HIPAA Privacy and Security 101
The Basics of the HIPAA Privacy and Security Rules

Session Facilitator

Marti Arvin
Chief Compliance Officer
UCLA Health System and the David Geffen School of Medicine
GROUND RULES

- THIS IS A BASIC SESSION
  - If you expected something beyond the basics this is not the session to attend
  - You are welcome to stay
  - However, if you stay you cannot write on your evaluation that this was too basic

- Please turn your cell phones and pagers to vibrate or off.

Agenda

1. Security Rule – 1:30 to 2:05 pm
2. Privacy Rule Part 1 - 2:05 pm 2:45 pm
3. Break – 2:45 to 3:00 pm
4. Privacy Rule Part 2– 3:00 to 4:30 pm
Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- Health insurance access, portability, and renewal
- Attempts to prevent healthcare fraud and abuse
- Allows health insurance tax deduction for self-employment
- Promotes administrative simplification

Security Standards
Scope

- All electronic PHI (ePHI)
- In motion AND at rest (created, received, maintained or transmitted)
- To ensure confidentiality, integrity, and availability
- To protect against reasonably anticipated threats or hazards, and improper use or disclosure

Definitions

- Confidentiality
- Integrity
- Availability
- Reasonably Anticipated
Who must comply?

A Covered Entity

- **Health plan** - A plan that provides or pays the cost of medical care. Includes Medicaid, Medicare and self-funded plans. Does NOT include small health plans with receipts less than 5M/yr.

- **Health care clearinghouse** - Process health information from a non standard content into standard data elements or to a standard transaction. Such as billing services, health information systems, etc. NOT TPAs.

- **Health care provider** - A provider of medical or health services such as SNFs, home health, hospitals, physician clinics, etc. that transmit in electronic form.

Security vs. Privacy

- Closely linked

- **Security enables** Privacy

- **Security Rule scope** – addresses electronic PHI

- **Privacy scope** – addresses electronic, paper and oral PHI
Security Threats

- Active, evolving, never static

- **Goal:** Controlling threats, by reasonable measures
  - people oriented
  - hackers, viruses, insiders, disgruntled persons
  - must be *actively* managed by IT professionals

Standards/Safeguards

45 CFR 164.308

**Administrative**

**Physical**

**Technical**
Implementation Specifications

- Are more specific measures that pertain to a standard
- Required (R) – Covered entity MUST implement the specification in order to successfully implement the standard
- Addressable (A) – Covered entity must:
  - Consider the specification, and implement if reasonable and appropriate
  - If not reasonable and appropriate, document reason why not, and what WAS done in its place to implement the standard

Administrative Safeguards 45
CFR 164.308

- Security Management Process - 164.308(a)(1)
  - Risk Management (R)
  - Sanction Policy (R)
  - Risk Analysis (R)
  - Information System Activity Review (R)

- Assigned Security Responsibility - 164.308(a)(2) (R)

- Workforce Security – 164.308(a)(3)
  - Authorization and/or Supervision (A)
  - Workforce Clearance Procedure (A)
  - Termination Procedures (A)
Administrative Safeguards, cont.

- **Information Access Management - 164.308(a)(4)**
  - Isolating Health Care Clearinghouse Function (R)
  - Access Authorization (A)
  - Access Establishment and Modification (A)

- **Security Awareness and Training - 164.308(a)(5)**
  - Security Reminders (A)
  - Protection from Malicious Software (A)
  - Log-In Monitoring (A)
  - Password Management (A)

Security Standards Training

- Awareness training for all employees & staff
- Vulnerabilities of the health information in the entity’s possession
- Policies/procedures that must be followed to ensure the protection of the information
- Periodic security reminders
- Education concerning computer viruses
- Education in login procedures and password management
Administrative Safeguards, cont.

- **Security Incident Procedures** – (164.308(a)(6))
  - Response and Reporting (R)
- **Contingency Plan** - 164.308(a)(7)
  - Data Backup Plan (R)
  - Disaster Recovery Plan (R)
  - Emergency mode Operation Plan (R)
  - Testing and Revision Procedure (A)
  - Application and Data Criticality Analysis (A)
- **Evaluation** - 164.308(a)(8) (R)
- **Business Associate Contracts and Other Arrangements** - 164.308(b)(1)
  - Written Contract or Other Arrangement (R)

Physical Safeguards
45 CFR 164.310

- **Facility Access Controls** - 164.310(a)(1)
  - Contingency Operations (A)
  - Facility Security Plan (A)
  - Access Control and Validation Procedures (A)
  - Maintenance Records (A)
Physical Safeguards, cont.

- Workstation Use - 164.310(b) (R)
- Workstation Security – 164.310(c) (R)

Physical Safeguards, cont.

- Device and Media Controls - 164.310(d)(1)
  - Disposal (R)
  - Media Re-Use (R)
  - Accountability (A)
  - Data Backup and Storage (A)
Technical Safeguards 45 CFR 164.312

- **Access Controls - 164.312(a)(1)**
  - Unique User Identification (R)
  - Emergency Access Procedure (R)
  - Automatic Logoff (A)
  - Encryption and Decryption (A)

- **Audit Controls - 164.312(b) (R)**

- **Integrity - 164.312(c)(1)**
  - Mechanism to Authenticate Electronic Protected Health Information (A)

Technical Safeguards, cont.

- **Person or Entity Authentication - 164.312(d) (R)**

- **Transmission Security - 164.312(e)(1)**
  - Integrity Controls (A)
  - Encryption (A)
Bottom Line...

- Consideration **MUST** be given to implementing **all** standards
- Using a combination of required and addressable implementation specifications and other security measures
- Need to document choices
- This arrangement allows the covered entity to make its own judgments regarding risks and the most effective mechanisms to reduce risks

Bottom Line...Your organization?

![Diagram](image.png)

Requirements, Responsibilities and Expectations
Common Foundation...

A common foundation to address...

• Regulations, laws, requirements
  HIPAA, PCI, SOX, FERPA, NIH, contracts, federal and state legislation…

• Expectations
  Shareholders, customers, sponsors, partners/collaborators, our constituents, media, the public…

• Efficiency
  Unified approach is more effective, less confusing, easier to understand

Well designed polices and standards are ultimately an enabler

Numerous areas, similar requirements and expectations

---

Policies you should consider

Information Security and Technology Policy and Standards Map

<table>
<thead>
<tr>
<th>General</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Responsibility IS P5001</td>
</tr>
<tr>
<td>Business Continuity Planning and Disaster Recovery IS P5002</td>
</tr>
<tr>
<td>Intellectual Property (IP) IS P5003</td>
</tr>
<tr>
<td>Policy Exceptions IS P5004</td>
</tr>
<tr>
<td>Sanction Policy IS P5005</td>
</tr>
<tr>
<td>Security Incident Policy IS P5006</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Accounts and Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts and Acceptable Use IS P5007</td>
</tr>
<tr>
<td>Passwords IS P5008</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Service IS P5010</td>
</tr>
<tr>
<td>Web Sites IS P5011</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Centers and Facilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Facility Security IS P5009</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Computing Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation and Computing Devices IS P5012</td>
</tr>
<tr>
<td>Server Computing Devices IS P5013</td>
</tr>
<tr>
<td>Protection from Malicious Software IS P5014</td>
</tr>
<tr>
<td>Backup and Retention of Data IS P5015</td>
</tr>
<tr>
<td>Inventory, Tracking, Discarding or Redeploying Computing Devices or Media IS P5016</td>
</tr>
</tbody>
</table>
## Details in the Policies you want to consider

**Information Security and Technology Policy and Standards Map**

<table>
<thead>
<tr>
<th>General</th>
<th>Accounts and Usage</th>
<th>Network Services</th>
<th>Competing Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Planning and Disaster Recovery (IS P092)</td>
<td>- Consistency and Relevancy</td>
<td>- Network Service</td>
<td>- Implementation Documentation</td>
</tr>
<tr>
<td>- Gap analysis</td>
<td>- Network Service Flexibility for University</td>
<td>- Compliance, Use &amp; Licensing</td>
<td>- System Maintenance</td>
</tr>
<tr>
<td>- Risk Assessment</td>
<td>- Network Use</td>
<td>- Physical System Access</td>
<td>- Security Policies</td>
</tr>
<tr>
<td>- Business Impact Analysis</td>
<td>- Monitoring/Testing</td>
<td>- Software</td>
<td>- Information Technology</td>
</tr>
<tr>
<td>- Continuity and Resilience Strategy</td>
<td>- Network Traffic</td>
<td>- Firewalls</td>
<td>- Technology</td>
</tr>
<tr>
<td>- Maintenance and Availability</td>
<td>- Guest/Temporaty Network Use</td>
<td>- Enforcement</td>
<td>- Security, Compliance</td>
</tr>
</tbody>
</table>

**Intellectual Property (IS P052)**

- Understanding Copyright and IP Protection
- Protecting and Managing Electronic Information
- Peer To Peer Programs

**Password Policies (IS P059)**

- General
- C#I, Enterprise Access

**Data Centers and Facilities**

- Data Center Security (IS P089)
- Standards

**Security Incident Policy (IS P084)**

- Standards

**Security Incident Policy (IS P084)**

- Standards

**Protection from Malicious Software (IS P085)**

- Advanced and Preparation of Incident
- Technical Standards for Anti-Virus, Anti-Spyware and Parental Control Software
- Software Standards

**Strategy for Policy and Standards Implementation**

1. **Educate and Encourage Use**
   - Training
   - Awareness
   - Consulting

2. **Improve Compliance using**
   - Consulting
   - Auditing and Monitoring, Assessment, Adjustment
   - Enforcement

3. **Maintain Policy Relevance using**
   - Self Assessment/audit
   - Feedback
   - Adjustment
Real Life Issues

- Ongoing training and monitoring
  - Business Associates
  - Physicians and Physician Staff

- Keeping up with both privacy and security rules and laws

- Keeping in compliance without shutting down operations

Electronic PHI Breach
Security Conclusion

1. **On-going process of continuous improvement**, no guarantees.
2. **Diligence, education, awareness (at all levels)** can provide a defensible position for compliance risk while supporting business operations.
3. **Policies and standards** are a key part of this.

**Final Points to consider:**

1. Tone from the Top
   - **Most important**: Executive leadership by example
2. Training and Awareness!
   - **More important** than fancy technology
3. Technology
   - **Use technology effectively**, not as a substitute for #1 or #2!

Privacy Standards

I said to shred the document not the person reading it!
What’s protected?

- All medical records and other individually identifiable health information held or disclosed by a covered entity in any form, whether communicated electronically, on paper, or orally.

HIPAA Identifiers

- A) Names;
- (B) Street address, city, county, precinct, zip code, and equivalent geo-locations;
- (C) All elements of dates (except year) for dates directly related to an individual and all ages over 89;
- (D) Telephone numbers;
- (E) Fax numbers;
- (F) Electronic mail addresses;
- (G) Social security numbers;
- (H) Medical record numbers;
- (I) Health plan ID numbers;
- (J) Account numbers;
- (K) Certificate/license numbers;
- (L) Vehicle identifiers and serial numbers, including license plate numbers;
- (M) Device identifiers/serial numbers;
- (N) Web addresses (URLs);
- (O) Internet IP addresses;
- (P) Biometric identifiers, incl. finger and voice prints;
- (Q) Full face photographic images and any comparable images; and
- (R) Any other unique identifying number, characteristic, or code.
How can a covered entity use and disclose PHI?

- REMEMBER, every time you look at, touch, share, disclose or doing anything else with PHI you must either have the patient’s authorization or meet a HIPAA exception.

- The exception you can use will depend on the purpose for which you are looking at, touch, sharing or disclosing the PHI.

- Exceptions
  - TPO
  - Other statutory exceptions
U & Ds without the patient’s explicit permission.

- Treatment, Payment & Health Care Operations. 164.506
- As required by law. 164.512
- Marketing & fundraising (pursuant to strict limitations)

U & Ds for TPO

- Examples:
  - A healthcare provider can discuss the patient’s case with her colleagues to determine the best course of treatment
  - A health plan can share information with the nursing home regarding payment for services
  - A compliance office can obtain charts for compliance audits
U & Ds that do not require an authorization

- Mandatory disclosures:
  - HIPAA only mandates disclosures in two instances. 164.502(a)
    - To the patient with some exceptions
    - To the Secretary of DHHS to investigate an alleged privacy violation

U & Ds for Other Purposes

- Permissive disclosures 164.512

<table>
<thead>
<tr>
<th>Public Health Activities</th>
<th>Report Abuse &amp; Neglect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Oversight Activities</td>
<td>Legal Proceedings</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>Information about Decedents</td>
</tr>
<tr>
<td>Organ &amp; Tissue Donation</td>
<td>Research</td>
</tr>
<tr>
<td>Avert Serious Threat</td>
<td>Specialized Gov. Functions</td>
</tr>
<tr>
<td>Workers’ Compensation</td>
<td></td>
</tr>
</tbody>
</table>
Public Health Activities

- Prevent or control disease, injury or disability
- Vital statistics, birth & deaths
- Public health surveillance
- Public health investigations
- Report child abuse or neglect
- FDA reporting
- Alert individual of possible exposure to communicable disease
- Employers under limited circumstances

Report Abuse or Neglect

- Report to authorities authorized by law to receive information about victims of abuse, neglect or domestic violence
  - Based on reasonable belief

- CE must inform the individual of the disclosure unless
  - There is a reasonable belief this would place the individual at risk for serious harm or
  - It would mean informing a personal representative who is believed to be responsible for the abuse or neglect
Health Oversight Activities

- Disclosures may be made to entities authorized by law to oversee:
  - The health care system
  - Government benefit programs for which health information is relevant to beneficiary eligibility
  - Entities subject to government regulatory programs
  - Entities subject to civil rights laws

Health Oversight Activities (cont.)

- This does not include investigations where the individual is the subject of the investigation if it is not directly related to:
  - The receipt of health care
  - A claim for public benefits related to health or
  - Qualification or receipt of public benefit or service if health is integral to the claim
Legal Proceedings

- Court orders
  - Limited to the PHI expressly authorized

- Subpoenas, discovery requests or other lawful process if satisfactory assurances is received that either:
  - Subject of information has been notified & given a chance to object
  - A qualified protective order has been requested
  - The CE notifies the individual or seeks a protective order

Law Enforcement

- If pursuant to process or otherwise required by law

- Identification and location

- Victims of a crime

- Decedents – if suspicion that death was result of criminal conduct

- Crime on the premises

- Report crime in an emergency
Information about Decedents

- Coroners & Medical examiners
  - Determine cause of death
  - Identification
  - Other duties authorized by law

- Funeral Directors
  - Information necessary to carry out their duties

Organ and Tissue Donation

- May disclose information necessary to facilitate organ, eye, or tissue donation
Research

- Waiver or alteration of authorization approved by privacy board or IRB
- Reviews preparatory to research
- Research on decedents information
- De-identified data
- Limited data set used

De-identified data?

- A) Names;
- (B) Street address, city, county, precinct, zip code, and equivalent geo-codes
- (C) All elements of dates (except year) for dates directly related to an individual and all ages over 89
- (D) Telephone numbers;
- (E) Fax numbers;
- (F) Electronic mail addresses;
- (G) Social security numbers;
- (H) Medical record numbers;
- (I) Health plan ID numbers;
- (J) Account numbers;
- (K) Certificate/license numbers;
- (L) Vehicle identifiers and serial numbers, including license plate numbers;
- (M) Device identifiers/serial numbers;
- (N) Web addresses (URLs);
- (O) Internet IP addresses;
- (P) Biometric identifiers, incl. finger and voice prints;
- (Q) Full face photographic images and any comparable images; and
- (R) Any other unique identifying number, characteristic, or code.
**Limited Data Set?**

- A) Names;
- B) Street address, **town or city, county, precinct, zip code, and equivalent geo-codes**
- C) **All elements of dates (except year) for dates directly related to an individual and all ages over 89**
  - D) Telephone numbers;
  - E) Fax numbers;
- F) Electronic mail addresses;
- G) Social security numbers;
- H) Medical record numbers;
- I) Health plan ID numbers;
- J) Account numbers;
- K) Certificate/license numbers
- L) Vehicle identifiers and serial numbers, including license plate numbers;
- M) Device identifiers/serial numbers;
- N) Web addresses (URLs);
- O) Internet IP addresses;
- P) Biometric identifiers, incl. finger and voice prints;
- Q) Full face photographic images and any comparable images; and
- R) **Any other unique identifying number, characteristic, or code.**

---

**Data Use Agreement**

- Sets out the permitted uses and disclosures of the PHI in the LDS
- Identifies who is permitted to use or disclose the information
- Provides that the recipient will
  - Properly safeguard the data
  - Not use the information in a manner inconsistent with the DUA
  - Report any improper uses or disclosures to the CE
  - Not use the information to attempt to identify or contact individuals based on the information in the LDS
  - Require all agents and subcontractors to comply with the terms of the DUA
Avert a Serious Threat

- May disclose PHI consistent with applicable law & standards of ethical conduct if
  - Good faith believes the disclosures is necessary to avert a serious & imminent threat to
    - The public
    - An individual

- May not make the disclosure if the information is learned under certain conditions

Specialized Governmental Functions

- Military & veteran activities
- National security
- Protection of the President & others
- Medical suitability determinations
- Correctional institutions
- CE that are governmental entities providing public benefits
Workers’ Compensation

- May disclose to the extent necessary to comply with workers’ compensation laws or other similar programs

U & Ds that require an opportunity to object. 164.510

- Facility Directories
- Family, Friends and others
  - Involved in the patient’s care
  - Involved in payment for the patient’s care
- Notification
U & Ds Requiring an Authorization

- All uses and disclosures of PHI that are not explicitly required or allowed under the regulations may only be done with an authorization.
  - Marketing
  - Fundraising

Valid Authorization

- Description of information to be used or disclosed that identifies the information in a specific and meaningful fashion

- Name or other specific ID of person(s) or class of persons to
  - Make the requested use or disclosure
  - Whom the CE may make the requested use or disclosure
### Valid Authorization (cont.)

- Description of each purpose of the requested use or disclosure

- Expiration date or event
  - For research only the expiration date can be “at the end of the study” or “none”

- Signature of the individual or personal representative

---

### Valid Authorization (cont.)

- Required statements
  - Inform the individual of the right to revoke, how to revoke and any exceptions to a revocation
  - Whether participation is conditional on signing the authorization
  - Potential for information to be re-disclosed by a person or entity receiving the information

- Must give the individual a copy
Patient’s Rights Under HIPAA

- Access and copy information 164.524
- Request restriction of use for TPO or under 164.510(b)
- Request confidential communication
- An account of disclosures
- Receive a copy of the notice of privacy practices
- Request amendments
Request Restrictions

- Only applies to PHI used or disclosed for TPO or to family, friends or others involved in the patient’s care
- A covered entity is not required to agree
- If the CE agrees, it is bound by the restriction
- Change under HITECH – must agree to request for restriction if it meets certain criteria.

Request Confidential Communications

- Providers
  - Must accommodate reasonable requests
- Health Plan
  - Must accommodate if the individual clearly states that the disclosure or all or part of the information could endanger the individual
Access and Copy Information

- Individuals have a right to access the PHI about them in a DRS except
  - Psychotherapy notes
  - Prepared in reasonable anticipation of litigation
  - Information to comply with CLIA if CLIA prohibits access

Access and Copy Information

- Denial of access is non-reviewable if
  - PHI is excepted from right to access
  - Individual is an inmate and access would jeopardize the facility
  - Research information – if explained in research authorization
  - Information is subject to the Privacy Act
  - Information obtained with promise of confidentiality from someone other than a health care provider
Access and Copy Information

- Reviewable grounds for denial
  - Licensed health care professional believes access would endanger the individual or another person
  - Information was received from another person and access could cause substantial harm to that individual
  - Request is made by a personal representative and access could cause substantial harm to the individual

Access and Copy Information

- Must have process for review
- Requests for access must be acted upon within 30 or 60 days
- Can get one 30-day extension
- Can charge for copies
Request an Amendment

- Individual may have information in the DRS amended

- CE may deny the request if
  - Determines the information is correct
  - CE did not create the information
  - Information is not part of the DRS
  - Individual would not have the right to access under 164.524

- CE must respond to request in 60 days

Accounting of Disclosures

- CE must account for all disclosures of PHI unless the disclosure was made
  - For TPO *
  - With an authorization
  - In a LDS
  - As an incidental disclosure
  - To the subject of the information
  - For national security purposes
  - Pursuant to 164.510
  - Prior to 4/14/03
  - To correctional institution

- *HITECH will require accounting for TPO disclosures from the EHR
Receipt of Notice of Privacy Practices

- Individual has a right to receive the notice of privacy practices at their first encounter after 4/14/03 or upon request.

- Notice must be posted in prominent place where patients are likely to see it.

Other HIPAA Issues

- Minimal Necessary

- Organizational Arrangements
  - Organized Health Care Arrangements
  - Affiliated Covered Entities
  - Hybrid Covered Entities

- Business Associates

- Group Health Plans

- Miscellaneous issues
  - Psychotherapy notes
  - Verification processes

- Preemption of state law
### Minimal Necessity

- **Role based access**
  - Assure that individuals only have access to the information needed to do their job

- **Disclosures**
  - Disclose on the minimal necessary for the purpose of the disclosure
  - Does not apply to disclosures made
    - With an authorization
    - To a provider for treatment
    - To the subject of the information
    - To the Secretary of DHHS
    - As required by law
    - As required to comply with the regulations

### Organizational Arrangements

- **Organized Health Care Arrangements (OHCA)**
  - Clinically integrated
  - More than one CE participates

- **Affiliated Covered Entities (ACE)**
  - Legally separate CEs that are affiliated by common ownership or control

- **Hybrid Covered Entity (HCE)**
  - Single covered entity with non-health care components
Business Associates

- Business associates are entities that perform services for or on behalf of a CE involving PHI.
- Must have a business associate agreement
- A CE can be the business associate of another CE

Group Health Plans

- Group health plans are covered entities under HIPAA
- The employer is not the covered entity
- A GHP’s notice of privacy practices requires a statement regarding the use and disclosure for plan administrative functions
**Miscellaneous Issues**

- Psychotherapy notes
  - Part of the DRS
  - Require an authorization for uses and disclosures even for TPO

- Verification process
  - Must verify that individuals to whom you are disclosing information are really who they say they are

**Administrative Requirements**

- Designate a privacy official

- Train members of the workforce on privacy requirements

- Safeguard PHI

- Develop sanctions for violations of the privacy policies and procedures

- Establish a means for individuals to complain about privacy violations
Enforcement Changes

- Changes to the CMP provisions of the HIPAA statute
- Enforcement allowed by State Attorneys General

Changes to CMPs

- ARRA changes the CMP provisions of HIPAA
- It also changes the provision that previously precluded the imposition of CMPs for violations that could also be considered violations of the criminal provisions of HIPAA to now only preclude the imposition of CMPs if a penalty has been imposed under the criminal provisions
Changes to CMPs

- Under the original HIPAA statute the CMPs for violating a provision of the statute was $100 per individual violation limited to a $25,000 annual cap for each identical requirement or prohibition.

Changes to the CMPs

- The new penalty ranges are
  - $100 up to cap of $1,500,000 for violations of each identical requirement or prohibition
  - $1,000 up to cap of $1,500,000 for violations of each identical requirement or prohibition
  - $10,000 up to a cap of $1,500,000 for violations of each identical requirement or prohibition
  - $50,000 up to a cap of $1,500,000 for violations of each identical requirement or prohibition
What determines which penalty will be imposed?

- If the violation is one that the covered entity did not know about and with the exercise of reasonable diligence would not have known about the Secretary has the discretion to impose the $100 penalty up to the $50,000 penalty.

DEFINITIONS

- Reasonable diligence would be defined as “the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.”

- Willful neglect is “conscious, intentional failure or reckless indifference to the obligation to comply with the administrative simplification provision violated.”
What determines which penalty will be imposed?

- If the violation is determined to be a reasonable cause and not willful neglect then the penalty range starts at $1,000 and can go up to $50,000 per violation.

- If the violation is due to willful neglect and the covered entity corrects it within 30 days of discovery the penalty range starts at $10,000 and can go up to $50,000 per violation.

“Reasonable cause” would be defined as “circumstances that make it unreasonable for the covered entity, despite the exercise of ordinary business care and prudence, to comply with the administrative simplification provision violated.”
What determines which penalty will be imposed?

- If the violation is due to willful neglect and the covered entity does not correct it within 30 days of discovery the penalty range starts at $50,000 per violation.

- A violation is deemed to be discovered when the covered entity knew or by exercise of reasonable diligence should have known that the failure to comply occurred.

Application of CMPs

- The new CMPs are in addition to and not in lieu of any fines and penalties that the state might impose.

- Our organizations could be hit from both a state agency and OCR.

- This could occur at different times.
Where will the CMPs go?

- The statute allows for the CMPs collected and any monetary settlement to go to OCR for enforcement activities in both privacy and security.
- There is also a provision requiring the Secretary to promulgate regulations within three years that identifies a method to distribute any CMPs or monetary settlement received to an individual(s) harmed by a misuse of information.

State Attorneys General can now bring a HIPAA action

- The ARRA provides for State Attorneys General to bring civil actions under HIPAA.
- They are currently limited to pursuing $100 per violation of an individual requirement or prohibition up to $25,000 cap.
- It also allows for the Attorney General to seek attorney fees.
- This provision is effective immediately.
Breach notification requirement for Covered Entities

- A breach requires notification if
  - (1) Unauthorized acquisition, access, use, or disclosure of
  - (2) unsecured PHI which
  - (3) compromises the privacy or security of the PHI.

What is not a breach?

- (i) Any **unintentional** acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
What is not a breach?

- (ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule.

What is not a breach?

- (iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
Definition of Unsecure PHI

- Unsecured PHI is defined as
  - PHI not secured through technology or a method specified by the Secretary through guidance

- Federal Register /Vol. 74, No. 79 /Monday, April 27, 2009:
  "...two methods for rendering PHI unusable, unreadable, or indecipherable to unauthorized individuals: encryption and destruction."

Analysis of what is a breach

- Does it compromise the privacy and security of the PHI?
  - Poses a significant financial, reputational or other harm to the individual
  - Requires a risk assessment
Risk assessment

- Things to consider,
  - Who impermissibly used or disclosed the information?
  - To whom was the information disclosed?
    - Was it another covered entity?
  - What mitigating steps were taken and when?
    - Reasonable assurances from the recipient that the information would not be further used or disclosed
    - The information is destroyed by the recipient.

Risk assessment

- Was the PHI retrieved or returned before it could be impermissibly accessed?
  
  Cannot delay notification hoping that a lost computer will be recovered.

- Is the nature of the PHI such that it does not pose a significant financial, reputational or other risk of harm to the individual?
“The risk assessment should be fact specific, and the covered entity or business associate should keep in mind that many forms of health information, not just information about sexually transmitted diseases or mental health, should be considered sensitive for purposes of the risk of reputational harm – especially in light of fears about employment discrimination.”

Breach notification requirement for Covered Entities

A covered entity or BA is on notice of a breach on the first day anyone, other than the employee committing the breach, in the organization knows of the breach or with the exercise of reasonable diligence should have known of the breach.
Breach Notification

- The covered entity or BA must notify the individual, their next-of-kin or personal representative without unreasonable delay but no later than 60 days after breach is discovered.

- An investigation of the facts and circumstances surrounding the breach may take some time to investigate.

- The time to investigate can be a reason for delaying notification.

Breach notification requirement for Covered Entities

- Written notification through first class mail at the last known address of the individual, the personal representative or the next-of-kin.

- If you do not have a good address, then you must try other means of notification.
  - Substitute notice is not required when you do not have not have a good contact information for the personal representative or next-of-kin.
Breach notification requirement for Covered Entities

- If you have more than 10 persons for whom you do not have good contact information, then the details of the breach must be posted on the home page of the covered entity’s website or in major print or broadcast media.

- The post must be for 90 days

- Must include a toll free number for individuals to contact and see if their information was impacted

Breach notification requirement for Covered Entities

- If the nature of the breach puts the individual in imminent danger of misuse of unsecured PHI, the covered entity may also notify via telephone.

- If the breach involves the unsecured PHI of more than 500 people in a particular state or jurisdiction, the covered entity must also notify the prominent media outlets serving the state or jurisdiction where the individuals reside
  - Jurisdiction is defined as a geographic area small than a state such as a county, city or town.
Breach notification requirement for Covered Entities

- The covered entity must notify the DHHS Secretary.

- If the breach is more than 500 people, immediate notice is required.
  - Immediate means without undue delay and at the same time as notice to the individual involved

Breach notification requirement for Covered Entities

- If the breach is less than 500 people, the covered entity can keep a log of all such breaches and turn it in to the Secretary annually.
  - The information must be submitted annually to the Secretary within 60 days of the end of the calendar year
Content of the notification

- Brief description of
  - What happened
  - Unsecure PHI involved in breach
  - Steps the individual should take to protect themselves
  - The covered entity’s investigation, mitigation of harm to the individual and corrective action plan

- Contact method such as toll-free number, email address, website or postal address for individuals to ask questions

Additional requirements for the notice

- The notice has to be written at the appropriate reading level.

- The interim final rule discusses avoiding any extraneous information
  - My interpretation, no fluff.

- It may have to be translated.
**Deadlines**

- Breach notification provisions will apply to breaches that occur 30 days after publication of the interim final regulations or September 23, 2009.

- The Secretary will wait 180 days for enforcement or February 20, 2010.

---

**Questions & Answers**
Contact Information

Marti Arvin, JD, CHC-F, CCEP-F, CHRC, CHPC, CPC
Chief Compliance Officer
UCLA Health System and the David Geffen School of Medicine
Phone (310) 794-6763
e-mail Marvin@mednet.ucla.edu