crowell moring

HOOPS West
2012

The Dish on Data and Disks
HIPAA Privacy and Security Breach Developments

Robin B. Campbell

Ethan P. Schulman

Jennifer S. Romano

HIPAA Privacy and Security Breach Developments

- Overview of the Laws
- Incident Response-First Steps
- Regulatory/Enforcement Implications
- Emerging Litigation Issues
- Breach Prevention Tips
- Government Audits

Laws That Protect PHI

- HIPAA/HITECH and regulations
- Gramm-Leach-Bliley Act (for insurers)
- State
  - State Breach Notification Laws
  - State SSN Laws
  - State Medical Privacy Laws

HIPAA/HITECH Definition of Breach

- Statutory definition of breach
  - The unauthorized acquisition, access, use or disclosure of protected health information, which compromises the security or privacy of such information . . .
  - HHS has determined that "compromises the security or privacy of the protected health information" means that the breach poses a "significant risk of financial, reputation, or other harm to the individual"

***Question remains whether the risk of harm standard will be included in the final rule that has not yet been released.**

HIPAA Notification Requirements

- Notification is necessary if the breach poses a "significant" risk of harm
- Requires written notification to affected individuals without unreasonable delay but *no later than 60 days from discovery*
- Content Requirements
- Notification to HHS/Media

State Laws

- Breach notification laws
- SSN laws
- CA Customer Records Act (CRA)
- CA Confidentiality of Medical Information Act (CMIA)

Breach Notification/SSN Laws

Breach Notification Laws

Similar to HITECH but differ on:

- Definition of personal information
- Risk of harm threshold
- Paper versus electronic data
- Timing/Content of notification
- Authorities to notify
- Media notification

Restrictions on the Use/Disclosure of SSNs

- Prohibit public display and transmission over Internet unsecured
- No notification requirement

California Customer Records Act (CRA) (The CA Breach Law)

- Applies to any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information
- Mandates disclosure of "any breach of the security of the system" to "any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person"

Key CRA Terms

- Breach - unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business
- Personal information – name in combination with any one or more (if either is unencrypted):
  - SSN, CDL or California ID Card number
  - Medical information
  - Health insurance information, including health insurance policy number or subscriber ID number, unique identifier, or "any information in an individual's application and claims history"

Notification Under CRA

- Requires written notice, but allows for substitute notice if cost/volume thresholds are met
- Timing
  - "In the most expedient time possible and without unreasonable delay" Privacy Office recommends 10 days
  - May delay notification if law enforcement agency determines it will impede a criminal investigation
- Form and contents (SB 24)
  - Plain language
  - Types of personal information affected
  - If known, estimated date of breach and general description of breach incident
  - Copy of notification to Attorney General (if more than 500 California residents affected)

Strict Liability or Room for Discretion?

CA law has no specific harm threshold

However, breach definition provides for:

- "unauthorized acquisition"
- "compromises the security, confidentiality, or integrity of personal information"

Can there be a breach where notification is not required?

Incident Response-First Steps

- Follow your incident response process (including documentation, establishing a team, escalation)
- Contain the incident/determine and fix cause
- Notify insurance carrier (if there is breach coverage)
- Gather the facts (bring in forensics if needed)
- Assess the impact/determine risk of harm
- Determine communication/notification requirements and timing obligations
- Identify customer support team and other roles and responsibilities
- Arrange vendors for notification letters, credit services, call centers
- Prepare for enforcement actions/private lawsuits/class actions
- Develop and implement a corrective action plan

Regulatory/Enforcement Actions/Complaints

Players

- State: AGs/DOIs/Other regulators (e.g. DMHC)
- Federal: HHS/OCR/CMS
- Employer groups/Individual members

Enforcement Trends

- HHS/OCR Recent Enforcement Actions:
  - BCBS TN: $1.5 million and CAP, hard drives stolen
  - UCLA: $865,500 and CAP, employees' unauthorized viewing of patient medical records.
  - Mass General: $1 million and CAP, employee took PHI off premises and lost it in public.
  - Cignet: $4.3 million, CE refused patients access and ignored OCR, refused to cooperate, defaulted on subpoena, failed to respond to the initial notice of determination, and "made no attempts to resolve the complaints through informal means."
  - Management Services Org: $35,000 and CAP, "HHS investigation showed that MSO intentionally did not have in place or implement appropriate and reasonable administrative, technical, and physical safeguards to protect the privacy of the protected health information."

Emerging Litigation Issues

- Principal theories of liability
  - Confidentiality of Medical Information Act
  - Common law claims
- Standing to sue
- Class certification issues
- Damages
  - Statutory damages
  - Compensatory damages
  - Due process issues

California Confidentiality of Medical Information Act (CMIA)

- Covers health care providers, health care service plans, and contractors
- General prohibition against "disclosure" of "medical information" regarding a patient without authorization
  - Mandatory and permissive exceptions
- Also requires covered entities that create, maintain, preserve, store, abandon, destroy, or dispose of medical records to do so in a manner that preserves the confidentiality of the information they contain

CMIA Definitions

- Medical information
  - Any individually identifiable information . . . regarding a patient's medical history, mental or physical condition, or treatment
- "Disclosure" or "release"
- "Confidential information or records"

CMIA Remedies

- Violation that results in economic loss or personal injury to a patient
  - Criminal penalties
  - Compensatory and punitive damages
- Negligent release of confidential information or records
  - Nominal damages of $1,000 per person
  - No actual or threatened damages required
  - Administrative fines or civil penalties

Unresolved Litigation Issues

- Meaning of "disclosure" or "release" under CMIA
  - Loss of media containing PHI included?
  - Unnecessary disclosure to business associates or other third-party vendors covered by exception?
- Threshold issues
  - Standing to sue (federal court)
  - Actual injury or harm (common law claims)

Emerging Litigation Issues

- Class certification issues
  - Scope of class definition
  - Removal of multistate class actions under CAFA
  - Coordination or transfer of multiple actions
  - Impact of arbitration clauses
- Damages
  - Aggregate exposure to nominal damages
  - Due process violation?
- Settlement approaches

Breach Prevention Tips

- Collect only what is necessary for your business purposes (or what is required by law)
- Know your data flows
- Develop and implement strong policies and procedures
- Develop a comprehensive Incident Response Plan
- Maintain reasonable and adequate security safeguards for protected data (required by many state and federal laws, various degrees of detail from proper document destruction to technical encryption requirements)
- Utilize *industry standard* tools available to protect data through all stages (encryption, security operations center, data loss prevention products, intrusion detection)

Prevention Tips (cont.)

- Limit access to personal/confidential data
- Require adequate security of third parties through contract and know your own contractual obligations as a vendor
- Monitor compliance of vendors with stated security/privacy measures
- Train, Train, Train—not just on policies and procedures, but how to recognize a breach and what to do when you suspect one
- Consistently enforce your policies and procedures, the law, and your training
- Encourage a culture of compliance

Government Audits

- A security breach opens door to full scale audit of HIPAA compliance
- In addition, HHS has begun random audits of Covered Entities, with Business Associates to follow shortly

HHS Audit Overview

Covered Entities/Be Prepared

- HIPAA compliant documents (P&Ps, forms, notices)—know what you have and where to find it
- Review P&P for legal compliance
- Identify P&Ps not currently or properly followed
- Ensure that ***all*** safeguards are properly documented and implemented
- Identify key personnel with whom auditors should speak
- Ensure that all personnel is trained and knows the relevant P&Ps
- Be cooperative—highest fines have been associated with unresponsive and uncooperative behavior

HHS Audit Plan

Summary

- All Roads Lead to Prevention
  - Breach and public notification
  - Enforcement actions
  - Individual complaints and/or lawsuits
  - Scheduled HHS Audits
- Get Your House in Order and Keep it in Order
  - Don't rely on contract language alone
  - Be prepared to demonstrate a true and continuous effort to protect data and maintain a culture of compliance within your organization