Lessons Learned from Recent HIPAA Enforcement Actions, Breaches, and Pilot Audits

Dallas Bar Association
April 15, 2015

Jamie Sorley, JD, MBA, CIPP/US
Investigator, Region VI
• Enforces Civil Rights laws including the Civil Rights Act of 1964, Title II of the ADA, Sec. 504 of the Rehabilitation Act of 1973, Age Discrimination Act of 1975, Sec. 1557 of the Patient Protection and Affordable Care Act

• Enforces HIPAA Privacy, Security and Breach Notification Rules, and PSQIA

• Headquartered in DC, 10 Regional Offices
  – Region VI conducts complaint investigations and compliance reviews for TX, NM, OK, LA, AR
• **HITECH Privacy & Security**
  - Business associates (BA)
  - Marketing & Fundraising
  - Sale of protected health information (PHI)
  - Right to request restrictions
  - Electronic access

• **HITECH Breach Notification**

• **HITECH Enforcement**

• **GINA Privacy**

• **Other Modifications**
  - Research
  - Notice of privacy practices (NPP)
  - Decedents
  - Student immunizations

**General compliance date:** September 23, 2013
What’s Done:

- HITECH & Omnibus Final Rule
  - De-identification
  - Combined Regulation Text
  - Sample BA provisions
  - Refill Reminder guidance
  - Factsheets on Student Immunizations and Decedents
- Model Notices
- Guide to Law Enforcement
- Letters to Consumers and Providers
- Permitted Mental Health Disclosures
- HIPAA and Same Sex Marriage
NICS Notice of Proposed Rulemaking (NPRM)

- January 2013 – one of 23 executive actions to reduce gun violence
- April 2013 – Advance Notice of Proposed Rulemaking (ANPRM) on need for HIPAA rule change for NICS reporting
- January 2014 – NPRM published
  - Express disclosure permission in Privacy Rule for designated NICS reporters or entities making mental health commitment or adjudication decisions
  - Limited to identity, demographics; not clinical data or medical records
- March 10, 2014 – comment period closed
CLIA Final Rule

• Joint Rulemaking

• Centers for Medicare and Medicaid Services (CMS) – Amends CLIA regulations to allow labs to give patients access to completed test results

• OCR – Amends HIPAA right to access to remove exemption for CLIA labs
  – Individual has right to get copy of test reports directly from labs
  – Access obligations on labs same as for other CEs
  – Individual can still go through physician to obtain test results

• Dates
  – Published February 6, 2014
  – Effective April 7, 2014
  – Compliance Required By October 6, 2014
What’s to Come:

- NICS Final Rule
- From HITECH
  - Accounting of Disclosures
  - Methods for sharing penalty/settlement amounts with harmed individuals
- NPRM on Windsor Decision and Personal Representatives?
REMINDER of Changes to the Rules:

• Security Rule: BAs (and subcontractors) now directly liable

• Privacy Rule: BAs (and subcontractors) now directly liable for:
  – impermissible uses and disclosures;
  – non-compliance with their BA Agreements; and
  – certain individual rights.
• A person who on behalf of a CE or OHCA, but other than in the capacity of a member of the workforce:
  – creates, receives, maintains, or transmits PHI for a function regulated under HIPAA
  – Provides legal, actuarial, accounting, consulting, data aggregation, management, accreditation, or financial services for the CE or OHCA where the provision of the service involves the disclosure of PHI

• includes health information organizations, e-prescribing gateways, certain personal health record vendors, subcontractors
Revised Definition of “Breach:”

Breach Presumed UNLESS:

• “LoProCo:” The CE or BA can demonstrate that there is a low probability that the PHI has been compromised based on:
  – Nature and extent of the PHI involved (including the types of identifiers and the likelihood of re-identification);
  – The unauthorized person who used the PHI or to whom the disclosure was made;
  – Whether the PHI was actually acquired or viewed; and
  – The extent to which the risk to the PHI has been mitigated.

Focus on risk to the data, instead of risk of harm to the individual.

Risk Assessment must be documented.
HITECH Audit Program

• Identify best practices and uncover risks and vulnerabilities not identified through other enforcement tools; encourage consistent attention to compliance

• Phase I completed
  – 115 pilot audits
  – Evaluation

• Phase II under development
No findings or observations for 13 entities (11%)

- 2 Providers, 9 Health Plans, 2 Clearinghouses

Security accounted for 60% of the findings and observations—although only 28% of potential total.

Providers had a greater proportion of findings & observations (65%) than reflected by their proportion of the total set (53%).

Smaller entities struggle with all three areas
Breach Highlights

September 2009 through March 17, 2015

• Approximately 1,144 reports involving a breach of PHI affecting 500 or more individuals
  – Theft and Loss are 60% of large breaches
  – Laptops and other portable storage devices account for 32% of large breaches
  – Paper records are 22% of large breaches

• Approximately 157,000+ reports of breaches of PHI affecting less than 500 individuals
500+ Breaches by Type of Breach as of 3/17/2015

- Theft: 51%
- Unauthorized Access/Disclosure: 19%
- Loss: 9%
- Improper Disposal: 4%
- Hacking/IT: 7%
- Other: 9%
- Unknown: 1%
500+ Breaches by Location as of 3/17/2015

- Paper Records: 22%
- Desktop Computer: 12%
- Laptop: 21%
- Portable Electronic Device: 11%
- Network Server: 12%
- Email: 7%
- EMR: 4%
- Other: 11%

500+ Breaches by Location as of 3/17/2015.
• Investigated Complaints/Compliance Reviews
  – Over 40,000 cases investigated
  – Over 30,000 closed with corrective action

• In most cases, entities able to demonstrate satisfactory compliance through voluntary cooperation and corrective action

• In some cases though, nature or scope of indicated noncompliance warrants additional enforcement action

• Resolution Agreements/Corrective Action Plans
  – 23 settlement agreements that include detailed corrective action plans and monetary settlement amounts
  – 1 civil money penalty

As of 12/31/2014
• Anchorage Community Mental Health Services (December 2014)
  - Breach affecting 2,743 individuals due to malware compromising the security of its information technology resources.
  - $150,000 settlement and corrective action plan to correct deficiencies, including reporting to OCR for a two-year period.

• Parkview Health System Settlement (June 2014)
  - Over 5,000 medical records were left unattended in a public area
  - Corrective action plan requiring review of policies and procedures for safeguarding PHI and $800,000 settlement amount

• NYP and CU Settlements (May 2014)
  - ePHI of 6,800 patients accessible on internet search engines
  - Entities failed to make efforts prior to breach to assure information was secure
  - Corrective action plans and $4,800,000 settlement amount
• Adult & Pediatric Dermatology, P.C. (December 2013)
  – Unencrypted thumb drive stolen from employee vehicle affecting 2,200 patients
  – Covered entity did not have breach policies and procedures
  – Corrective action plan to address security management and $150,000 settlement

• Affinity Health Plan, Inc. (August 2013)
  – Breach affecting up to 344,000 individuals
  – Covered entity had not properly erased photocopier hard drives prior to sending the photocopiers to a leasing company
  – Corrective action plan included retrieval and safeguarding of ePHI and $1,200,000 settlement
• **Massachusetts Eye and Ear Institute (September 2012)**
  – Stolen personal laptop of physician using device as desktop substitute
  – Covered entity had not implemented a program to mitigate identified risks to e-PHI
  – Corrective action plan requiring review of policies and procedures and workforce training and $1,500,000 settlement

• **Hospice of Northern Idaho (December 2012)**
  – Breach affecting 400 individuals when laptop stolen
  – CE had not conducted a risk assessment or taken other measures to safeguard e-PHI as required by Security Rule
  – Corrective action plan and $50,000 settlement
Lessons Learned:

• HIPAA covered entities and their business associates are required to undertake a careful risk analysis to understand the threats and vulnerabilities to individuals’ data, and have appropriate safeguards in place to protect this information.

• Take caution when implementing changes to information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.
Lessons Learned (cont.)

• Senior leadership helps define the culture of an organization and is responsible for knowing and complying with the HIPAA privacy and security requirements to ensure patients’ rights are fully protected as well as the confidentiality of their health data.

• Train heavily and stringently implement security policies regarding portable media.
Public Awareness/Compliance Tools

- Emphasis on Access
  - Information Is Powerful Medicine Campaign
- Privacy and Security on YouTube
  http://www.youtube.com/user/USGovHHSOCR
- Collaborations with the HHS Office of the National Coordinator for Health IT on Security
  - Mobile Devices
  - Security Rule Games
  - Security Risk Assessment Tool
- Fact Sheets/Translations into 7 languages
HIPAA Privacy Rule and Sharing Information Related to Mental Health

• Provides guidance on when it is appropriate under the Privacy Rule to share the PHI of a patient who is being treated for a mental health condition
• Clarifies circumstances when health care providers are permitted to communicate with friends, family members, law enforcement, or others
Understanding *Spouse, Family Member, and Marriage*

- Addresses effect of 2013 Supreme Court Windsor decision on certain provisions
  - Permitted disclosures to family members
  - Prohibited uses & disclosures of genetic information for underwriting
- Clarifies that spouses include both same-sex and opposite-sex individuals who are legally married, whether or not they live or receive services in a jurisdiction that recognizes their marriage
Guidance on HIPAA Privacy in Emergency Situations

• Issued November 11, 2014 to remind HIPAA covered entities and their business associates of the ways in which PHI may be shared in an emergency situation, and to underscore that the protections of the Privacy Rule are not set aside during an emergency.

• Reviews the importance of protecting the privacy of PHI while balancing appropriate uses and disclosures of the information for treatment, public health, and other critical purposes.
New Guidance:

The HIPAA Omnibus Rule
https://www.youtube.com/watch?v=mX-QL9PoePU
Consumer Awareness:

Your New Rights Under HIPAA - Consumers
https://www.youtube.com/watch?v=3-wV23_E4eQ
Over 275,000 views since September 4, 2013
Model Notices of Privacy Practices

- Four Designs
  - Booklet
  - Layered
  - List
  - Plain text

- In English & Spanish
- Different versions for health plans and health care providers
- Customizable
- Tested for content & design
Guide for Law Enforcement

- Developed in cooperation with the Federal Bureau of Investigation
- Provides snapshot of entities that are and are not required to comply
- Outlines permissible law enforcement disclosures
• Medscape: free CME and CE Training
  – Resource Center
  – Training Modules

http://www.medscape.org/sites/advances/patients-rights
Electronic Protected Health Information:

http://www.healthit.gov/
Mobile Devices:

http://www.healthit.gov/mobiledevices
www.healthit.gov/mobiledevices

- Fact sheets
- Posters
- Brochures
QUESTIONS?

http://www.hhs.gov/ocr/privacy