

Indian Health Service Privacy Act of 1974 and HIPAA Privacy of 1996

GARY M. RUSSELL-KING
CHIEF MEDICAL RECORDS ADMINISTRATOR
SHIPROCK SERVICE UNIT PRIVACY LIAISON



Course Learning Objectives

1. Provide an overview of the two Federal privacy laws
2. Know how IHS uses & discloses PHI for Treatment, Payment & Operations (TPO)
3. Define employee's role to protect patient privacy
4. Review what the monetary penalties for violating privacy
5. Learn how to report a privacy incident or compromises



The Privacy Act & HIPAA Privacy

SIMILARITIES:

- Both laws cover IHS medical records.
- Both have provisions that allow disclosures of health information without the patient's consent.
- Both privacy laws have similar policy & procedures.
- Both privacy laws have strict penalties.



Privacy Act of 1974

- Applies to all Federal record systems in Government agencies.
- Protects privacy of all U.S. citizens, regardless of age.
- Limits the collection, maintenance, use and dissemination.

Privacy Act does not cover:

- Deceased individuals (*HIPAA Privacy covers medical record for 50 years after death*)
- Tribal Governments operating under Public Law-93-638



5 - IHS System of Records

- Medical Staff Credential & Privilege Records
- Scholarship & Loan Repayment Records
- Medical, Health & Billing Records
- Sanitation Facilities Construction (OEHE)
- Personal Health Record (PHR)



Time to COWBOY-UP!



And take HIPAA by the HORNS!



H.I.P.A.A.

Health Insurance Portability & Accountability Act of 1996



HIPAA changed privacy access and transmission of data in health care.



3 Major Components of HIPAA

- Privacy Rule

- Paper or electronic (Hybrid)

- Security Rule

- Password management, COTS systems, computer access

- Transaction Code Sets

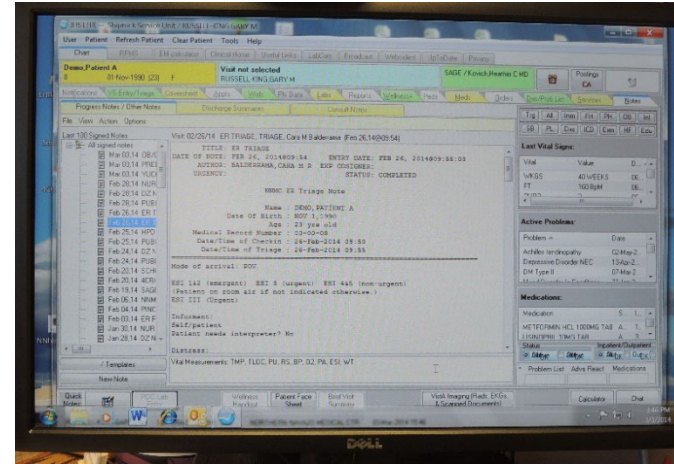
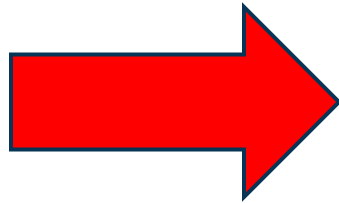
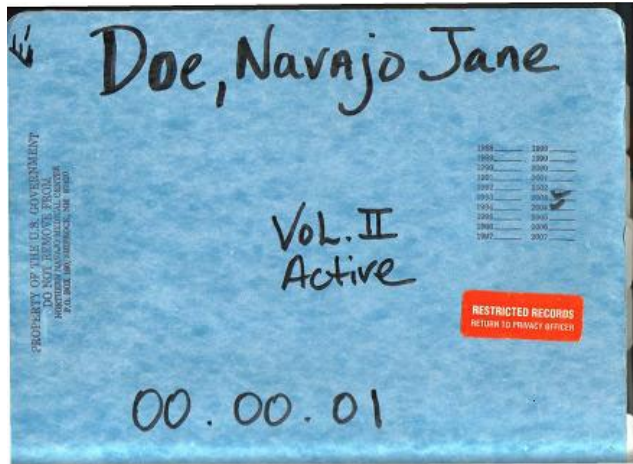
- Medical coding systems: ICD, CPT, HCPCS, CDT, DSM



What is PHI ?

Protected Health Information

PHI is a person's personal health and medical information



What is PII ?

Personally Identifiable Information

- Information which can be used to distinguish or trace an individual's identity.

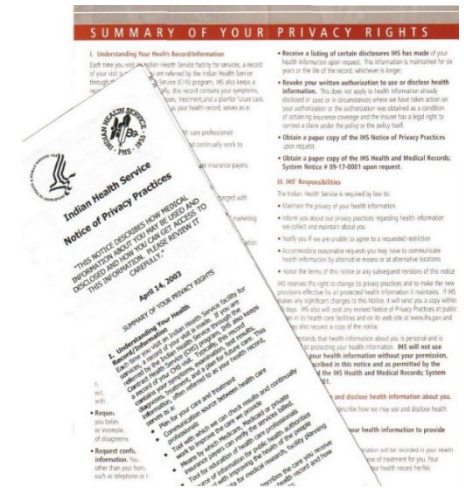
Examples: SSN, DOB, chart number, tribal enrollment number, etc.

- Refer to 18 PHI element under HIPAA Privacy



Notice of Privacy Practices

- Must inform all patients of both privacy laws and their rights.
- Informs how we will use their PHI for Treatment, Payment & Operation (TPO)
- Acknowledgement of receipt of NPP pamphlet.



HIPAA Privacy versus Privacy Act

- IHS will apply the Federal privacy law that best protects patient privacy.
- The Privacy Act of 1974 covers Government agency records.

Example: Many computer software systems and products may say they are “*HIPAA-Compliant*”, but are not “*Privacy Act Compliant*”.



HIPAA Privacy versus Privacy Act

- Request for Restrictions – A patient may request restriction on their medical record, however the restriction cannot impact TPO. Restrictions must be reviewed by OGC.
- If restriction is against an employee, patient is encouraged to document the incident so that the behavior can be addressed by the supervisor. *Locking up the record will not lock up the employee's lips.*



HIPAA Privacy versus Privacy Act

- Restrictions for the hospital directory at the time of admission are the only ones that can be approved locally. Hospital directories are public information.
- FYI - There is no way to restrict a medical record from all users as the system does not allow this.



Privacy Knowledge

- Basic knowledge of HIPAA Forms for Restriction, Corrections and alternate communications is good to have to assist the patient.
- Minors under the age of 18 have the rights to privacy under the Privacy Act. Parents do not have access to the child's record.



Use & Disclosures

IHS may use and disclose health information **without** the patient's written consent:

- Privacy Act routine uses
- HIPAA Privacy disclosure provisions



Use & Disclosures

- For reimbursement & payment purposes – *Covers the entire revenue cycle from Registration, billing, benefits coordination*

Examples:

- Coordination of referred care services through PRC.
- Copy of EHR note requested by health insurance carrier/auditor.
- Validating date of service on a health insurance claim for a health insurance plan.



Use & Disclosures - Reimbursement

- Contacting health insurance carrier to confirm coverage, providing name, DOB, SSN for validation.
- Contacting patient's employer to validate health insurance plan and/or coverage. *Use caution not to disclose condition or validate treatment.*
- Disclosing patient demographic information to a State Health Insurance Plan (Medicare/Medicaid) for eligibility and enrollment.
- Contacting another health care facility to obtain patient demographic for a patient in emergency room.



Use & Disclosures - Common

- To provide health care treatment
From IHS-to-IHS, contract facilities, 638 facilities, doctor's offices
- For health care operation
Risk manager, safety officer, patient advocate, CEO
- For Business Associates
Contractors, Tribal Programs, vendors (Pxyis, Chargemaster)
- Public Health Authorities
NM/AZ/Tribe Dept. of Health, CDC, NIH



Use & Disclosures - *Continue*

- Communication with family or caregivers
- Adults & Emancipated Minors with Personal Representative or Legal Guardians
- Funeral homes
- Correctional Institutions
- Law Enforcement
- Health Oversight Authorities

Joint Commission, CMS



Use & Disclosures - *Continue*

- Members of the Military
- Personal Health Record
- Health Information Exchange (HIE)
- Congressional Inquiry
- Interpreters
- Research (*approved by IRB*)
- Treatment Alternatives & Other Health-related benefits & services
- Food & Drug Administration
- Appointment Reminders
- Worker's Compensation
- Organ donor programs
- Disaster Relief



Accounting of Disclosure

- When copies of records are disclosed using a routine use/disclosure provision, an accounting of disclosure is REQUIRED by both privacy laws.
- Patients do have a right to know who IHS disclosed copies of their medical record to without their written consent.
- Send all requests for medical records to HIM.



42 CFR Part 2 – 42 CFR

- Protects Substance Abuse & Opioid treatment records.
- Requires patient's **written consent** to disclose, file, and re-disclose substance abuse and opioid treatment records, each time.



Interviewing Patients In Public Area

- Be sensitive to the patient's privacy and ask the patient's permission first when discussions are done in an open area.



Interviewing Patients In Public Area

- Private interview area and locations should be available.
- HIPAA requires that we offer reasonable accommodations.
- Remove your plexiglass. *Pandemic is over!*
- If using a sign-in clip board, limit to name and time only.



Handling Paper Documents with PHI/PII

- Shred extra copies of documents or RPMS reports containing PHI/PII, including worksheets.
- Refrain from printing up documents from RPMS or EHR as work copies.
- Do not remove any patient documents from the facility.
- Do not hoard copies of patient records.
- Don't keep copies of documents with PHI/PII.



Sending PHI/PII By E-Mail

- Never send PHI or PII using your Government email account employee.name@ihs.gov
- Always use Secure Data Transfer System – It's encrypted and secure.



The screenshot shows the login interface for the Indian Health Service Secure Data Transfer Service. At the top left is the IHS logo. The header reads "Indian Health Service" and "The Federal Health Program for American Indians and Alaska Natives". Below this is "Secure Data Transfer Service". The main text instructs users to enter their IHS username and password to sign in, or their email address if they are not an IHS user. A "User sign in" section contains fields for "Username" and "Password", a "Remember my username" checkbox, and a "Sign in" button. A "Forgot your password?" link is located below the sign-in button. To the right, there are "Quick User Guides" for "Accessing Secure Data (PDF)", "Sending Secure Data (PDF)", and "How to use Secure Data Transfer Service", with a note that the guides were last updated on 4/11/2013. A "Frequently Asked Questions" link is also present.



No Cell Phone Usage for Charting

- Personal cell phones are prohibited to use for:
 1. Taking photos of patients, work area, documents, computer screen
 2. Recording patient discussions
 3. Texting patients (appts or test results)
 4. Video recording of patients



Social Media

- Keep patient and facility information off of your personal social media accounts.
- The Public Information Officer (PIO) is the only person who can release any information to the public or news media.



Access to Patient Records

- Access to any patient record is based on “*need-to-know*” in the performance of your official duties:
 - a. RPMS applications (EHR, PCC, Moonwalk, etc.)
 - b. VistA Imaging
 - c. Health Information Exchange patient portal systems.
- Employees cannot access their own medical record in RPMS/EHR. Use PHR.



Reassure the Patient

- What if patient don't trust giving IHS personal information in fear that “**someone**” will get it:
 - *All information is secure in RPMS.*
 - *Employee access is based on need-to-know in the performance of their job.*
 - *Employees are required to take Privacy training yearly*
 - *All access to medical records is tracked electronically.*



RPMS Sensitive Patient Tracking

Administrative tool available to Privacy Liaison only.

Nosey employees beware!

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

Don't be accessing your family, friends or co-workers medical records.



Patient Privacy - Education

- Patients are unaware that their personal information is available in cyberspace when they disclose their information to businesses and by on-line internet activity.
- Certain agencies have access to other agency web sites.
Example: Courts of Jurisdiction have access to State Dept of Motor Vehicle data base.
- Encourage patients to question why personal data is needed (cell number, SSN, address) when asked from businesses and companies.



Patient Privacy

- Uphold privacy oath of confidentiality at all times in the performance of your job.
- Know when to avoid any possible confrontation, especially when interviewing friends and relatives in the performance of your job.
- Ask the person if they feel comfortable with you assisting them and if not, have someone else conduct the interview.



Privacy Complaint

- Complaint must be in writing with date, time, PHI or PII disclosed, to whom, any witnesses or proof.

Who What When

- Privacy Liaison cannot do an official investigation and corrective action cannot be taken unless complaint is in writing.
- Privacy complaint must be filed within 180 days (6 months) of the violation.



HITECH Act – Reporting Incidents

- Requires reporting of when PHI or PII is compromised electronically.
- Employees can report any privacy incidents by filing a CSIRT Report on-line.
- Do not report privacy incidents in iSTAR.



Report Privacy Incident

- Important for employees to report any suspicious activity or behavior involving patient privacy, ***to avoid the following . . .***



Shiprock Breach 2016



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 additional

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 training for all department staff

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 to protect your personal and

Criminal Penalties for Employee

- \$50,000 & 1 year imprisonment for knowingly obtaining or disclosing PHI.
- \$100,000 & 5 years if done under false pretenses.
- \$250,000 & 10 years if done with a personal intent.
- Enforced by the Department of Justice. Fines are paid directly to DOJ.



Privacy References

All IHS Agency Privacy Policies can be found on the www.ihs.gov web site:

- Indian Health Service Manual, Part 2, Chapter 7
“HIPAA Privacy & The Privacy Act”
- Office for Civil Rights (for Dept. of HHS)
www.hhs.gov/ocr/privacy



Know who your Service Unit Privacy Officials are

- Systems Manager (*CEO*)
- Privacy Liaison
- Area Privacy Coordinator
- IHS Privacy Officer:

Heather McClane, IHS Headquarters (240) 479-8521



Quality Patient Care includes ...



Respect of Patient Privacy



Ahee' Ahee'



Gary M. Russell-King

Chief Medical Records Administrator

Northern Navajo Medical Center

Phone: 505-368-6032

Email: gary.russell-king@ihs.gov

