Health Privacy Training Seminar: Health Insurance Portability and Accountability Act ("HIPAA") and Select State Privacy Laws

Iowa State Association of Counties

May 1, 2014

Alissa Smith, Esq.
In the News

The Des Moines Register

FBI looking into patient-records security breach at UnityPoint Health

October 2, 2013
Tony Leys

The FBI is investigating an incident in which someone gained unauthorized access to the medical records of up to 1,800 patients at UnityPoint Health hospitals, the company said today.

The unidentified person worked for another company and was not authorized to view medical records. UnityPoint said in a press release. The person apparently used other people’s passwords to get into the computer system.

UnityPoint, which used to be called Iowa Health System, operates hospitals and clinics throughout Iowa and parts of Illinois. It said it has sent letters about the breach to the affected patients and has offered to provide free credit service to them.

The company said it is working with authorities, which is investigating.

It said theandler information could include addresses, birth dates, Social Security numbers and insurance accounts and possibly more than 10 percent of the patients.

Security numbers of 3,400 employees also might be affected, the company said.

The incidents happened through August 2013, UnityPoint said in the release.

The Des Moines Register

DHS employees blamed for security breach

Data for about 2,000 people transmitted outside network

March 7, 2014
Tony Leys

Inappropriate practices by two state workers led to a security breach involving personal information about 2,042 people in Polk County, state officials said Friday.

The Iowa Department of Human Services said “appropriate personnel action” was taken against the unidentified employees. Officials would not say whether that means the workers were fired, suspended or subject to other punishments.

According to a department news release, the incidents happened over five years, starting in 2008. The information involved Social Security numbers and personal information about children and dependent-adult abuse.

The department said the employees “inappropriately used personal email accounts, online storage accounts and personal electronic devices.”

“Individuals who receive a letter notifying them of the breach can get more information if they are concerned their identity may be compromised, and they can sign up for free credit monitoring,” the state agency said. “They can call the Iowa Concern Hotline at 1-800-447-1985.”

The department said it would block access to online file-storage sites and would stress proper practices during regular training. The company is based in West Des Moines. In central Iowa, its hospitals include Iowa Methodist Medical Center and Iowa Lutheran Hospital, both in Des Moines.

“Individuals who receive a letter notifying them of the breach can get more information if they are concerned their identity may be compromised, and they can sign up for free credit monitoring,” the state agency said. “They can call the Iowa Concern Hotline at 1-800-447-1985.”

The department said it would block access to online file-storage sites and would stress proper practices during regular training. The company is based in West Des Moines. In central Iowa, its hospitals include Iowa Methodist Medical Center and Iowa Lutheran Hospital, both in Des Moines.
Outline of Presentation

- HIPAA Background
- HIPAA Audits and Enforcement; Affirmative Defense
- Compliance To Do List; Review Manual
- Select Issues
  - Hybrid Entity/Affiliated Covered Entity/Privacy Officer/Security Officer Designation
  - Workforce Designation/Hiring and Termination Procedures
  - Risk Assessments
  - Business Associates
  - Mobile Devices and Social Media
  - HIPAA and Mental Health Privacy/Select Iowa Privacy Laws
  - Breach Notification
HIPAA Statutory and Regulatory Background

- Aug. 8, 1996- HIPAA signed into law
- Feb. 20, 2003- **Security Final Rule** (compliance by April 21, 2005)
- Feb. 17, 2009- **ARRA HITECH** signed into law
- Aug. 24, 2009- HITECH Breach Notification Interim Final Rule (effective Sept. 23, 2009)
- July 14, 2010- Proposed Regulations to implement a number of HITECH’s Privacy, Security and Enforcement provisions
- Jan. 25, 2013- **HIPAA HITECH Omnibus Final Rule** published (effective March 26, 2013; and **compliance generally required by Sept. 23, 2013**)


HIPAA: Overview

- The Privacy Rule: addresses the Use and Disclosure of PHI by Covered Entities and Business Associates and establishes individuals’ privacy rights to understand and control how their health information is access, used or disclosed.

- The Security Rule: establishes requirements for protecting electronic PHI.

- The Enforcement Rule: establishes both civil money penalties (“CMPs”) and federal criminal penalties, as well as procedures for agency enforcement and factors for assessing CMPs.

- The Electronic Transactions and Code Sets Rules: HIPAA adopted certain standard transactions for Electronic Data Interchange (EDI) of health care data (claims and encounter information, payment and remittance advice, claims status, eligibility, enrollment and disenrollment, referrals and authorizations, coordination of benefits and premium payment). Certain standards must be used when conducting a standard transaction electronically. HIPAA also adopted specific code sets for diagnoses and procedures to be used in all transactions (HCPCS, CPT-4, CDT, ICD-9, ICD-10 and NDC).

- The Breach Notification Rule: requires notification to HHS, the individual and potentially the media following a Breach of Unsecured PHI.
HIPAA’s Impact on Our Work Environment

– **Internal Compliance**
  • Safeguards, audits and enforcement more important than ever

– **Patient/Family Interaction**
  • Think before sending PHI

– **Interaction with Colleagues/other health care providers, payors, agencies**
  • Use appropriate safeguards

– **Interaction with Business Partners**
  • BA Agreements; Assess risk; HIPAA liability for actions of agents

– **Mobile Devices and Social Media**
  • Common and easy; But, biggest risk
• **General Rule:** Covered entity workforce members may only use or disclose protected health information as permitted under HIPAA (or, under state law if state law is more restrictive in a particular area, such as privacy for mental health).

• **Key Definitions:**

**Covered Entity** - health care provider (individual and organization) that exchanges health information electronically in a transaction for which HHS has adopted standards (billing, insurance, etc.); also health plans and healthcare clearinghouses.

**Protected Health Information** - individually identifiable health information. Information is “individually identifiable” unless all 18 identifiers are removed and no actual knowledge that the health information could be used alone or in combination with other information to identify the individual.
General HIPAA Security Rules

- The HIPAA Security Rule applies to electronic PHI ("ePHI").
- Covered Entities must implement administrative, technical and physical safeguards to protect the confidentiality, integrity and availability of all ePHI it creates, receives, maintains or transmits.
- As with the Privacy Rule, workforce members must only be allowed access as needed for their job/function/assignment, workforce members must be trained, and appropriate sanctions must be applied to workforce members who fail to comply.
HIPAA Security Rule: Risk Analysis

• **Risk Analysis:**
  – This must be completed to document all repositories of ePHI:
    • identify security measures in place for all repositories
    • identify vulnerabilities related to each repository
    • assign risk level
    • determine risk mitigation strategies
    • reassess periodically
  – All safeguards implemented flow from the findings in the documented risk analysis.
• Some of the Security Rules:
  – Workforce members must be assigned a unique user name/number.
  – Information systems activity must be reviewed regularly to track user access.
  – Passwords must be required and changed.
  – Automatic logoff procedures should be implemented.
  – Termination procedures must be implemented to turn off workforce access at the end of employment/engagement.
HIPAA Enforcement

• HHS OCR interprets and enforces the Privacy Rule, Security Rule and Breach Notification Rule

• Civil Penalties
  – One Affirmative Defense

• Criminal Penalties

• No Private Right of Action (Note, state privacy laws may include private rights of action)

• Liability for Actions of Business Associates

• Investigations, Corrective Action, Working with Other Governmental Agencies
• **Civil Penalties**
  – Increased Penalties in 2011 (up to $1.5M per violation per year)
  – Tiered penalty structure based on level of negligence and how quickly the violation was corrected
  – Secretary of HHS has discretion in assessing penalty based upon nature and extent of violation and harm caused
  – **Key Affirmative Defense**: No CMPs may be assessed if violation corrected within 30 days (except in cases of wilful neglect)
  – HHS cannot impose a civil penalty if a criminal penalty is imposed
HIPAA Enforcement: Criminal Penalties

**Criminal Penalties**

- Covered Entities and individuals who knowingly obtain or disclose PHI in violation of HIPAA face fine up to $50,000 plus imprisonment for up to 1 year.
- Offenses committed under false pretenses allow penalties up to $100,000 with up to 5 years in prison.
- Offenses with intent to sell, transfer or use PHI for commercial advantage/malicious harm permit fines up to $250,000 and imprisonment up to 10 years.
Enforcement: Liability for BA

- Covered Entities are liable for acts of Business Associates acting as “agents”
  - OCR made clear in the Final Rule that it will hold a CE liable for the activities of its BA (and a BA liable for the activities of its sub) if there is an agency relationship, and will apply the Federal Common Law of Agency to determine if there is an agency relationship.

  - Of reported breaches involving more than 500 individuals, more than 1/4th were caused by business associates.

  - Much higher estimates for reported breaches involving less than 500 individuals.
HIPAA Enforcement: Investigations, etc.

• Investigations and Compliance Reviews
  – OCR required to conduct an investigation or compliance review when a preliminary review of the facts indicate possible violations based on willful
  – As a practical matter, OCR currently investigates in all cases where an initial review indicates a possible HIPAA violation

• Resolution by Informal Means
  – OCR does not have to work to obtain voluntary corrective action/resolution by informal means, but can move directly to formal enforcement action, especially in cases of willful neglect

• OCR may disclose PHI to another governmental agency for a joint or separate civil or criminal enforcement activity (e.g. State Attorneys General & FTC)
## HIPAA Enforcement Pre-2011: Resolution Agreements

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity/Entities</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 2010</td>
<td>Management Services Organization (improper disclosure)</td>
<td>$35,000 + CAP</td>
</tr>
<tr>
<td>July 2010</td>
<td>Rite Aid Corp. (improper trash disposal)</td>
<td>$1 million + CAP</td>
</tr>
<tr>
<td>Jan. 2009</td>
<td>CVS Pharmacy (improper trash disposal)</td>
<td>$2.25 million + CAP</td>
</tr>
<tr>
<td>July 2008</td>
<td>Providence Health &amp; Services (stolen backup tapes and laptops)</td>
<td>$100,000 + CAP</td>
</tr>
</tbody>
</table>
HIPAA Enforcement Actions

• In 2011, HIPAA enforcement rules were significantly strengthened to provide for much higher penalties and to grant HHS enhanced authority to investigate and assess penalties.

• In recent enforcement actions, HHS has clearly focused on electronic PHI and mobile devices.

• As a result, covered entities should implement appropriate safeguards to protect their ePHI, especially ePHI on mobile devices and laptops.
## HIPAA Enforcement: 2011

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity/Entities &amp; Basic Facts</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>July 2011</td>
<td>UCLA (employees snooping on patients, including celebrities)</td>
<td>$865,500 + CAP</td>
</tr>
<tr>
<td>Feb. 2011</td>
<td>The General Hospital Corporation and Massachusetts General Physicians Organization Inc. (records left on train)</td>
<td>$1 M + CAP</td>
</tr>
<tr>
<td>Feb. 2011</td>
<td>First and only CMP Case: Cignet Health (denied patients access to records; failure to cooperate with OCR’s investigations)</td>
<td>$4.3 M</td>
</tr>
</tbody>
</table>
## HIPAA Enforcement: 2012

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity/Entities &amp; Basic Facts</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dec. 2012</td>
<td>The Hospice of Northern Idaho (unencrypted laptop stolen - first with less than 500)</td>
<td>$50,000 + CAP</td>
</tr>
<tr>
<td>Sept. 2012</td>
<td>Massachusetts Eye and Ear Infirmary and Massachusetts Eye and Ear Associates, Inc. (unencrypted laptop stolen)</td>
<td>$1.5 M + CAP</td>
</tr>
<tr>
<td>June 2012</td>
<td>Alaska Medicaid (unencrypted USB hard drive stolen)</td>
<td>$1.7 M + CAP</td>
</tr>
<tr>
<td>April 2012</td>
<td>Phoenix Cardiac Surgery, P.C. (patient appointments posted on the internet)</td>
<td>$100,000 + CAP</td>
</tr>
<tr>
<td>March 2012</td>
<td>BCBST (57 unencrypted computer hard drives stolen)</td>
<td>$1.5 M + CAP</td>
</tr>
</tbody>
</table>
## HIPAA Enforcement: 2013

<table>
<thead>
<tr>
<th>Date</th>
<th>Entity/Entities &amp; Basic Facts</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>December, 2013</td>
<td>Adult and Pediatric Dermatology (first settlement for not having policies, procedures and training related to the breach notification rule) unencrypted thumb drive stolen from employee vehicle</td>
<td>$150,000 + CAP</td>
</tr>
<tr>
<td>August, 2013</td>
<td>Affinity Health Plan, Inc. (returned multiple leased photocopiers with PHI of 344,579 individuals not deleted)</td>
<td>$1,215,780 + CAP</td>
</tr>
<tr>
<td>July, 2013</td>
<td>WellPoint  (leaving information accessible over patient access web-based app/portal)</td>
<td>$1.7 M</td>
</tr>
<tr>
<td>June, 2013</td>
<td>Shasta Regional Medical Center (disclosure of PHI to media outlets)</td>
<td>$275,000 + CAP</td>
</tr>
<tr>
<td>May, 2013</td>
<td>Idaho State University (breach of unsecured ePHI due to disabled firewall protections)</td>
<td>$400,000 + CAP</td>
</tr>
</tbody>
</table>
HIPAA Enforcement: 2014

- Skagit County, Washington
  - Skagit County Public Health Department serves 118,000 residents by providing health services, including mental health services
  - March 7, 2014
  - $215,000 settlement
  - Agreed to ongoing corrective action plan (3 years)
  - “This case marks the first settlement with a county government and sends a strong message about the importance of HIPAA compliance to local and county governments, regardless of size,” said Susan McAndrew, deputy director of health information privacy at the HHS Office for Civil Rights (OCR). “These agencies need to adopt a meaningful compliance program to ensure the privacy and security of patients’ information.”
HIPAA Enforcement: 2014 (cont’d)

- Investigation opened after OCR received a breach report that money receipts with ePHI of 7 individuals were inadvertently left on a publicly accessible web server maintained by the County.

- When OCR investigated, they found that 1,581 individual’s PHI was accessible by the public on the server. ePHI included sensitive information (testing and treatment of infectious diseases)

- OCR also found “general and widespread non-compliance by Skagit County with the HIPAA Privacy, Security and Breach Notification Rules.”
  - Left ePHI of 1,581 patients on public web server for 14 days
  - Failed to provide breach notification to the 1,581 patients
  - Failed to implement sufficient HIPAA policies and procedures
  - Failed to provide HIPAA training to workforce
• 2 HIPAA Settlements in April
  – Both involved thefts of unencrypted laptops
  – Concerta Health (a health care clinic chain)
    • In multiple risk assessments, Concerta identified lack of encryption on laptops as a “critical risk”, but did not implement policies to address risk.
    • HHS investigation launched after breach notification
    • $1,725,220 + CAP
  – QCA (AR-based health plan)
    • Unencrypted laptop with 148 individuals’ data stolen
    • Investigation found no good policies or safeguards
    • $250,000 + CAP
  – Both must report to Congress annually on HIPAA compliance.
OCR Audit Program

- The HITECH Act mandates the performance of periodic privacy and security audits
- KPMG LLP was contracted by OCR to perform the Audits in the Audit Pilot Program
- Pilot Program: 115 audits
  - 20 initial audits
  - 95 final pilot audits through Dec. 2012
  - Covered privacy, security and breach notification
  - Focused on education and prevention (but OCR may determine it is necessary to open a compliance review based on initial findings)
  - Results were reviewed through 2013
- Essentially any covered entity can be subject to an audit regardless of size or type
OCR Pilot Audit Results

• Uncovered a wide variety of HIPAA compliance failures

• 2/3rds of the entities audited did not have a completed and accurate risk assessment.
Initial 20 Audits: Privacy Rule Violations

Deceased Individuals: 4
Personal representatives: 4
Confidential communications: 4
Business associate contracts: 2
Permitted uses and disclosures: 1
Required uses and disclosures: 1
Consent for uses and disclosures: 3
Opportunity to Object: 1
Authorization for uses and disclosures: 1
Disclosures for administrative purposes: 1
Limited uses and disclosures: 1
Disclosures for internal use: 1
Re-identification of PHI: 1
De-identification of PHI: 1
Minimum Necessary Disclosures: 2
Uses and Disclosures for fundraising: 2
Verifications of requesters: 3
Uses and Disclosures for Underwriting: 1
Initial 20 Audits: Security Rule Violations
The next phase of audits are likely to be in the latter part of 2013, “but certainly by 2014…” Leon Rodriguez, Director of HHS OCR

HHS evaluating Audit Pilot Program findings

“...I think we’re learning from the audits, and from the monetary settlement cases we have done [after investigations], is there’s plenty of noncompliance out there and plenty of room for improvement. From that perspective alone, I expect that we’re going to continue to see monetary settlements for a long time to come.” Rodriguez
Future of the HIPAA Audit Program (cont’d)

- In February, 2014, HHS announced that it will soon launch the next phase of audits.
- First, it will survey 1,200 organizations (800 CEs and 400 BAs). From the survey responses, HHS will select who will be audited.
- HHS currently revising its audit tool.
Upcoming HIPAA Audits

- Very likely to focus on risk assessments.
  - On September 23, 2013 OCR director Leon Rodriguez reported that the covered entities audited in the pilot program often had conducted a "shallow risk analysis" that was not properly updated as circumstances changed, such as the when the entities developed new business strategies or implemented new information systems.
  - Rodriguez observed, "With any business change, an entity must review its risk analysis; yet, two-thirds of pilot participants -- including 80 percent of providers -- did not have a complete and accurate risk analysis."
Upcoming HIPAA Audits (cont’d)

- Very likely to focus on encryption and an organization’s underlying risk analysis in deciding whether to encrypt or not encrypt.

- Encryption is addressable (if no encryption, must document to justify decision and must select reasonable alternative)

- Leon Rodriguez reported that OCR's pilot audit program revealed that encryption was not always implemented (or even considered) by organizations. OCR observed that organizations either implemented encryption or did nothing at all in justifying and documenting reasonable alternatives.
Audit Readiness

• Key is to be able to quickly demonstrate compliance through:
  – Up to date policies, procedures, forms and logs
  – Active enforcement of policies and procedures (and documentation of enforcement) to demonstrate consistency between policies, procedures and controls
  – Current staff training
  – Documentation to demonstrate appropriate controls exist (testing, auditing, monitoring, investigating, log files, risk assessments)
Compliance To Do List

1. Identify Covered Entity
2. Identify Hybrid Entities and Affiliated Covered Entities
3. Designate Privacy Officer and Security Officer
4. Adopt Policies and Procedures
5. Designate Workforce
6. Assign Workforce Access Levels
7. Train Workforce; Establish regular retraining
Compliance To Do List (cont’d)

8. Complete Risk Assessment and Implement Mitigation/Safeguards

9. Establish a master list of business associate relationships to track compliance

10. Establish Privacy Policies and Procedures
   • Who is in charge of receiving requests for records?
   • Who is in charge of receiving complaints?
   • Is there a HIPAA compliance committee?
   • How often are policies reviewed and updated?
   • How often are risk assessments completed?
   • Who updates the Notice of Privacy Practices?
   • Who handles Business Associate Relationships?

11. Establish audit schedule for HIPAA audit preparation and tracking internal access
Designations

- Hybrid Entity
- Affiliated Covered Entity
- Privacy Officer/Security Officer
- Compliance Committee
- Workforce
- Hiring Checklist
- Termination Checklist
New Tool to Assist with Risk Assessment

• On March 28, HHS published a new tool to assist CEs with their risk assessments.

• 156 Y/N questions in a paper or web-based format

• Every question has a next set of steps to fill in for implementing safeguards

• Each question provides resources to help understand the context of the question, the potential impact on the provider if the requirement is not met, and includes the actual language from the Security Rule.

• Tool can be printed in PDF or Excel to produce report for auditors.
Business Associates

• BA Policy Changes
• BA Agreement Checklist
• Update BAA Template Agreement
• Inventory/Catalog BAs
• Amend Current BAAs (note grandfathering)
Business Associate Policy Changes

• Update the Definition of a BA
Business Associates and Subcontractors: Who is a Business Associate?

- Final Rule Expanded the Definition of a BA:
  - Subcontractors of BAs, and Subs of Subs, are now BAs
  - An entity that maintains PHI (including physical storage and e-storage/cloud storage) is a BA, even if the entity does not actually view the PHI
    - This includes Google and Microsoft cloud providers
  - An entity that provides data transmission services of PHI on behalf of the CE and requires access to the PHI on a routine basis.
    - A mere “conduit”, such as a courier service, does not require access to PHI on a “routine basis,” but rather on a random or infrequent basis, and thus is not a BA; e.g., USPS, UPS, internet service provider.
Business Associates and Subcontractors: Who is a Business Associate?

• The definition also now explicitly includes:
  • Health information organizations (no def. because industry is still evolving), E-prescribing gateways, or other entities that provide data transmission services to a CE and that require access on a “routine basis” to PHI.
  • A person that offers a personal health record to one or more individuals on behalf of a CE.
• Changes to requirements of the terms that must be in the BAA:
  – No more requirement to report to the Secretary of HHS a BA’s pattern of activity or practice that is a material breach of the BAA, when termination of the HAA is not feasible.
  – BA must comply, where applicable, with the Security Rule with respect to ePHI
  – BA must report to the CE any breaches of unsecured PHI (consider a short timeframe, such as 5-10 days; consider adding other details of the BA notification to and cooperation with the CE)
• Changes to requirements of the terms that must be in the BAA (cont’d):
  – BA must ensure that any subcontractors that create, receive, maintain or transmit PHI on behalf of the BA agree to the same restrictions and conditions that apply to the BA in the BAA between the BA and the CE.
  – To the extent the BA is to carry out a CE’s obligations under the Privacy Rule, the BA must comply with the Privacy Rules that would apply to the CE in performance of such obligations.
Business Associate Agreement Changes (considerations)

- CEs are liable for the actions of BAs if the BAs are the “agents” of the CEs.

- OCR’s final rule indicates that “agency” will likely be construed broadly to encompass many BAs.

- Given the potentially broad application of the “agency” test, and the significantly increased penalties under HIPAA, now is a good time to consider adding additional provisions to BAAs:
  - Indemnification clauses
  - A requirement for BA to obtain insurance to cover breaches
  - A requirement for the BA to pay for any breach notifications, expenses, costs, and fines, associated with breaches caused by the BA or its sub.
  - A requirement for the BA to pay for a certain period of credit monitoring for individuals when the BA or its sub caused the breach.
Current BAAs Must be Amended

• Grandfathered Agreements:
  – HIPAA-compliant BAAs that were in place prior to January 25, 2013; and
  – the BAA is not renewed or modified from March 26, 2013 until September 23, 2013.

• Grandfathered Agreements must be amended to comply with the HIPAA Final Rule the earlier of:
  – The date the BAA is renewed or modified (evergreen contracts do not trigger the requirement), or
BAA Grandfathering Reminder

- Grandfathering of the BAA ONLY applies to the requirement to amend the BAA to include certain mandatory provisions, but does **not** affect any other HIPAA compliance obligations.
  - E.g., as of Sept. 23, 2013, the BA is prohibited from using or disclosing PHI in a manner contrary to the Privacy Rule, even if the BAA has not yet been amended to say so.
Business Associate Strategy

• Inventory Business Associates
  – Have you recognized all BAs under new definition?
    • E.g., document storage companies (physical or e-storage) are now clearly BAs.
    – Do you unnecessarily have BAAs with non-BAs?

• Consider assigning risk levels to BAs to determine, and take appropriate action (terms of BAAs, auditing, monitoring, etc.)
  – Amount of PHI
  – Evidence of BA controls

• Consider agency relationship for each BA arrangement
  – Timing for Breach notification
  – Level of monitoring

• Amend current BAAs to comply with law and to reflect level of risk-agency status of individual BA

• Add BAAs for previously unrecognized BAs; delete BAAs if unnecessary.
Biggest Risk Areas: Mobile Devices and Social Media

- **Mobile Devices**
  - It has become common for health care providers to communicate with patients using mobile devices or to access/relay PHI to other providers using mobile devices.
  - The unauthorized disclosure of ePHI is a big risk when using mobile devices because they are small, portable, highly visible, unlikely password protected, unlikely to have encrypted PHI, and likely to connect with Wi-Fi (further risking interception).

- **Social Media**
  - Staff and providers must not post or share information about patients that could potentially identify a patient
Statistics on Mobile Device Data Breaches

• Privacy Rights Clearinghouse and the Open Security Foundation: Analysis of data from January 1, 2009 through May 31, 2012 concludes that mislaid, stolen or discarded portable devices caused records with personally identifiable information of 80.7 million individuals to be breached.

• As of November 1, 2012, approx. 40% of the breaches involving 500 or more individuals that were reported to HHS involved mobile devices.
Mobile Devices Data Breaches: Real World Examples

- July, 2013- $1.7M settlement with WellPoint for lack of administrative and technical safeguards surrounding an online application database. HHS also found a lack of sufficient policies and procedures. Breach affected over 600,000 individuals.

- August 7, 2013- $1.2M settlement with health plan for failing to erase ePHI stored on photocopiers before returning the machines to leasing agent. HHS also cited failure to implement policies and procedures, and failure to perform adequate risk assessment. Breach affected 344,579 individuals.

- Sept. 17, 2012- $1.5M settlement with Mass. Provider who had unencrypted personal laptop stolen, contained PHI of more than 500 patients and research subjects, including patient prescription and clinical information.
Statistics on Social Media Data Breaches

• Research indicates that 35% of practicing physicians have received friend request from a patient or patient’s family member, and 16% of practicing physicians have visited an online profile of a patient or patient’s family member.

• Can work experiences be shared without violating patient privacy?
  – One meta-analysis of physician blogs found that nearly 17% included enough information about patients for them to be identified.

Social Media Data Breaches: Real World Example

April, 2011: “Alexandra Thran, MD, a 48 year old emergency room physician formerly at Westerly Hospital, Westerly, RI, posted a few notable cases she had seen in the ER on Facebook. She avoided using patient names or ages. Apparently, "unauthorized third parties" were able to determine one patient's identity from the post. When Dr. Thran learned of this, she immediately deleted her account.

Westerly Hospital concluded that Dr. Thran used her Facebook account "inappropriately." Both the hospital and Dr. Thran agreed that she had "no intention to reveal any confidential patient information."

The hospital's solution? Terminate Dr. Thran's hospital privileges.

On April 13, 2011, the Rhode Island Board of Medical Licensure found Dr. Thran guilty of "unprofessional conduct." The Board handed out a $500 fine with instructions for her to attend a CME course dealing with physician-patient confidentiality issues.”

http://boards.medscape.com/forums?128@834.aac1agTygA9@.2a090c48!comment=1
http://www.boston.com/lifestyle/health/articles/2011/04/20/for_doctors_social_media_a_tricky_case/
Protecting Yourself from a Mobile Device or Social Media HIPAA Breach

1. Create (and follow) HIPAA Privacy and Security policies specifically addressing the exchange of PHI using mobile devices and social media

2. Impose appropriate safeguards on use of mobile devices and social media

3. Train workforce members; Audit for compliance
Why Create (and follow) Mobile Device and Social Media Policies and Procedures?

• HIPAA allows providers to communicate with patients and with other providers and to share ePHI using mobile devices as long as “reasonable safeguards” are applied when doing so.

• There is no specific requirement to have a social media/networking and mobile device policy.

• However, given today’s environment of near-constant use of social media/networking, common access to PHI via mobile and highly portable devices, and where the vast majority of reported breaches stem from inappropriate safeguarding of ePHI, would the government conclude the lack of a policy on these topics resulted in a covered entity’s failure to implement the reasonable safeguards required under HIPAA?
What Safeguards Should be in a Mobile Device Policy?

• Require providers to register their mobile devices if Bring Your Own Device (“BYOD”) is allowed
• Require use of passwords or other use authentication
• Install and enable encryption for ePHI including text or SMS messages
• Install and activate remote wiping and/or remote disabling ability
• Disable and do not install or use file sharing applications
• Install and enable a firewall
• Install and enable security software (and update it)
• Do not share ePHI over public Wi-Fi
• Delete all stored ePHI before discarding or reusing the mobile device.

What Safeguards Should be in Place for Social Media Policies and Procedures?

• Restrict the types of information workforce members can share via social media

• Prohibit social media use during the work day

• Keep personal and professional sites separate

• Model Policy Guidelines for the Appropriate Use of Social Media and Social Networking in Medical Practices published by the Federation of State Medical Boards

Train All Workforce Members; Audit

- Ensure all staff and personnel receive copies of your HIPAA Privacy and Security Manuals, including policies relating to mobile devices and social media.
- Consider annual testing for employees.
- Audit to ensure staff and personnel with access to ePHI on mobile devices have implemented the appropriate safeguards.
HIPAA and Mental Health Privacy

• There is often a lot of confusion about HIPAA and mental health information.

• In general, HIPAA treats all health information the same.

• Exception: Psychotherapy notes
  – Notes recorded by a mental health professional documenting or analyzing the contents of a conversation during a private counseling session/group session and that are separate from the rest of the patient’s medical record. These do not include information regarding prescriptions, treatment, summaries of diagnosis/functional status/treatment plan/symptoms/prognosis/progress or other information in the medical record.
  – Individual cannot access; no combination of authorization; usually need authorization to disclose even for TPO.
  – Exception for disclosures required by law (mandatory reporting/duty to warn)
HIPAA and Mental Health (cont’d)

- Recent Guidance from HHS Regarding HIPAA and Mental Health Information
  - Notice to law enforcement or others when individual is imminent threat
  - Notice to law enforcement about patient release when required by State law
  - Communication with family and friends involved in patient’s care
  - Minimum necessary rule applies
  - Minors

http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/mhguidance.html
Iowa law and Mental Health Information

• **HIPAA Preemption:**
  – HIPAA is meant to be comprehensive and uniform throughout the United States.
  – However, HIPAA does not repeal (or “preempt”) any state laws that are not contrary to the provisions of HIPAA, which are related to the privacy of individually identifiable health information that are more stringent than HIPAA.

• Iowa’s Mental Health Privacy Law is more protective than HIPAA of mental health information in several respects, so before disclosing any mental health information, Iowa law must be reviewed.
Iowa’s Mental Health Privacy Law (cont’d)

• **Definitions**

  • *Mental Health Information* is defined as oral, written, or recorded information which indicates the identity of an Individual receiving professional services and which relates to the diagnosis, course, or treatment of the Individual’s mental or emotional condition.

  • *Professional Services* means diagnostic or treatment services for a mental or emotional condition provided by the mental health professional.
Iowa’s Mental Health Privacy Law (cont’d)

- General Iowa Rules Governing Disclosure of Mental Health Information
  - Voluntary Authorizations
  - Medical Emergencies
  - Disclosures to Providers of Professional Services
  - Administrative Disclosures
  - Compulsory reporting or disclosure requirements of other state or federal law relating to the protection of human health and safety
  - Disclosures for Claims Administration and Peer Review
  - Disclosures to Family
Iowa’s Mental Health Privacy Law (cont’d)

- Potential consequences for violating Iowa’s Mental Health Privacy Law
  - Private right of action for emotional distress has been recognized by Iowa’s Supreme Court for violation of Iowa’s mental health privacy law (no need for individual to show physical injury or outrageous conduct in order to prevail, but individual will need to show substantial evidence of emotional distress caused by illegal disclosure)

  *Doe v. Central Iowa Health System* (Iowa Supreme Court, 2009)
Iowa Chemical/Substance Abuse Treatment Privacy Law

- Iowa’s chemical/substance abuse treatment privacy law is more protective of these records than HIPAA.

- Records of the identity, diagnosis, prognosis, or treatment of a person which are maintained in connection with the provision of substance abuse treatment services are confidential under Iowa law.

- Exception for medical emergencies.

- Criminal penalties associated with illegal disclosure.
Iowa Chemical/Substance Abuse Treatment Privacy Law (cont’d)

• A physician or any person acting under the direction or supervision of a physician, or a Facility (as defined under Iowa Code §125.2) shall not report or disclose to any law enforcement officer or agency, the name of an Individual who has applied for voluntary treatment or rehabilitation services for substance abuse, or the fact that the treatment was requested or undertaken, nor shall such information be admissible as evidence in any court, grand jury or administrative proceeding unless authorized by the Individual seeking treatment.
Iowa Chemical/Substance Abuse Treatment Privacy Law (cont’d)

• If a minor personally makes application seeking such treatment, the fact that the minor sought treatment or rehabilitation or is receiving treatment or rehabilitation services shall not be reported or disclosed to the parents or legal guardian of such minor without the minor’s consent.

• Further, federal law adds restrictions on disclosures of drug abuse information obtained by a federally assisted drug abuse program, that must be followed by third party payors, entities having direct administrative control over such programs, and persons who receive patient records directly from such programs who are notified of the restrictions on redisclosure of the records.
Iowa law and HIV Tests

• Iowa law is more protective than HIPAA of information related to HIV or AIDS tests. Any information related to HIV or AIDS tests, including reports and records obtained, submitted or maintained under Iowa law is strictly confidential medical information and shall not be disclosed except as provided by Iowa law.

• AIDS/HIV information disclosed under Iowa law must include a notice to the recipient that the recipient must continue to maintain the confidentiality of the information and that the recipient must not further disclose the information without a specific authorization of the Individual or as otherwise permitted by law.

• Both civil and criminal penalties for illegal disclosure.
HIPAA Breach Notification Rule

• A potential breach is presumed to be a “Breach” (requiring breach notification) unless
  – an exclusion applies or
  – a 4-part risk assessment demonstrates that there is a low probability that the PHI has been compromised.
Breach:

The access, acquisition, use or disclosure of **unsecured PHI** not permitted under the Privacy Rule that **compromises the security or privacy of the PHI**

Unsecured PHI:

PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by HHS (e.g., encrypted, shredded).
HIPAA Breach Notification Rule: Exclusions

• Three Exclusions
  – Unintentional access by workforce member/person acting under CE/BA authority if in good faith, within the scope of authority and no further HIPAA violation
  – Inadvertent disclosure by authorized person at CE or BA to another authorized person at the same CE or BA or OHCA in which the CE/BA participates, and no further HIPAA violation
  – CE/BA has good faith belief that person to whom disclosure was made would not reasonably have been able to retain the information
HIPAA Breach Notification Rule: Risk Assessment

- CE can simply make breach notification without performing the 4-part risk assessment.
- BUT, in order to determine a breach notification is not required, entity must have addressed all four factors in the risk assessment and determined that the use/disclosure of the PHI poses a low probability that the PHI has been compromised.
1. The nature and extent of the PHI involved (including the types of PHI, and the likelihood of re-identification);
   - Analyze probability PHI could be used by unauthorized recipient in a manner adverse to the individual or to further recipient’s own interests (thus, the risk of harm standard still relevant)
   - SSN, credit card numbers, etc. increases risk of identity theft or financial harm
   - Analyze types of clinical data disclosed
HIPAA Breach Notification Rule: 4 Part Risk Assessment (cont’d)

2. The unauthorized person who used the PHI or to whom the disclosure was made;
   - A CE, BA, or member of workforce may be less likely to result in compromise to PHI because recipient is accustomed to protecting confidentiality
3. Whether the PHI was actually acquired or viewed; and
   – Technical/forensic investigation critical (access logs, audit trails)
   – Stolen laptop example from preamble
   – Wrong address example from preamble (letter not opened)

4. The extent to which the risk to the PHI has been mitigated
   – Satisfactory assurances from recipient
   – How quickly was PHI recovered
HIPAA Breach Notification Rule: Timing

• CE has 60 days from its discovery to make notifications of the breach to
  – the affected individual
  – the Secretary of HHS (an annual report by end of Feb for all Breaches that affect less than 500; otherwise an immediate report if breach affects 500 or more)
  – to the media if Breach affects more than 500 in a state.

• A Breach is “discovered” when “any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate” knows or should reasonably have known of the breach.
Breach Notification Scenarios

- Is this a “Breach”?
- Follow Flowchart
- Complete Risk Assessment
- Complete Letter to Patient
- When is this reported to HHS?
- When is this reported to the media?
- Keep Records of all investigations and assessments for at least 6 years.
Breach Notification Scenarios

- 1. Deceptive Spouse Case
- 2. Lost Thumb Drive Case
- 3. Photograph Case
- 4. Misdirected Fax Case
- 5. Misdirected Voicemail Case
- 6. Business Associate Case
Compliance To Do List

1. Identify Covered Entity
2. Identify Hybrid Entities and Affiliated Covered Entities
3. Designate Privacy Officer and Security Officer
4. Adopt Policies and Procedures
5. Designate Workforce
6. Assign Workforce Access Levels
7. Train Workforce; Establish regular retraining
8. Complete Risk Assessment and Implement Mitigation/Safeguards

9. Establish a master list of business associate relationships to track compliance

10. Establish Privacy Policies and Procedures
    • Who is in charge of receiving requests for records?
    • Who is in charge of receiving complaints and breaches?
    • Is there a HIPAA compliance committee?
    • How often are policies reviewed and updated?
    • How often are risk assessments completed?
    • Who updates the Notice of Privacy Practices?
    • Who handles Business Associate Relationships?

11. Establish audit schedule for HIPAA audit preparation and tracking internal access
Questions

Alissa Smith, Esq.
(515) 699-3267
smith.alissa@dorsey.com