Who Is In The Record?
An Advanced Discussion on Building Privacy Into the Culture

Carole A. Klove, RN, JD
Chief Compliance and Privacy Officer – UCLA Medical Sciences

Agenda

- Privacy and Security Regulatory Environment
- Highlights of the New State Privacy Laws
- Federal Regulations on the Horizon
- How to Build Confidentiality Protection into a Compliance Program to Identify, Detect and Mitigate Identity Theft
Information you should know

- Privacy and Security is more than HIPAA these days
  - New states laws are more stringent and impose increased fines/penalties
- The Privacy and Security environment is constantly changing
  - Internally - need for access to clinical data electronically
  - Externally - patient expectation to communicate electronically to providers

Privacy and Security regulations and perspectives are increasing expectations

- Internal
  - Higher degree of organizational focus on privacy and information security practices
  - Op-out review process is required for all fundraising mailing lists
  - Best practice is to review access rights of all employees at least annually.
- External
  - Heightened media and governmental focus on breaches and delays in notification
  - New state laws
  - New Federal Requirements
### New California State Laws – Highlights – 
Perhaps the Foundation for ARRA

**Key Requirements**

<table>
<thead>
<tr>
<th>AB-211</th>
<th>SB-541</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC56.36/ H&amp;S130200</td>
<td>H&amp;S 1280.15</td>
</tr>
</tbody>
</table>
| Mandates the confidentiality of medical information. Requires implementation of appropriate administrative, technical and physical safeguards to protect the privacy of a patient’s medical information, and implementation of reasonable safeguards to prevent unauthorized access, use, or disclosure. | Mandates prevention of unlawful or unauthorized access to, use of, or disclosure of patient medical information.  
**Reporting obligations:**  
An incident of unlawful access, use, or disclosure of a patient’s medical information must be reported within 5-days of detection of the breach to CDPH and the affected patient(s)/legal representative. |

### New California State Laws - Highlights

**Authorizes**

<table>
<thead>
<tr>
<th>AB-211</th>
<th>SB-541</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC56.36/ H&amp;S130200</td>
<td>H&amp;S 1280.15</td>
</tr>
<tr>
<td>Fines and civil penalties against any individual that negligently discloses or knowingly and willfully obtains, discloses, or uses medical information in violation of state / federal laws.</td>
<td>Fines to the institution for failure to prevent or report for unauthorized access, use, or disclosure of medical information.</td>
</tr>
</tbody>
</table>
## New California State Laws - Highlights

### Fines & Penalties

<table>
<thead>
<tr>
<th>AB-211</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC56.36/ H&amp;S130200</td>
</tr>
<tr>
<td><strong>Individual Fines/ Penalties:</strong></td>
</tr>
<tr>
<td>- $2,500 - $25,000 per violation</td>
</tr>
<tr>
<td>- $250,000 – maximum penalty/ violation</td>
</tr>
<tr>
<td>- Misdemeanor if patient suffers economic loss or personal injury</td>
</tr>
<tr>
<td>- Potential for civil action by patient with statutory damages ($1000) in addition to actual damages</td>
</tr>
<tr>
<td>- Cal-OHII may notify licensing board for further investigation/ discipline of individual providers</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SB-541</th>
</tr>
</thead>
<tbody>
<tr>
<td>H&amp;S 1280.15</td>
</tr>
<tr>
<td><strong>Institutional Fines for failure to prevent or report:</strong></td>
</tr>
<tr>
<td>- $25,000 – initial violation (per patient)</td>
</tr>
<tr>
<td>- $17,500 – subsequent occurrence</td>
</tr>
<tr>
<td>- $250,000 – maximum penalty</td>
</tr>
<tr>
<td>- $100/ day for late reporting</td>
</tr>
</tbody>
</table>

### Spotting Identify Theft

- Image of four penguins on a beach.
Why did the government adopt the Red Flag Rules?

- More than 10 million Americans are victims of identity theft each year.
- The total financial losses due to identity theft are estimated to be about $50 billion every year. FTC received 258,427 complaints of ID theft in 2007, 32% of total complaints.
- Victims spent an average of $550 in 2007 for damage to existing accounts.
- When ID thieves opened new accounts victims spent an average of $1,865.

On the Horizon: Federal Regulation “Red Flag Rule”

- Identity Theft “Red Flag Rules”
  - Full compliance required by May 1<sup>st</sup>, 2009
  - Part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. Under the Rule, financial institutions and creditors with covered accounts must have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.
  - Applicable when an institution extends credit for services provided.
- Identity/Medical Identity Theft facts you should know
  - Medical Information has a higher street value than financial information
  - 90% of Medical Identity Theft is an insider job*
    *Pamela Dixon- World Privacy Forum
What is a Red Flag and What Must be Included in the Red Flag Program?

- **What is a Red Flag**
  - a pattern, practice, or specific activity that indicates the possible existence of identity theft.
  - Regulation provides many examples of “Red Flags”

- **Elements of the program**
  - Must include policies and procedures to:
    - Identify relevant red flags and incorporate them into the program.
    - Detect red flags that are part of the program.
    - Respond appropriately to any red flags that are detected.
    - Ensure the program is updated periodically to address changing risks

---

Additional New Federal Laws

- **HITECH Act** - Health Information Technology for Economic and Clinical Health Act
  - The HITECH Act is Title XIII of ARRA
What Does the ARRA Address?

- Immediate Funding for HIT Infrastructure and Implementation Assistance
- State Grants and Loan Programs
- HIT Education
- Medicare Incentives for “Meaningful Use” of Electronic Health Records (EHRs) by Eligible Professionals
- Medicare Incentives for “Meaningful Use” of EHRs by Hospitals
- Medicaid Incentives
- New Enforcement/Penalties
- Audits and Reports
- Privacy/Security Requirements

What Does the ARRA Address?

- Highlights Include:
  - BAs are civilly and criminally liable for violations of:
    - The HITECH Act privacy/security requirements
    - Security Rule administrative, physical and technical standards, requirements for documentation and for policies and procedures
    - BA requirements of Privacy Rule
  - Mandatory Restriction
    - No disclosure to health plan for services paid in full out of pocket by patient
Importance of Knowing Who is in the Record under ARRA

- Highlights Include:
  - Additional Civil Fines and Penalties effective 2/18/09
  - Notification Requirements effective 9/17/09
    - The notification must be made within 60 days unless law enforcement requests a delay
    - The notification must be to public media if >500 patients’ PHI involved
    - Applies to breaches of “unsecured PHI”
  - Accounting of Disclosure reduced to 3 years but there is no exception for TPO as existed under HIPAA

On the Horizon: National Health Record

- National and State work to establish centralized Health Information Exchanges
- President Obama’s goal for computerized medical records
- Significant Privacy Concerns with this movement
Building Confidentiality Protection Into Your Existing Compliance Program – Five Steps

- HIPAA and other existing California laws require, in whole or in part, all providers to maintain a compliance program to manage Protected Health Information (PHI) and Personally Identifiable Information (PII) which require:
  - Understanding your electronic record systems as well as paper documentation
  - Knowing who has access to your system and the extent of the access
  - Maintaining auditable records of the electronic record systems
  - Taking reasonable precautions to protect all PHI
  - Coordinating the Reporting Process, if needed

Building Confidentiality Protection Into Your Existing Compliance Program – Step One

Understanding the Electronic and Paper Record Systems

- Identify all systems and applications where PHI or PII exists within your organization and their relationships with other systems
- Determine where PHI/PII is exposed in applications or in the physical environment and to whom.
- Ensure that any vendor-supported product has appropriate controls relating to access, both physical and contractual
  - Current Business Associate Agreement, covering both Privacy and Security Rules
  - Evaluate if Modification need to be implemented to support SB 541 and AB 211, Red Flag and ARRA
Building Confidentiality Protection Into Your Existing Compliance Program – Step Two

Knowing who has access to clinical systems and other databases and the extent of the access:

- Evaluate process for authorizing access to clinical systems
- Require approval for database downloads and mainframe interfaces.
- Ensure appropriate controls for research use.
- Work with the Information Security Officer, CIO and other IT staff to understand the relationships between systems and data flows.

Cont’d…

Knowing who has access to clinical systems and other databases and the extent of the access:

- Understand the process for terminating access or updating access when job function or duties change
- Ensure process is in place for timely and accurate modifications to access privileges
- Evaluate role-based access and develop policies to define appropriate access
- Consider building the review of access into the Job Description and Performance Evaluation of each employee
- Protect sensitive data (e.g. SSN, psychiatric, HIV)

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Two

Knowing who has access to clinical systems and other databases and the extent of the access:

- Ensure appropriate controls are in place for vendors, observers or trainees;
  - Business Associate Agreements – Centralized BAA database
  - Confidentiality Statements
  - Check-in and ID badge process

- Ensure secure transmission of data to external business associates and collaborators, such as via a secure email system

Building Confidentiality Protection Into Your Existing Compliance Program – Step Three

Maintaining Auditable Records of the Electronic Health Systems:

- Required auditable records (HIPAA, ARRA, SB 541)

- Assist to detect inappropriate access
  - Understand the audit capability of your systems
  - Be familiar with the audit information available
  - Balance auditing requirements with quality of care needs

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Three

Maintaining Auditable Records of the Electronic Health Systems:

- Define the audit process and the role of the managers and key individuals, including Human Resources, in the enterprise who will assist with the process
  - Who will be audited
  - Which clinical systems and frequency of audits
- Develop a disciplinary process
- Establish additional safeguards, e.g., “break the glass” process requiring a reason for access

Cont’d…

Building Confidentiality Protection Into Your Existing Compliance Program – Step Three

Maintaining Auditable Records of the Electronic Health Systems:

- What to Consider in the Audit Process:
  - Proactive Audits – who are your high-value targets?
  - Random Audits
    - By user or by patient
  - Complaint Driven
  - Focused audits by stated criteria
    - Same last name
    - Co-worker
    - Unit based

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Three

Maintaining Auditable Records of the Electronic Health Systems:

- For example, evolution of Notification under California Law:
  - SB 1386 (7/1/03)
    - Required Notification to the Patient when SSN, DLN or pin
  - AB 1298 (1/1/08)
    - Must notify a patient for any unauthorized acquisition of unencrypted name and medical information or health insurance information
  - SB 541 (1/1/09)
    - Providers must report incidents of unlawful access, use, or disclosure of a patient’s medical information within 5 days of detection of the breach to the CA Department of Public Health (DPH), and the affected patient or legal representative

Building Confidentiality Protection Into Your Existing Compliance Program – Step Four

Taking Reasonable Precautions to Prevent Unauthorized Access to PHI:

- Understand and protect the entire lifecycle of information:
  - Intake/creation of PHI
  - Storage of PHI
  - Use of PHI
  - Transmission of PHI
  - Destruction of PHI
  - For any format of PHI

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Four

Taking Reasonable Precautions to Prevent Unauthorized Access to PHI:

- Verbal Awareness
- Encryption of mobile devices
- Written Paper/ Hard Copy Protections
- Safe Computing Skills
- Reporting Suspected Security Incidents

Publicize the audit process
- Annual confidentiality statements
- Mandatory Training
- Confidentiality Banners to Log On Screens
- E-mail reminders and posters

Publicize the disciplinary process to all workforce

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Four

Taking Reasonable Precautions to Prevent Unauthorized Access to PHI:

- Implement “privacy” rounds as part of environmental rounds
- Ensure confidential bins are readily available in all areas
- Educate workforce on the safe disposal of PHI and PII
- Medical devices can also store PHI/PII

Cont’d…

Privacy Rounds further education efforts by accomplishing the following:

- Every manager owns a piece of the Privacy Compliance Program becoming the “threads” in the “fabric” of the Compliance Program
- Allows for consistency in practice and of expectations across the medical enterprise to “walk the talk”

Cont’d…
Building Confidentiality Protection Into Your Existing Compliance Program – Step Four

Taking Reasonable Precautions to Prevent Unauthorized Access to PHI:

- Implementing a Privacy Code can facilitate communications with patients’ families and friends
  - Patients are either given or select a “Privacy Code”
  - Allows the patient to identify those who can obtain information in the inpatient setting

Building Confidentiality Protection Into Your Existing Compliance Program – Step Five

Coordinate the Reporting Process

- Define who will report and involve
  - Administration
  - Compliance Office
  - Privacy Office
  - Counsel
  - Media Relations
  - Law Enforcement

- Define when will send out the notification to the patient and DPH

- Document and track the reporting process and disciplinary process
Questions, Answers and Discussion