Credentialing & Privilege Records*
   3. *Scholarship & Loan Repayment Records*
   4. *Application Records for Sanitation Facilities (OEHE)*
   5. *Personal Health Record (PHR)*

3. **What is PHI and PII?**
   PHI = *Protected Health Information – This is the medical & health information of a person.*

   PII = *Personally Identifiable Information – Example: Name, HRN, DOB, and SSN*

4. **Example of Restrictions**
   IHS only has one (1) approved restriction – for Hospital Directory

5. **What is TPO?**
   Treatment, Payment, Operations
   Which do I or my department fall under?

6. **When do I use the Accounting of Disclosure form?**
   Whenever copies of medical records are disclosed without the patient's written consent

7. **Can I send PHI/PII through email?**
   No. Government email system is not secure. Use Secure Data Transfer system which is encrypted.

8. **Know when and how to discard documents containing PHI/PII**
   General Records Disposition

9. **Privacy Complaint must be filed in *180* days**
   Who, what, when, where, and if any proof should be included in complaint.

10. **What is IRT?** https://disirf.ihs.gov/
    Incident Response Team. Under the HITECH Act, we are required by law to report any breach compromises immediately within 30 minutes of the incident.

20 PRIVACY TIPS & REMINDERS

1. Safeguard the medical record when in your possession. Do not leave patient records **unattended** in rooms, hallways, or offices where anyone can access or take the record. Secure your work area.
2. Don't **display** patient appointment listings that contain patient identifiers in public view, such as clinic hallways, bulletin boards, etc.
3. Be sensitive to confidentiality of your patient, by not discussing or distributing specific PHI in **open meetings** or areas. Sanitize copies & discussion of PHI to protect patient privacy.
4. **Shred** work copies of patient documents (*work copies of lab reports, etc.*) that are no longer needed. Shred all patient documents placed in the designated shred box daily. Please do not recycle.
5. **Discard** copies of sign-in sheets, worksheets, copies of RPMS appointment listing, etc. immediately after usage, or in accordance to the IHS General Records Schedule.
6. Refrain from using the **overhead paging** system to call a patient back to a clinic as this may jeopardize patient confidentially.
7. **Lock** up any reports, disc, or files that contain PHI or patient identifiers if you are working on performance improvement or performing case studies. Use encrypted USB to store raw data.
8. Please **log off** your computer and remove your PIV card every single time you walk away from your monitor.
9. Do not **share** your computer codes with anyone, as your menu options are set up in accordance to your profession/job.
10. Do not **remove** any patient documents or patient information from the facility to work on at home.
11. Always ask the **patient's permission** to discuss confidential PHI if another person is present with the patient. Document for the record.
12. When disclosing copies of health information using a Privacy Act Routine Use or HIPAA Privacy Provision for Treatment, Payment or Operations, document the disclosure on the patient's **Accounting Disclosure Record**, form IHS-505, located in the back of the patient' chart.
13. When disclosing PHI by **fax**, file the fax cover sheet in the patient's record because it is still a release of information, and every disclosure must be accounted for.
14. Parents do not have direct access to their **child's PHI**. The parent only has the authority to tell us *(IHS)* to whom or where to disclose the medical information with a signed consent.
15. Patients must request in **writing** to access their medical record before they can review it. Requests for review can be forward to the HIM Director.
16. **Telephone disclosure**. If health information is needed for continuity of care, first verify the caller and their phone number before disclosing any information. If a patient is calling wanting their next appointment date, ask for three or more patient identifiers to confirm identity.
17. The **RPMS** and medical record (paper & electronic) is only to be utilized in the performance of your duties and information should never be provided to another person who does not have a right, privilege or access. All access to patient information via RPMS/EHR is electronically monitored.
18. Personal **cellular phones** are prohibited to use for taking photos, recording or texting PHI/PII.
19. Do not use the Government **e-mail** system to transmit PHI/PII as e-mail is not a secure system. Use the **Secure Data Transfer** system.
20. Refrain from posting hospital business or PHI/PII on **social media**.

PROTECTING PATIENT PRIVACY is PRIORITY # 1 & EVERYONE'S JOB.

Shiprock Service Unit Privacy Liaison & Navajo Area Privacy Officer: *Gary M. Russell-King* Ext.3-6032

VALIDATING COMPLIANCE

- Notice of Privacy Practices is displayed in waiting rooms
- Timely shredding of patient documents daily
- Staff knowledge of IHS General Records Schedule.

SECTION 3 - MEDICAL RECORDS

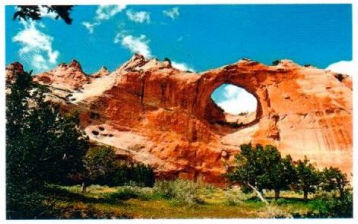
ITEM NO.	TITLE AND DESCRIPTION OF RECORDS	DISPOSITION AUTHORITY
3-4	**MASTER PATIENT INDEX (MPI) FILES.** A permanent MPI maintained by each facility containing the patient's basic identification data for each patient registered at each facility.	**PERMANENT.** Cut off on death of individual or transfer of individual to another service area. Transfer to FRC when at least 1 cubic foot accumulates. Transfer to the National Archives when 20 years old. Auth: N1-513-92-4
3-5	**ADMISSION LOG FILES.** Records of chronological admission log sheets.	Destroy when 6 months old. Auth: N1-513-92-4
3-6	**ADMISSIONS AND DISCHARGES FILES.** Daily patient admission and discharge sheets. **NOTE:** A master set will be maintained to contain a copy of each admission and discharge sheet created during the latest 12-month period.	Cut off master set annually. Destroy when 1 year old. Destroy all other copies after purpose has been served. Auth: N1-513-92-4
3-7	**BENEFICIARIES EFFECTS AND VALUABLES AUDIT FILES.** Records of audits of effects, valuables, Government-issued clothing, incidentals and related records.	Destroy 1 year after completion of subsequent audit and resolution of all discrepancies. If no audit is done, destroy when 1 year old. Auth: N1-513-92-4

NAVAJO AREA HIM

- Establishment of privacy work group with all SU Privacy Act Liaisons (PAL) and Co-PALs
  1. Update privacy presentation for training
  2. Standardized forms
  3. Standardized privacy investigations
  4. Standardized audits

NAVAJO AREA PRIVACY WORKGROUP

Navajo Area Indian Health Service
Health Information Management Program



HIM Privacy Workgroup Meeting
Friday, January 27, 2017
GIMC Dental Conference Room
9:00 am

AGENDA

1. Introductions
2. Identify task and prioritize list to accomplish with workgroup:
   List: Update Privacy Powerpoint presentation (NAIHS vs. IHS)
   Privacy SPT Audit process/form
   Privacy Checklist for spot check
   Privacy Investigation Form
   Standard Privacy forms used: Letters to patients for Restrictions, Corrections, ROI cover letter, etc.
   Standardized privacy policies: Access to records, ROI, etc.
3. Administrative requirements:
   a. Designation of Privacy Liaison in writing
   b. Identify training needs for PALs
   c. Physical Security of HIM Dept.
   c. Other
6. Next meeting – date, place, time.

Any questions, please contact: Gary M. Russell-King
Acting Navajo Area HIM Consultant
(505) 368-6032

DESIGNATION OF PAL

- Designation of **P**rivacy **A**ct **L**iaison by the CEO
- This gives the PAL the authorization to conduct and investigate privacy complaints
- Accept and process HIPAA requests from patients, such as restrictions, amendments, etc.
- Co-PALs designated at health centers.

PAL DESIGNATION LETTER

DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Navajo Area
Indian Health Service
P.O. Box 9020
Window Rock, AZ 86515

DATE:

TO:

FROM: Chief Executive Officer

RE: Delegation of Authority – Service Unit Privacy Liaison

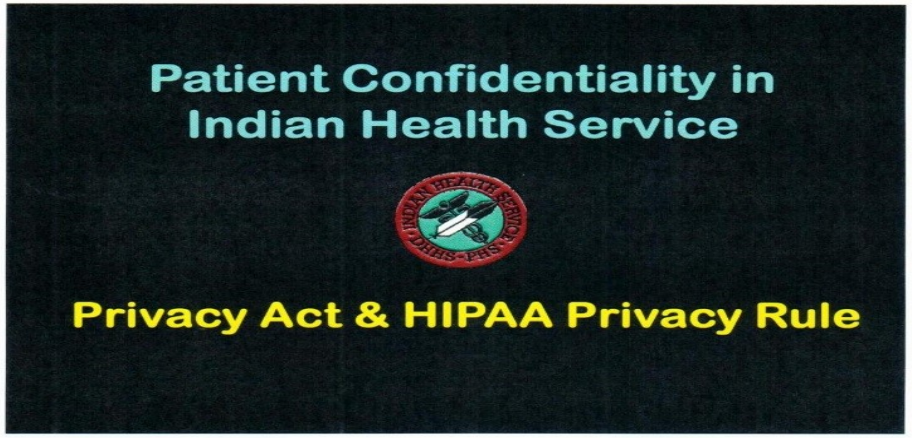
As the Chief Executive Officer of the Service Unit, I hereby designate the authority and responsibility to following individuals to coordinate, manage, conduct investigations and process administrative requests for the Privacy Program within the Service Unit:

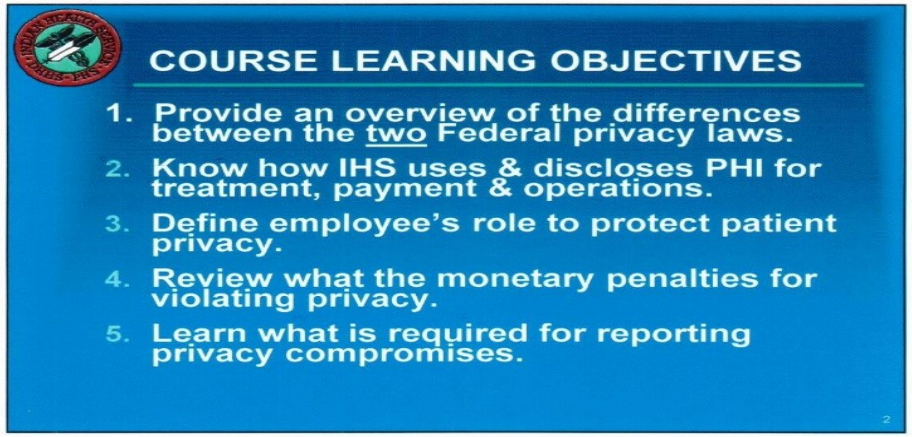
1. Service Unit Privacy Liaison:
   Name, Title, telephone number and email address

2. Alternate Service Unit Privacy Liaison:
   Name, Title, telephone number and email address

3. Co-Privacy Act Liaison – Health Center
   Name, Title, telephone number and email address

STANDARDIZED PRIVACY TRAINING





HEALTH STREAM PRIVACY QUESTIONS

1. **What is PHI ?**
   ( ) Private Hospital Investigator
   ( ) Protected Health Information
   ( ) Private Health Insurance
2. **What is Personally Identifiable Information (PII) ?**
   ( ) A chart number, date of birth, social security number
   ( ) A driver license number, census number, claim number
   ( ) All of the above
3. **All Service Unit employees have total access to medical records.**
   ( ) True ( ) False
4. **What is a privacy compromise (breach)?**
   ( ) Unauthorized access, use, or disclosure of PHI which compromises the security or privacy of health information.
   ( ) Transmission of PHI/PII using an unsecure email system.
   ( ) Viewing patient information in EHR of a co-worker, friend or relative for personal use.
   ( ) All of the above.
5. **I faxed patient information to another hospital. I must document an accounting of disclosure.**
   ( ) True ( ) False
6. **What is the major difference between the two Federal Privacy Laws?**
   ( ) There is no difference.
   ( ) Privacy Act is applicable to all Federal Records
   ( ) HIPAA only covers electronic medical records.
   ( ) Both Privacy Laws do not cover medical records for 638 facilities.
7. **What does TPO stand for?**
   ( ) Third Party Only
   ( ) Treatment, Payment and Operations
   ( ) Tribal Police Officer
   ( ) Treatment Plan Only
8. **What is your role as an employee to protect patient privacy?**
   ( ) Shred work copies immediately after usage.
   ( ) Remove PIV card when leaving work station.
   ( ) Return medical record to HIM Dept. at end of the day.
   ( ) All of the above.
9. **What is the Civil Penalty imposed to a hospital for not complying with the Privacy Laws?**
   ( ) Hospital is not fined due to HITECH Act.
   ( ) Hospital is fined $100 per violation.
   ( ) Not applicable to Indian Health Service because it's a Federal Agency.
   ( ) Hospital closes down.
10. **You are allowed to post patient health information or hospital business on your personal Facebook afterhours.**
    ( ) True ( ) False
11. **You can use your personal cellular phone to take a photograph of a patient to document patient care.**
    ( ) True ( ) False
12. **A parent has a right to a copy of their child's entire medical record under the Privacy Act of 1974.**
    ( ) True ( ) False
13. **You cannot send PHI/PII using the regular Government email system (Microsoft Outlook, web mail).**
    ( ) True ( ) False
14. **What is the first thing you do when you identify a possible privacy violation?**
    ( ) Ignore it.
    ( ) Tell other co-workers about it.
    ( ) Report incident on IRT web site immediately
    ( ) Call the local Chapter House official.
15. **Who is ultimately responsible for protecting patient privacy?**
    ( ) Privacy Liaison
    ( ) Chief Executive Officer
    ( ) Every Employee
    ( ) The President of the United States

PRIVACY TRAINING

- Updated power point privacy training to include HIPAA, Privacy Act, and Records Management
- Downloaded to Health Stream at all SUs
- Formulated a 10 question privacy test at the end of the training
- Employees must pass at 70% or more and receive a certificate.

CONDUCTING PRIVACY AUDITS

- Inform Department supervisor that you will be conducting random privacy audits on their staff members
- Results will be shared
- Any inappropriate access will need to be addressed with the employee with a corrective action.

PRIVACY AUDITS

- Do audits each quarter. Do one department in each Division
- Based on the number of employees in the department, use a sample size
- Audit different employees each time

PRIVACY AUDIT SHEET

PRIVACY AUDIT SHEET **Date:** _____

Employee Audited	Title	Department/Unit

Random sample of 25 patients from RPMS SDT report: Date Range of audit: _____

HRN#	VISIT DATE	RPMS PACKAGE ACCESSED	ACCESS VALID?	COMMENT(S)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				

COMMENTS/RECOMMENDATIONS:

PRIVACY AUDITING

- Using the RPMS Sensitive Patient Tracking report, randomly selecting a sample of 25 patient records to audit by employee by department.

ACCESS TO PATIENT RECORD Sep 25, 2007 14:52:33 Page: 1
Sensitive Patient Access for APR 1,2007 to APR 10,2007
Patient Name: DOE,NAVAJO JANE #1 Date of Birth : May 06, 19

+USER	DATE ACCESSED	OPTION/PROTOCOL USED	INPATIENT
CLYDE,ROBERTA MC	APR 04, 2007@14:07	Appointment Manageme	NO
BENALLY,JOHN D	APR 02, 2007@13:53	Edit Claim Data	NO
BEN,CAROL L NA	APR 09, 2007@08:48	Generate Multiple He	NO
DUNCAN,BERNICE	APR 09, 2007@10:59	EDIT a patient's fil	NO
DUNCAN,BERNICE	APR 09, 2007@10:56	EDIT a patient's fil	NO
HERROD,JON	APR 09, 2007@18:53	Multipurpose accessi	NO
BARTON,ROSALYNN PT	APR 09, 2007@08:34	View patient's regis	NO
BENALLY,MARJORIE A	APR 09, 2007@14:18	Print a FACE SHEET	NO
DODGE,DEANNA	APR 04, 2007@10:31	Appointment Manageme	NO
DODGE,DEANNA	APR 01, 2007@11:23	Appointment Manageme	NO
FOX,JUDE	APR 02, 2007@10:07	Print a FACE SHEET	NO
FOX,JUDE	APR 02, 2007@10:06	Print a FACE SHEET	NO
DEALE,TANYA	APR 09, 2007@19:06:20	Delete All Data For	NO
DEALE,TANYA	APR 09, 2007@19:06:10	Delete All Data For	NO

UNANNOUNCED PRIVACY SURVEY

- Each month, pick a department/clinic to do a privacy walk-through for potential privacy concerns and compliance
- Add problem-prone privacy issues to the checklist that maybe unique to your facility or SU
- Share results with Dept./Clinic supervisor.

PRIVACY CHECKLIST

PRIVACY CHECKLIST

DATE: _____ Department: _____

CRITERIA	YES	NO	COMMENT
1. Computer Screens used in high-traffic areas			
2. Shredding performed daily			
3. Shed container in a secure area			
4. PHI/PII not posted on walls/rooms			
5. Computers logged off when not in use			
6. Employee is wearing Employee I.D. badge			
7. Paper records in secure location			
8. NPP poster in dept/waiting area			
9. PIV card secure (not left in card reader)			
10. Fax machine located in secure area			
11. Copiers located in secure area			
12. Patient consultation/discussions in secure area.			
13. Employee knows how and when to use: 1. Secure Data Transfer 2. EHR Broadcast Employee Name:			
14. Employee's Pager contains no PHI/PII Employee Name:			
15. Employee has completed ISSA training Employee Name:			

Privacy Round conducted by: _____

PRIVACY INVESTIGATION

- Fact-find
- Privacy Interview

PRIVACY INVESTIGATION

- Determining if it is a valid complaint
- Identifying the tools and resources you need to do an investigation

  - RPMS Sensitive Patient Tracking

  - BUSA = IHS User Security Audit (optional)

  - RPMS Scheduling, EHR, PCC, etc.

FACT FIND

- Was access to PHI/PII a “need-to-know” in the performance of employee’s duties
- Is access validated
- Was this a first time offense or repeated

PRIVACY INTERVIEW

- Formulate detailed questions

  - On (Date/time) you accessed the record of Gary Demo

    Under what authority did you access the record?

  - Do you know this patient personally?

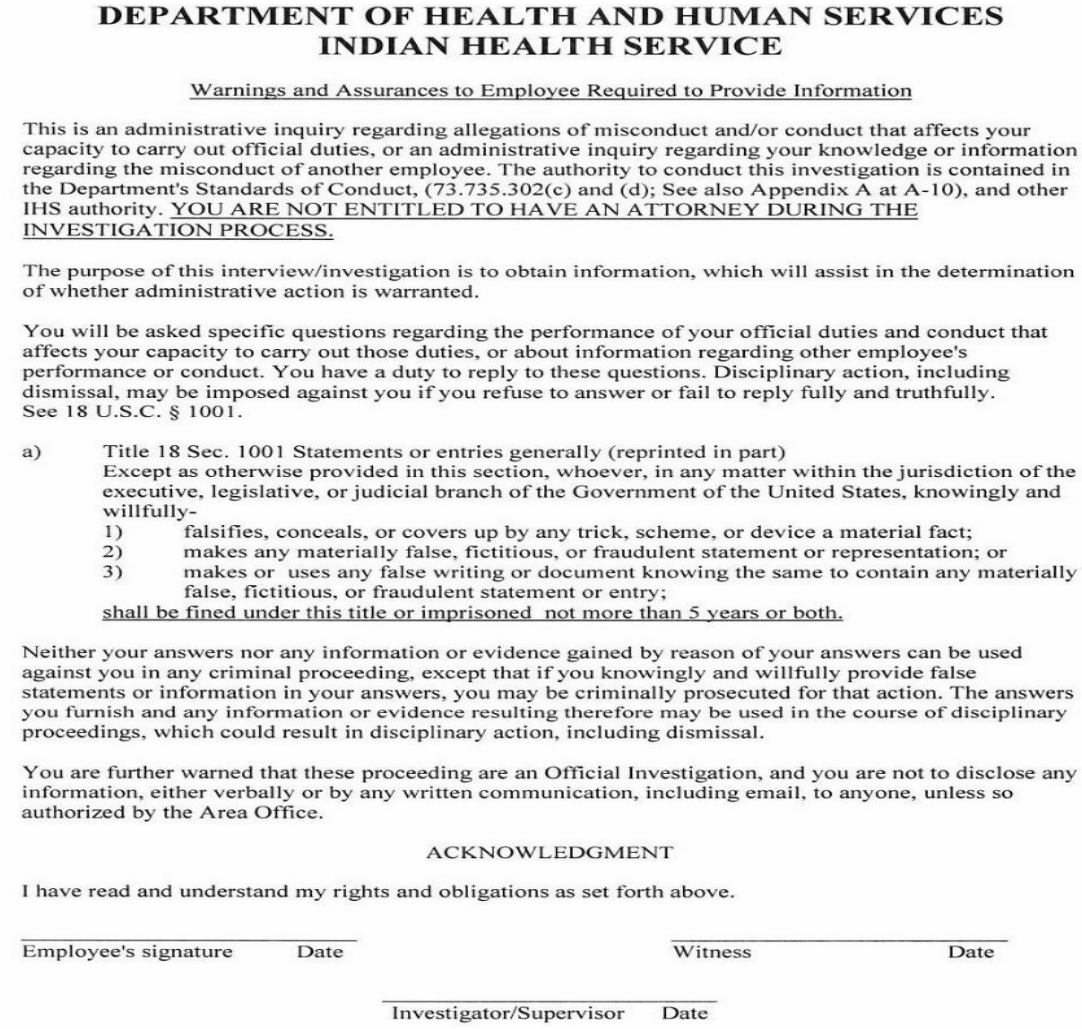
  - Did you disclose information on this person?

- Have a cascade of next questions to ask to obtain additional information. Example: Why did you do this?

OFFICIAL INVESTIGATION FORMS

Have the employee acknowledge and sign:

DHHS/IHS Warnings and Assurances to Employee Required to Provide Information



DEPARTMENT OF HEALTH AND HUMAN SERVICES
INDIAN HEALTH SERVICE

Warnings and Assurances to Employee Required to Provide Information

This is an administrative inquiry regarding allegations of misconduct and/or conduct that affects your capacity to carry out official duties, or an administrative inquiry regarding your knowledge or information regarding the misconduct of another employee. The authority to conduct this investigation is contained in the Department's Standards of Conduct, (73.735.302(c) and (d); See also Appendix A at A-10), and other IHS authority. YOU ARE NOT ENTITLED TO HAVE AN ATTORNEY DURING THE INVESTIGATION PROCESS.

The purpose of this interview/investigation is to obtain information, which will assist in the determination of whether administrative action is warranted.

You will be asked specific questions regarding the performance of your official duties and conduct that affects your capacity to carry out those duties, or about information regarding other employee's performance or conduct. You have a duty to reply to these questions. Disciplinary action, including dismissal, may be imposed against you if you refuse to answer or fail to reply fully and truthfully. See 18 U.S.C. § 1001.

a) Title 18 Sec. 1001 Statements or entries generally (reprinted in part)
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 or imprisoned not more than 5 years or both.

Neither your answers nor any information or evidence gained by reason of your answers can be used against you in any criminal proceeding, except that if you knowingly and willfully provide false statements or information in your answers, you may be criminally prosecuted for that action. The answers you furnish and any information or evidence resulting therefore may be used in the course of disciplinary proceedings, which could result in disciplinary action, including dismissal.

You are further warned that these proceeding are an Official Investigation, and you are not to disclose any information, either verbally or by any written communication, including email, to anyone, unless so authorized by the Area Office.

ACKNOWLEDGMENT

I have read and understand my rights and obligations as set forth above.

Employee's signature Date Witness Date

Investigator/Supervisor Date

INVESTIGATION FORMS

Obtain a written statement from the employee for the case file on the Declaration Form:

DECLARATION UNDER 28 U.S.C. 1746

Declaration

Pursuant to 28 U.S.C. 1746, I, _____declare as follows:

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. By my signature below I acknowledge that I have read and understood my statement consisting of this page and _____ other page. I have made all the changes and corrections I desire to make and have initialed each change I have made.

Executed on

_____ **Date**

_____ **Signature**

PRIVACY INVESTIGATION FORM

- Standardized investigation form to capture all data components needed for PAL and supervisor to use to validate and support disciplinary action when working with Human Resources Employee Relations/Labor Relations
- PALs do NOT recommend Disciplinary Action, but recommend Corrective Action to be taken. This is the responsibility of the Immediate Supervisor.

INVESTIGATION FORM

PRIVACY INVESTIGATION REPORT
(PRIVACY ACT, HIPAA, HITECH)

The privacy investigation report summarizes the investigation. It indicates who did the report, what was discovered, when and where the investigation was done, the full names of all individuals that provided information concerning the alleged breach violation. The report should verify and indentify:

1. Who is the alleged to have disclosed the information?

2. Name of Person receiving complaint?

3. What was the information disclosed?

4. What was the exact nature of the information disclosed?

5. When and where did the alleged violation occur?

6. How was the disclosure made? (I.e. verbally or directly from the physical record or electronic PHI?)

7. Which Privacy Law is cited for this incident? (Privacy Act, HIPAA or HITECH)
   - ☐ Privacy Act of 1974 (Check which System of Records)
     - ____ Medical, Health & Billing Records #09-17-0001
     - ____ Scholarship & Loan Repayment Records #09-17-0002
     - ____ Medical Staff Credential & Privilege Records #09-17-0003
     - ____ Sanitation Facilities Construction Individual Applicant Records
     - ____ Personal Health Records
   - ☐ HIPAA Privacy of 1996: ____ Privacy ____ Security ____ Transaction
   - ☐ HITECH

8. Name (s) of the individual (patient) whose records were disclosed?

MORE INVESTIGATION FORM

9. Name(s) to whom was the information disclosed?

10. Obtain details of the disclosure.

11. Did the individual (s) have a ***"Need to Know"*** to the information in order to perform duties?

12. Date and name(s) and title(s) of individuals interviewed.

13. Did the employee who made the alleged disclosure have Privacy Act & HIPAA Training? If so, when?

14. Did the training include confidentiality of medical records/Electronic Health Records?

FORM CONTINUED

Investigation Findings/Conclusion/Recommendation

Findings:

Conclusion:

Level of Offense: ( ) Low ( ) Medium ( ) High

Recommendation:

Signed: _____ Date: _____

Service Unit Privacy Liaison

LEVEL OF OFFENSE - EXAMPLES

Level of Offense, as recommended by the IHS Privacy Officer

- **High**
  - Unattended PIV – it compromises entire agency
  - Unauthorized disclosure or access of PHI/PII
  - Malice disclosure of PHI/PII
  - Sending unsecure email with PII/PHI to an outside agency unsecure
  - Inappropriate handling or sending of large patient listings
  - Unauthorized removal of PHI/PII from facility
  - Unprotected or unauthorized access to restricted area (HIM, server room)

LEVEL OF OFFENSE - EXAMPLES

- **Medium**

  Timely shredding of PHI/PII

  PHI/PII in garbage (BCMA labels, work copies)

  Unattended computer left logged on

- **Low**

  Internal email (one-to-one person) with HRN# or a patient name.

  Mistake or accidental disclosure of PHI/PII

  Unattended copy of PHI/PII left in copier/fax

  PHI/PII sent to Wrong printer

  Employee not wearing PIV card

AREA SANCTION POLICY

- Refer to Area Privacy Sanction Policy (if available) as incident categories may be defined

DEPARTMENT OF HEALTH AND HUMAN SERVICES
PUBLIC HEALTH SERVICE
INDIAN HEALTH SERVICE

OKLAHOMA CITY AREA INDIAN HEALTH SERVICE CIRCULAR NO. 2018-01

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT VIOLATION SANCTION POLICY

Sec.

1. Purpose

The regulations implementing the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with privacy or security policies and procedures of the entity, or the requirements of the Privacy or Security rules. See 45 C.F.R.§164.530(e)(1); 45 C.F.R.§164.308(a)(1)(ii)(C). Accordingly, the intention of the Oklahoma City Area Indian Health Service is to ensure the confidentiality and integrity of consumer and/or employee protected health information as required by law, professional ethics, and accreditation and/or licensure requirements. This policy establishes Oklahoma City Area policy, guidance, and standards for workforce performance expectations in carrying out the provisions of the HIPAA Privacy and Security rules and the corrective action(s) that may be imposed to address privacy and security violations.

2. Eligibility

All Oklahoma City Area employees, contracted employees, students and volunteers.

3. Definitions

A. Protected Health Information (PHI)

PHI is individually identifiable health information, including demographic information collected from an individual, that: (1) is created or received by a health care provider, health plan, employer, or healthcare clearinghouse; and (2) relates to the past, present, or

EXERCISE: SAMPLE COMPLAINT

- Patient files a complaint against a clinic clerk accusing the employee who is related to her, of accessing her medical record and obtaining PII to file a restraining order against her over a dispute involving land.

EXERCISE: SAMPLE COMPLAINT

- Nurse sent screen shots of patient information via unsecure email to a doctor who then forwarded to four (4) other staff members.

EXERCISE: SAMPLE COMPLAINT

- Patient requests a restriction to her medical record not to allow access to the entire family medicine clinic staff as she feels her privacy is violated every time she goes there for services

EXERCISE: SAMPLE COMPLAINT

- Facebook friend reported that an employee posted a picture that contained patient information on her Facebook page.

EXERCISE: SAMPLE COMPLAINT

- Anonymous employee submits concern of finding copies of patient documents in one of three (3) all-in-one copier/fax in the clinic.

EXERCISE: SAMPLE COMPLAINT

- Employee with 20 years of Federal Service accesses her teenager's medical records to see when her next appointment is.

PRIVACY PENALTIES

Civil monetary penalties under HIPAA:

- $100 per violation
- Capped at $25,000 per calendar year per violation

PRIVACY PENALTIES

Civil monetary penalties under HITECH:

- Up to $50,000 fine & 1 year imprisonment for knowingly obtaining or disclosing individually identifiable health information
- Up to $100,000 & 5 years imprisonment if done under false pretenses
- Up to $250,000 & 10 years imprisonment if done with intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm. Maximum penalty is $1.5 million under HITECH

PRIVACY IMPACT

- OCR posting of privacy breach on web site
- Lost of patient trust
- Reduction of workload as patients will go to another health care facility.

PRIVACY AWARENESS

- Send out bi-weekly/monthly emails to facility staff on a privacy topic
- Add a column on “Privacy Tips” to your facility staff newsletter
- Address minor incidents at staff meetings

PRIVACY AWARENESS

- Share appropriate methods of how to discard documents containing PII/PHI, such as patient ID bands, BCMA labels, reports, etc.
- Recognize individuals or departments that are protecting patient privacy

PRIVACY IS #1

- As PALs, it is important to stress to all levels of the organization that patient privacy is equally important as patient care

NOT OUR IHS PRIVACY THEME SONG!

PRIVACY REFERENCES

- Indian Health Manual Chapter 7 Part 2
  HIPAA Privacy Rule & the Privacy Act
- OMB Memorandum M-16-04

QUESTIONS

Gary M. Russell-King, HIM Chief

Northern Navajo Medical Center

Acting Navajo Area HIM Consultant & Privacy Coordinator

Phone: 505-368-6032 Fax: 505-368-6277

Email: gary.russell-king@ihs.gov