



OVERVIEW
FEDERAL PRIVACY ACT AND
HIPAA PRIVACY RULE (HITECH ACT)

PRESENTATION TO THE 12TH
ANNUAL I/T/U HIM/BO PARTNERSHIP
CONFERENCE

March 23–25, 2010
Nashville, Tennessee

PRIVACY ACT AND HIPAA PRIVACY RULE

Bill Tibbitts

IHS Privacy Officer

Address: Suite 450 (OMS/DRA)
12300 Twinbrook Parkway
Rockville, MD 20852

Telephone: 301-443-1116

Email: william.tibbitts@ihs.gov





Privacy in the News—Personal Data Compromised

“Federal Security Snafus in 2006”

“Department of Veterans Affairs: A laptop and an external disk containing personal data on 26.5 million veterans and active-duty personnel were stolen last month from the home of a data analyst.”

“Social Security Administration: Social Security numbers and other data on about 200 people were stored and not properly secured on an employee-owned laptop that was stolen at a conference.”

“Internal Revenue Service: An IRS employee lost a laptop containing personal data on 291 agency workers and job applicants after checking it as luggage on an airplane flight.”

“Department of Energy: The apparent hacking of a server that took place last September but was just disclosed resulted in the potential compromise of data on more than 1,500 individuals.”

Source: ComputerWorld.com, June 19, 2006




Privacy in the News—Personal Data Compromised

- **February 18, 2009 (Computerworld)**
A travel reservations Web site used by several federal agencies was hacked last week, and it shunted unsuspecting users to a malicious domain, according to information that *Computerworld* has obtained. The site, GovTrip.com, is currently unavailable to federal employees through their offices' intranet; the version accessible via the public Internet is also offline.
UPDATE: GOVTRIP IS BACK ONLINE
- **March 31, 2009 (ComputerWorld.com)**
Kaiser fires 15 workers for snooping in octuplet mom's medical records; and another eight hospital employees disciplined for improperly accessing Nadya Suleman's files.



Privacy Act of 1974 (5 U.S.C. §552a)

- Limits collection of personal information
- No *secret* government record systems
- Right to see and correct one's own records
- *Safeguards* for the security and accuracy
- Civil and criminal remedies

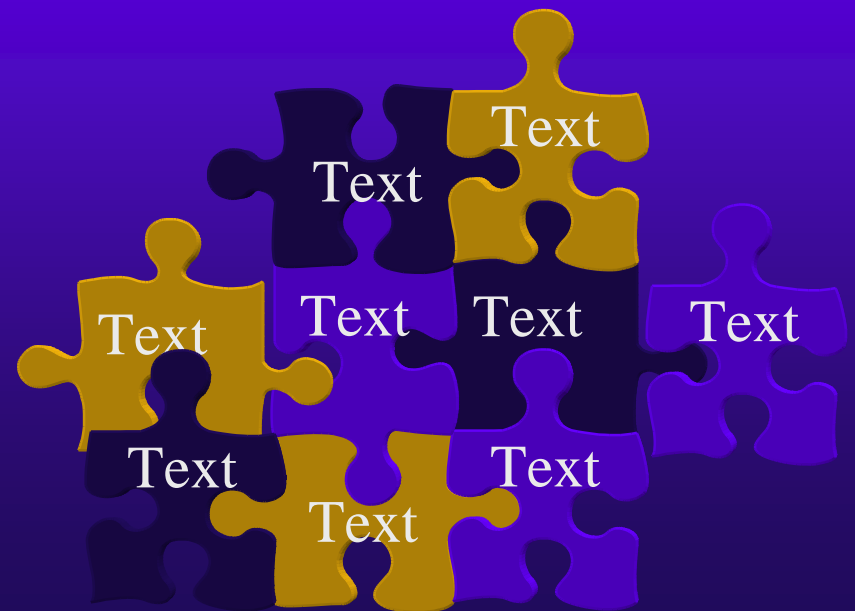


Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule (45 CFR §§160 & 164)

- Official Name: “Standards for Privacy of Individually Identifiable Health Information”
- **Provides** National standards for protecting PHI
- **Regulates** how covered entities “use and disclose certain PHI
- **Gives** patients more protection and control over their PHI
- **Sets** boundaries on the use and release of health records
- **Establishes** appropriate safeguards protecting the privacy of PHI

When is it a PA Records System?

- Group of records (more than one)
- Contains information about an individual
- Designed to be retrieved by name or other Personal Identifier





Privacy Act Record

- “any item, collection, or group of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as finger or voice print or a photograph.”

5 USC § 552a(a)(4)



HIPAA Privacy Rule

“Designated Record Set”

- A *group of records* maintained by or for a covered entity that is:
 - (i) the *medical* records and *billing* records about individuals maintained by or for a covered health care provider;
 - (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
 - (iii) used, in whole or in part, by or for the covered entity to make decisions about individuals.

(45 CFR 164-501)



HIPAA Privacy Rule “Record” – Continuation

- (2) The term “record” means any item, collection, or grouping of information that includes PHI and is maintained, collected, use, or disseminated by or for a covered entity. 45 CFR §164.501 – Definitions



Privacy Act Covers:

- **U.S. citizens**
- **Aliens lawfully admitted for permanent residence**

Privacy Act does *not* cover:

- **Nonresident aliens**
- **Deceased ***
- **Organizations**
- **Tribal Governments (PL93-638 excludes the 5 U.S.C. requirements (PA, FOIA, etc.))**



Limit Collection of Information

- Necessary to carry out an Agency function
- SSN—only when legally authorized otherwise ***voluntary*** (*OMB 07-16 requires all Federal Agencies to reduce or eliminate the SSN Usage)
- Inform individual of purpose and use of records collected: Privacy Act System of Record Notice Statement



Social Security Numbers (SSN)

- Before collection, must state whether: (1) disclosure is mandatory or voluntary, (2) by what statutory or other authority such number is solicited, and (3) what uses will be made of it. If no *statutory or law*, then SSN is voluntary by the individual.
- May *not* deny any right, benefit, or privilege provided by law due to refusal to provide SSN unless the SSN is required by federal statute.
- SSN is *voluntary* for Medical Records. SSN are required only for hiring, payroll, financial etc.

(*OMB 07-16 requires all Federal Agencies to start reducing or eliminating the SSN Usage or Justify Why the SSN is required*)



No Secret Government Records

- Publish a Privacy Act System Notice in the Federal Register *before* collecting data.
- System Notice: brief description of the type of record system and how the Government intends to manage and protect the system.
- IHS has four (4) SOR Notices
 - (1) Medical, Health and Billing Records
 - (2) Scholarship and Loan Repayment Program
 - (3) Medical Staff Credentials & Privileges Record
 - (4) Sanitation Facilities Construction Individual Applicant Records



← US Citizen

← Federal Agencies and its Contractors

PA
Of
1974
(5 USC 552a)

Computer
Matching and
Privacy Protection
Act of 1988

Government Wide
PA SOR Notices
(currently 21)

HHS
PA Regulation
(45 CFR 5b)

← Specifically defined
for HHS Agencies and
its Contractors

HIPAA Privacy /
Security Standards
45 CFR 160 & 164

IHS PA
System of Records
09-17-0001

(Medical, Health and
Billing Record)

IHS PA
System of Records
09-17-0002

(Scholarship and
Loan Repayment
Program)

IHS PA
System of Records
09-17-0003

(Medical Staff
Credentials &
Privileges Record)

IHS PA
System of Records
09-17-0004

(Sanitation Facilities
Construction Individual
Applicant Records)



Exceptions to Privacy Act

- The Privacy Act prohibits disclosure of PII without the written consent of the individual. However, there are 12 exceptions to this rule; three examples are listed below:
 - *Need to know within an agency* – this "need to know" exception authorizes disclosure of a record for necessary, official purposes within the Department
 - Example: Your supervisor may have a legitimate need to know information from your Official Personnel File in order to perform agency functions.
 - *Statistical data* – the record will only be used in statistical research or reporting in a non-identifiable format
 - *Routine use* – Disclosures outside of the Department that are compatible with the purpose for which the PII was collected. The agency publishes descriptions of routine uses in the Federal Register.



Privacy Act and HIPAA Effects

- SECURITY
- TRUST/QUALITY OF CARE
- PATIENT'S TRUST
- TRAINING
- ENFORCEMENT
- PENALTIES



The Importance of PHI Security

- Required by law
- Earns patient trust
- Privacy and security of information
- Sets federal minimum standards and safeguards to protect PHI
- Preempts weaker state laws
- Does not supercede federal laws, e.g., Privacy Act and Alcohol/Drug Abuse



Trust Impacts Quality of Care

- Detection and treatment of all conditions
- Accurate and complete health records
- Highest quality healthcare
- Reduces healthcare cost
- Patients do not move from one facility/provider to another



Trust Impacts Quality of Care

If patients *do not* trust us they...

- Do not seek treatment
- Give incomplete or inaccurate information
- Move from one provider to another
- Ask the provider not to record their actual condition



Earn Patient's Trust

- Know your policies and procedures and forms
- Respect patient's right to privacy
- Treat all records as if they are your own
- Be sensitive to privacy in all situations



Training Requirements

- IHS must provide training to all employees, volunteers, and contractors
- New employees must receive training no later than 30 days after entering on duty
- Department specific training for Health Record Staff, Medical Staff, and Administrative Staff
- When policies are revised
- Training must be documented and maintained for 6 years



Enforcement and Penalties for Noncompliance

- Civil Monetary Penalties
 - \$100 per violation
 - Capped at \$25,000 per calendar year per violation
 - Enforced by Office for Civil Rights (OCR)
 - Employees may face discipline up to and including termination
 - All employees may be held individually accountable



Penalties

- Up to \$50,000 fine and 1 year imprisonment for knowingly obtaining or disclosing individually identifiable health information
- Up to \$100,000 and 5 years imprisonment if done under false pretenses
- Up to \$250,000 and 10 years imprisonment if done with intent to sell, transfer, personal gain or malicious harm
- Enforced by U.S. Department of Justice (DOJ)



12 Provisions of Disclosure

- Employees with legitimate “need to know”
- Required under FOIA
- Routine use (not mandatory)
- Bureau of Census
- Statistical use (can’t identify individual)
- National Archives
- Civil or criminal law enforcement
- Compelling circumstances affecting health or safety of individual (must be justified)
- House of Congress (oversight capacity)
- Comptroller General (GAO activities)
- Court Order from a Court of Competent Jurisdiction (subpoenas signed by a *judge*)**
- Consumer Reporting Agency

** HHS OGC decision that only “federal courts” and not tribal courts are a Court of Competent Jurisdiction for *Privacy Act Purposes*.



Proper Use of PA Records

System Managers or designees *may* disclose records:

- *with* consent of individual (Get in writing, as narrow as appropriate)
- *without* consent of individual
 - * 12 exceptions (disclosures) from the Privacy Act
 - * Routine Uses for the IHS four (4) SORs (same applies for recording of information)

(Disclosures #3–#12 of PA and RU#1-25 of IHS Medical, Health & Billing Records, you *must* keep an Accounting. Includes: name and address of person/agency to whom disclosure is made, date, nature and purpose).



ACCOUNTING OF DISCLOSURES

- **When the Third-Party Requestor cites the Privacy Act, (we) *must* keep a record of/ or from the HIPAA Privacy Rule (TPO) :**
 - * **date, nature, and purpose of each disclosure,**
 - * **name and address of the person or agency to whom the disclosure is made.**
- **New: The HITECH Act now requires all Business Associates and its subcontractors that collect/ maintain PHI keep an AOD.**

(HIPAA Privacy Rule sets the same reqts. – 45 CFR 164.528)

Right to Access and Correct Data

- An individual has some degree of control over information government collects on them:

- * Right to Access

- Permits access; permits designating another individual; permits the reviewing of the record; *and permits a copy made of all or any portion thereof in a form “understandable” to the individual,* (PA-5 USC 552a(d))

- System Manager must reasonably satisfy themselves of an individual’s identity

- * Right to Correct/Amend

- change only factual information but cannot change matters of opinion

- * Right to Appeal

- denial of amendment
(Appeals at the lowest level:
CEO>>AD)

(HIPAA Privacy Rule sets the same reqts. - as defined in 45 CFR 164.522; 164.534; and 164.526)





HIPAA PRIVACY POLICIES AND PROCEDURES

- **IHS INDIAN HEALTH MANUAL (IHM) –**
- **PART 2, CHAPTER 7**
- **Approved on September 16, 2008**
- **>Exhibits A through T**
- **IHM is in compliance with the HIPAA Privacy Rule (45 CFR 164.530(i)(1) Standard: Policies and procedures)**
- **The IHS HIPAA Privacy Compliance Workgroup has reviewed the IHS HIPAA Forms in January 2009 – Submitted for Approval. The IHM is and will be reviewed this year pending the new HIPAA Provisions issued under HITECH Act.**



Health Information Technology for Economic & Clinical Healthcare (HITECH) Act Modifies HIPAA

- Accounting of Disclosures
 - Account for TPO from an electronic health record
 - Effective dates as early as JAN 2011 to JAN 2016
- Business Associates
 - Covered by the privacy and security rule and are subject to the same penalties as the covered entity (CE)



HIPAA Modified

- Encryption
 - Making PHI inaccessible or unreadable by an unauthorized user, e.g., encryption
- Sale of PHI
 - New prohibitions on the sale of PHI
 - Regulations due in August and planned effective date for compliance is Feb 2011
 - Be aware of the rule and avoid any type of sale of PHI for pharmaceutical and medical device marketing.



HIPAA Modified (Continued)

- **State Attorneys General**
 - **Can now bring lawsuits against practices on behalf of patients and receive costs and fees.**
- **Breach Notification**
 - **ARRA requires investigation, mitigation, correction, and reporting of any breach “wrongful use/disclosure of PHI”**
 - **New requirements for notifying breach victims and the federal government**
 - **Legislation extends to noncovered entities, primarily vendors of personal health records, e.g., Google**
 - **Increase in penalties for wrongful disclosure of PHI**
 - **ARRA introduces the concept of “willful neglect” – willfully disregarding knowledge of a violation**



Privacy Considerations

- Information collection:
 - Do you have a good reason for requesting the information?
 - Are you obtaining it in a safe manner so that it cannot be overheard or seen by others?
- Storage:
 - What computer security measures have been placed around the systems storing personal data?
 - Are you storing sensitive data in an encrypted format?
- Use:
 - Will you be using the information for the purpose it was provided?

(HIPAA Privacy Rule sets the same reqts. as defined in 164.530(c)(1))



Privacy Considerations

- **Distribution:**
 - Are personnel trained in the proper procedures regarding information disclosure?
 - Do you publicly display, use, or exchange personal information (especially Social Security Numbers) in your workplace?
- **Disposal:**
 - What is in your dumpster? ***
 - Are electronic/paper documents and databases containing personal information rendered unreadable prior to disposal?

***OCR settle agreement with CVS Pharmacy for \$2.25 million to toughen Disposal Practices (HIPAA Privacy Case)



Relationship to FOIA

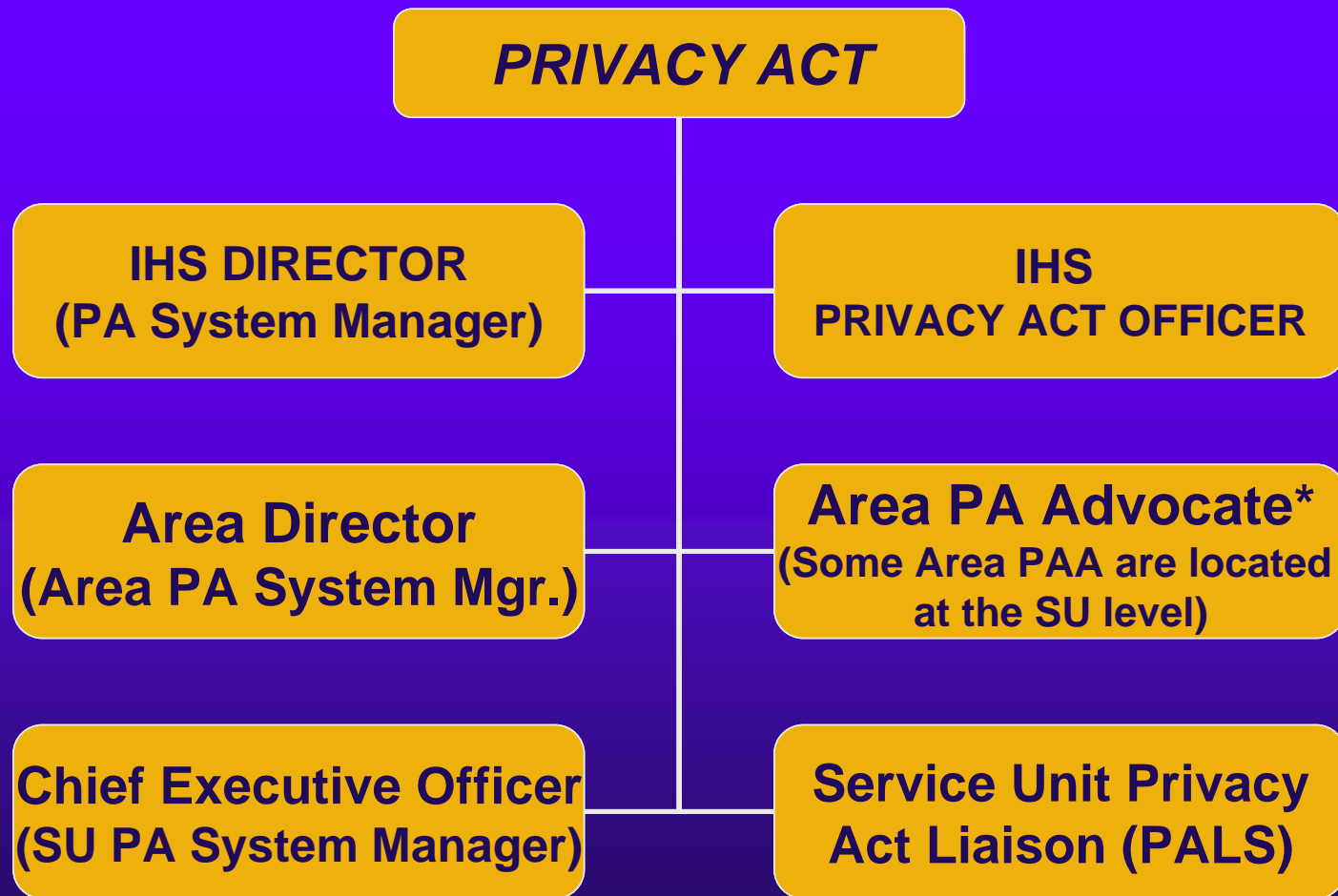
- **FOIA: *third-party requests*** (annual reporting)
- **Privacy Act: *first-party requests*** (no more reporting to FOIA)
- **FOIA: 9 Exemptions or Full/Partial Release vs. Privacy Act: 12 Exceptions or written consent of the individual**
- **FOIA Exemption 6 (Personal Privacy)**
 - *Parts of files may be withheld if disclosure “would constitute a clearly unwarranted invasion of personal privacy”
 - *Must consider personal privacy interest of individual (or even the immediate family) balanced against the public interest (Supreme Court Decision: **NARA v. Favish**)



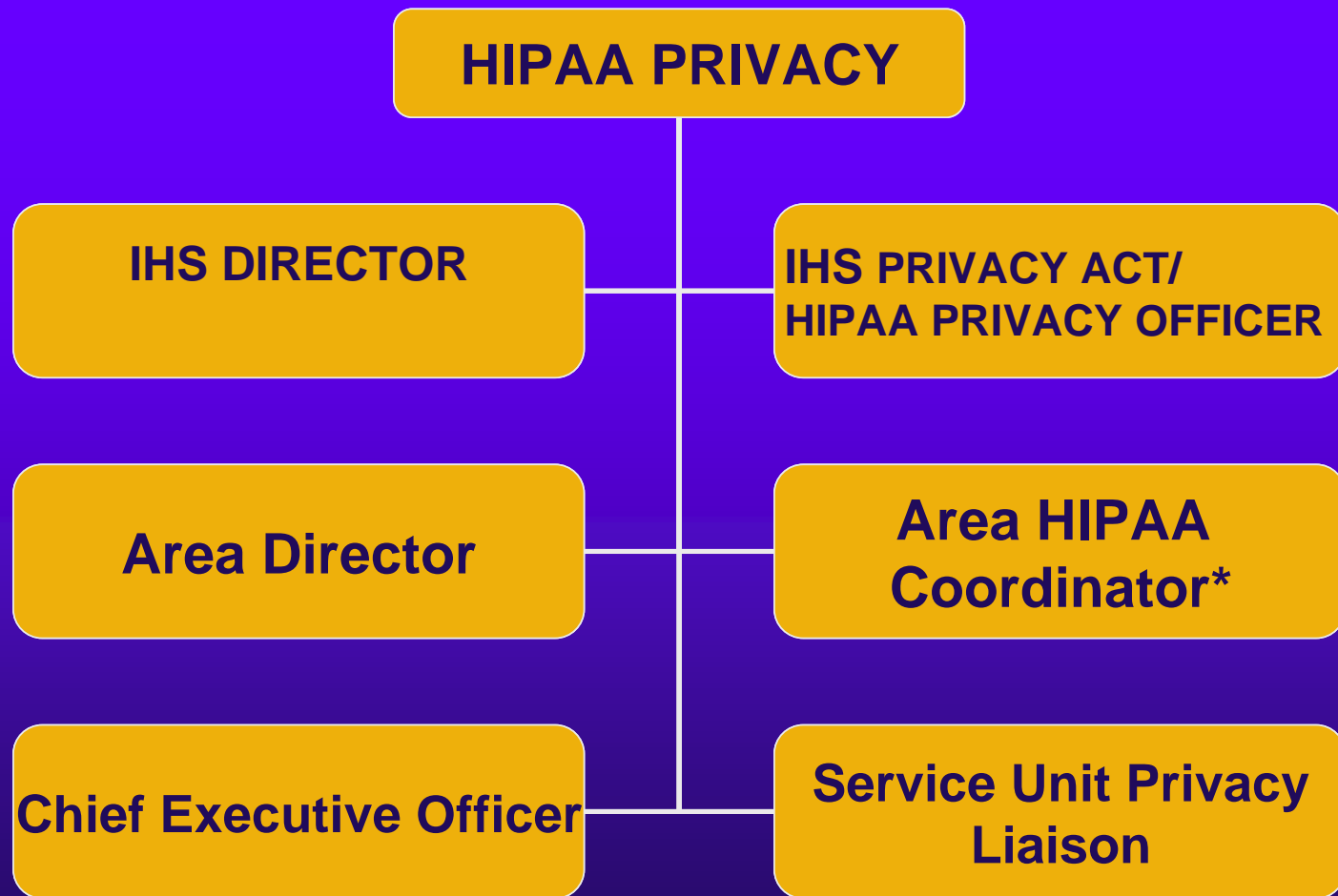
Supervisor's Notes

- They are *not* agency records when:
 - *Personal property of supervisor only
 - *Never shared with others (i.e., not circulated)
 - *Never passed to replacement supervisor
 - *memory joggers only
 - *no official use (i.e. not required by agency)
- Considered part of employee's personnel record (agency record) when:
 - *Used as basis for employment action
 - *Otherwise treated as official Agency records

IHS KEY PLAYERS



IHS KEY PLAYERS





Area Privacy Act Advocates (PAA)

- Coordinates with the IHS PA Officer
- Advises Area/SU on privacy issues and policy
- Supports and provides Area/SU level training
- Investigate and resolve local PA privacy complaints at the lowest level (SU>AD)



Area HIPAA Coordinators

- Coordinates with the IHS Privacy Act/HIPAA Privacy Officer
- Advises Area/SU on HIPAA Privacy issues and policy
- Supports and provides Area/SU level training
- Investigate and resolve local HIPAA Privacy complaints at the lowest level (SU>AD)

System Manager Responsibilities

- Tracks location of covered records
- Staff Training: inform users of requirements
- Security: enforce safeguards
- Approval/denial of access
- Track access and amendments to records
- Ensure records are complete/accurate/timely/relevant
- Monitor contractor compliance
- Follow IHS records schedule
- Ensure Notification Statement is on data collection forms
- Report requirements: annual updates/reports





Computer Data: When it is a Record?

- If a computer system is set up for use, or is used in practice, to retrieve information by individual identifiers (name, SSN, assigned tracking number) and the system contains personal information, the computer data is covered as a Privacy Act system of records.

(Example[s]: Resource and Patient Management System [RPMS] and Electronic Health Record)

Civil Remedies (PA vs. HIPAA)

WHICH VIOLATIONS COULD LEAD TO CIVIL PENALTIES

- Unlawful refusal to amend a record or grant access
- Failure to maintain accurate, relevant, timely, and complete data
- Failure to comply with any Privacy Act and/or HIPAA Privacy Rule provision or agency rule that results in any adverse effect





Civil Remedies (PA vs. HIPAA)–Continued

Penalties:

- Actual Damages
- Attorney Fees
- Removal from Employment
- Under HIPAA (PL 104-191, Title II, Part C Administrative Simplification, Sec. 1176), it states any person who violates a provision of this part *shall impose a penalty of not more than \$100 for each violation* except that the total amount imposed on the person for all violations of an identical requirement or prohibition during a CY may not exceed \$25,000.

Criminal Remedies (PA vs. HIPAA)

- Applies to individual(s)
- Fine up to \$5,000 + court costs
 - *If an officer or employee of agency knowingly releases records improperly to a person not entitled to receive
 - *Willfully maintains PA system without publishing in FR
 - *Knowingly requests or obtains a record about individual under false pretenses





Criminal Remedies (PA vs. HIPAA)–Continued

- Under HIPAA (PL 104-191, Title II, Part C Administrative Simplification, Sec. 1177), it states a person who knowingly violates this part (wrongfully uses, obtain or discloses) ***shall be punished and fined not more than \$50,000, imprisoned not more than 1 year, or both; if the offense is committed under false pretenses, be fined not more than \$100,000, imprisoned not more than 5 years, or both; and if the offense is committed with intent to sell, transfer, or use PHI for commercial advantage, personal gain, or malicious harm, be fined not more than \$250,000, imprisoned not more than 10 years, or both.***
- **NEW:** HITECH Act increases the civil and criminal penalties



IHS PRIVACY ACT WEB SITE

- **Go to: www.ihs.gov/**
- **Click the Letter “P” on the A to Z Index Block**
- **Click on: Privacy Act**

Intranet Web site: home.ihs.gov

- **Click on Administration and Management Resources and then on Privacy Act Office (Training Material Only)**



HHS PRIVACY TRAINING

- **Go to:**
<http://intranet.hhs.gov/infosec/education.html>
- **Scroll Down to Training Courses –**
- **Click on: Privacy Awareness Training**

Note: If you want credit for this, go to the HHSU Learning Lab and take the course online. The Web address is:
<https://lms.learning.hhs.gov>



IHS HIPAA WEB SITE

- Go to: www.hipaa.ihs.gov/
- Scroll Down on Hot Topics Listing
- On the left-side of the welcome screen is link to the hipaa training
- **NPP; FORMS; POLICIES/PROCEDURES ETC.**

ANY QUESTIONS



A Tribe of the Wind River Reservation - Shoshone-Bannock Tribes of the Fort Hall Reservation of Idaho - Shoshone-Paiute Tribes of the Duck Valley
Shoshone Tribes of the Lakeview Reservation - Shoshone Tribes of Alaska - Shoshone Villages - Shoshone Tribes of the Shoshone Reservation - Shoshone
of Utah - South River Rancheria - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation
of Chippewa Indians - South Dakota Village - Southern Ute Indian Tribe of the Southern Ute Reservation - Spirit Lake Tribe - Spokane Tribes of the

Spokane Reservation - Squamish Indian Tribe of the Squamish Indian Reservation - St. Croix Chippewa Indians of Wisconsin - St. Croix Reservation
of New York - Standing Rock Sioux Tribe of North Dakota - Standing Rock Community Association - Standing Rock Community Association - Standing Rock
Indians of Wisconsin - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation
of the Fort Madison Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation - Sisseton Reservation

THANK YOU