OVERVIEW
FEDERAL PRIVACY ACT AND HIPAA PRIVACY RULE

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

APRIL 17-19, 2007

JOHN ASCUAGA'S NUGGET HOTEL

RENO, NEVADA

PRIVACY ACT AND HIPAA PRIVACY RULE

Bill Tibbitts

IHS Privacy Act Officer

Address: Suite 450 (OMS/DRA)

12300 Twinbrook Parkway

Rockville, MD 20852

Telephone: 301-443-1116

Email: william.tibbitts@ihs.gov

Privacy Act of 1974
(5 U.S.C. §552a)

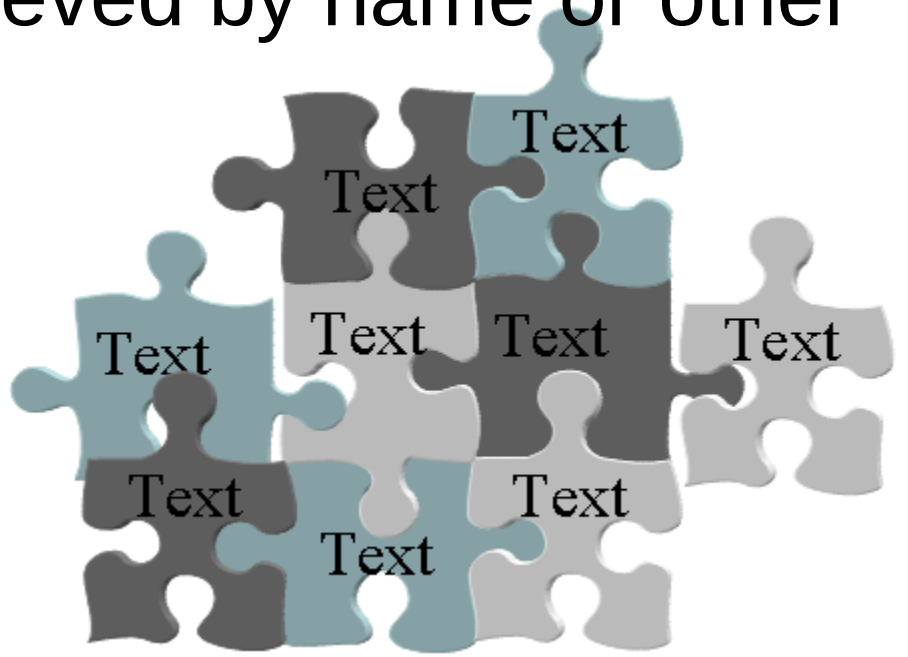
- Limits collection of personal information
- No *secret* Government record systems
- No *secret* use of Government records
- Right to see and correct one's own records
- *Safeguards* for the security and accuracy
- Civil and Criminal remedies

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 protected health information (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 Privacy Act (PA) Records System?

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



PA 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.

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

"HMMM – sounds like a Privacy Act Record to me."

Privacy Act Covers:

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

Privacy Act does *not* cover:

- Non-resident 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*
- 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 statute or other authority such number is solicited, and (3) what uses will be made of it. If no statute 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.

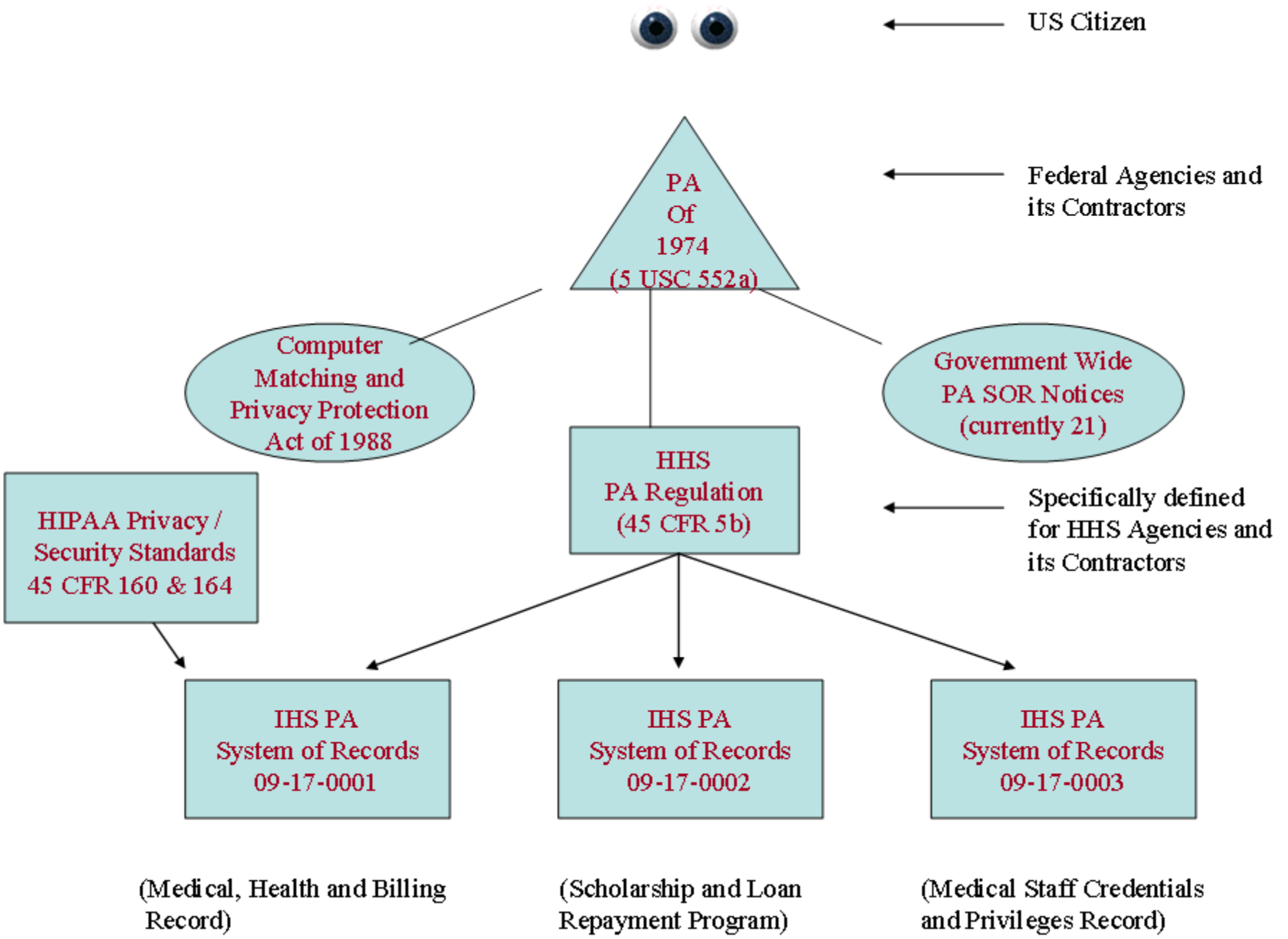
No Secret Government Records

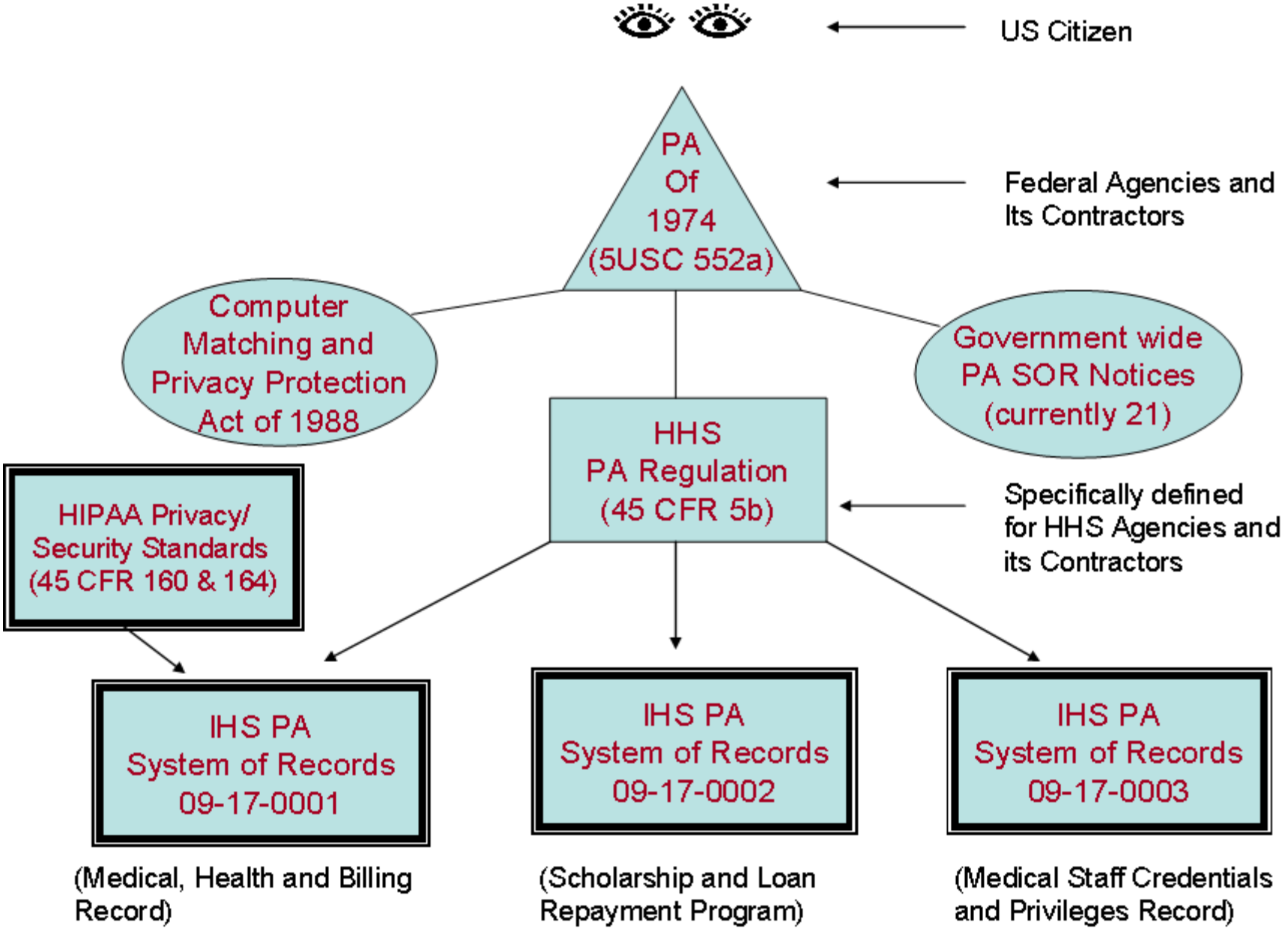
- Publish a Privacy Act System Notice in the Federal Register *before* collecting data.
- System Notice: brief description of the type of record system and how the Government intends to manage and protect the system.
- IHS has three System or Record (SOR) Notices:

  (1) Medical, Health and Billing Records,

  (2) Scholarship and Loan Repayment Program

  (3) Medical Staff Credentials and Privileges Record


US Citizen
PA
Of
1974
(5 USC 552a)
Federal Agencies and
its Contractors
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
IHS PA
System of Records
09-17-0002
IHS PA
System of Records
09-17-0003
(Medical, Health and Billing
Record)
(Scholarship and Loan
Repayment Program)
(Medical Staff Credentials
and Privileges Record)


US Citizen
PA
Of
1974
(5USC 552a)
Federal Agencies and
Its Contractors
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
IHS PA
System of Records
09-17-0002
IHS PA
System of Records
09-17-0003
(Medical, Health and Billing
Record)
(Scholarship and Loan
Repayment Program)
(Medical Staff Credentials
and Privileges Record)

Parts of a System Notice

- Number
- Name
- Security classification
- Location
- Who it covers
- Types of Records
- Authority for Collection
- Purpose of System
- Routine Uses: Third-Party Disclosures
- Storage
- How Information is Retrieved
- Safeguards: Authorized users, Physical and Procedural Safeguards
- Retention and Disposal
- System Manager(s) address
- Notification Procedure
- Record access procedure
- Authority for Collection
- Contesting Record Procedure
- Record Source Categories
- Exemptions

No Secret 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 provisions (disclosures) from the Privacy Act
  - Routine Uses for the IHS three SORs (same applies for recording of information)

(Disclosures #3-#12 of PA and RU#1-24 of IHS Medical, Health and Billing Records, you *must* keep an accounting, includes: Name and address of person/ agency to whom disclosure is made, date, nature, and purpose)

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.

Accounting Of Disclosures

- When the Third-Party Requestor cites the Privacy Act (we) *must* keep a record of:
  - date, nature, and purpose of each disclosure
  - name and address of the person or agency to whom the disclosure is made.

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

Right to See and Correct Data

- An individual has some degree of control over information government collects on them:
  - **Right to Access** (except for the ten exemptions)
    - System Manager must reasonably satisfy themselves of an individual's identity
  - **Right to Correct/Amend**
    - May change only factual information and cannot change matters of opinion
  - **Right to Appeal** denial of amendment (Keep 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)

Safeguards

- Must collect information from individual to greatest extent possible that is consistent with the Purpose.
- Establish appropriate administrative, technical, and physical safeguards to insure security (physical, IT, and confidentiality)
- Do risk analysis every three years or less

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

Relationship to FOIA

- FOIA: Third-party requests (annual reporting)
- Privacy Act: First-party requests (annual reporting to FOIA)
- FOIA: Nine Exemptions or Full/Partial Release vs. Privacy Act: 12 Exceptions or written consent of the individual
- FOIA Exemption 6 (Personal Privacy)

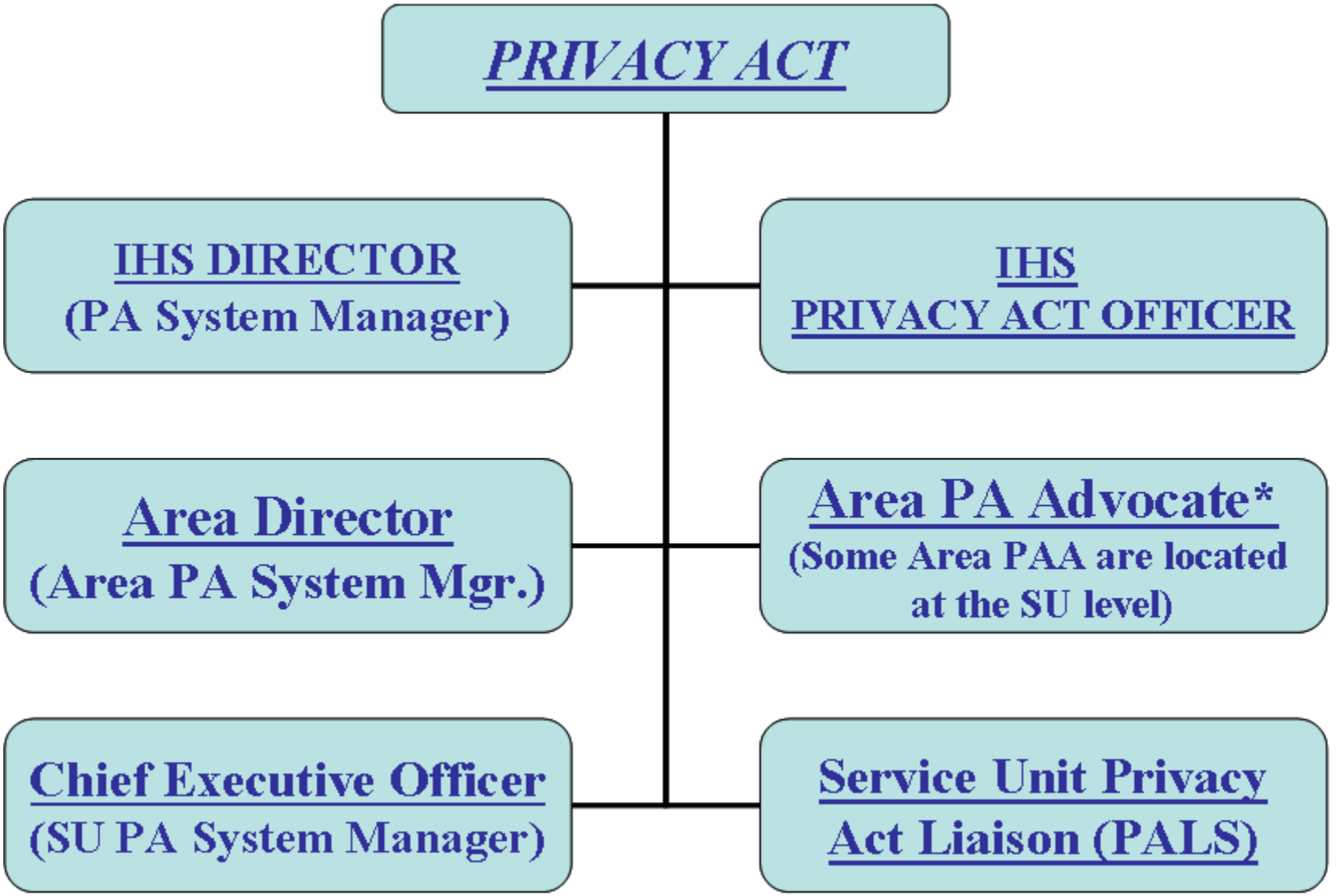
  *Parts of files may be withheld if disclosure “would constitute a clearly unwarranted invasion of personal privacy”

  *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



Area Privacy Act Advocates (PAA)

- Coordinates with the IHS PA Officer
- Advises Area/Service Unit (SU) on PA and HIPAA Privacy issues and policy
- Supports and provides Area/SU level training
- Investigate and resolve local PA & 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 to be used, 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)

WHAT VIOLATIONS LEAD TO CIVIL PENALTIES

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

Civil Remedies (PA vs. HIPAA) - Continuation

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 Federal Register
  - Knowingly requests or obtains a record about individual under false pretenses

Criminal Remedies (PA vs. HIPAA) - Continuation

- Under HIPAA (PL 104-191, Title II, Part C Administrative Simplification, Sec. 1177), it states a person who knowingly violates this part (wrongfully uses, obtains, 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.*

IHS PRIVACY ACT WEBSITE

- Go to: www.ihs.gov/
- Click on: Resources for IHS Management
- Click on: Privacy Act

Intranet Web site: home.ihs.gov

- Click on Privacy Act (Training Material Only)