Privacy and Security: HIPAA/HITECH/meaningful Use – Looking Back, Forging Ahead

Patti Kritzberger, RHIT, CHPS
Quality Health Associates of North Dakota
HIT/Quality Improvement Specialist

Quality Health Associates (QHA) of ND
• Formally known as North Dakota Health Care Review, Inc.
• Non-profit organization (no affiliation with any hospital in ND)
• Corporate office in Minot, ND
• Expertise in Quality Improvement, Data Analysis, Quality and Utilization Review, and Health Information Technology
• Contract with Centers for Medicare & Medicaid Services (CMS)
  – Subcontractor to the Great Plains Quality Innovation Network QIN-QIO to serve the state of North Dakota
  – Partnership with 3 other states (Kansas, Nebraska, and South Dakota)
  – New contract began on August 1, 2014

Objectives
• Overview of HIPAA
• Impact of HITECH
• Meaningful Use (CMS) versus Office of Civil Rights Audits
• Future of HIPAA, Meaningful Use and Audits
Overview of HIPAA

• Original Translation (6th Century BCE): "...All that may come to my knowledge in the exercise of my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal."
• Classic Translation (A long time ago): "...What I may see or hear in the course of treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep myself holding such things shameful to be spoken about."
• Modern Version – 1964: "...I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know. Most especially must I tread with care in matters of life and death."
• August 21, 1996 – President Clinton’s ‘First 100 Days’: Kassebaum-Kennedy Health Insurance Portability and Accountability Act

Significant Events

• Supreme Court recognized an implicit constitutional right of privacy in Griswold V. Connecticut in 1965
• Freedom of Information Act of 1967
• Privacy Act of 1974
• Health Insurance Portability and Accountability Act of 1996
• Joint Commission Information Management Requirements
• Medicare Conditions of Participation Requirements
• Confidentiality of Alcohol and Drug Abuse Patient Records Rule
• American Recovery and Reinvestment Act of 2009 – HITECH
• Healthcare Reform – Patient Protection and Affordable Care Act
• State Law (Examples: California, Minnesota)

Timeline

1996 • HIPAA Regulation Enacted
2003 • Privacy Rule Mandated
2005 • Security Rule Mandated
2009 • Interim ARRA/HITECH provision on Privacy and Security
2013 • Final ARRA/HITECH provision on Privacy and Security
External Factors Affecting Privacy and Security

- Amount and mobility of data is growing
- Technology advancements
- Massive interconnectivity
- Portable devices
- Cloud service
- Social networking
- Malware

Privacy and Security Issues in Healthcare Organizations

- Reduce costs
- EHR implementation
- Resistance to change
- Whose responsibility is it to protect PHI
- EHR security complexity
- Vulnerabilities in infrastructure or application changes
- Gaps in expertise

Categories of Breaches in 2015

- Banking/Credit/Financial: 34.4%
- Business: 10%
- Educational: 6.7%
- Government/Military: 8.9%
- Medical/Healthcare: 40%
2014 PHI Data Breaches by Type

<table>
<thead>
<tr>
<th>Type</th>
<th># of Breaches</th>
<th>% of Total</th>
<th># of Records</th>
<th>% of Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking / IT Incident</td>
<td>23</td>
<td>14.0%</td>
<td>4,750,716</td>
<td>53.4%</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>33</td>
<td>20.1%</td>
<td>2,732,738</td>
<td>30.7%</td>
</tr>
<tr>
<td>Theft</td>
<td>67</td>
<td>40.8%</td>
<td>847,918</td>
<td>9.5%</td>
</tr>
<tr>
<td>Other</td>
<td>17</td>
<td>10.4%</td>
<td>332,565</td>
<td>3.8%</td>
</tr>
<tr>
<td>Loss</td>
<td>16</td>
<td>9.8%</td>
<td>159,124</td>
<td>1.8%</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>8</td>
<td>4.9%</td>
<td>6,549</td>
<td>0.1%</td>
</tr>
<tr>
<td>Total</td>
<td>164</td>
<td>100%</td>
<td>8,899,610</td>
<td>100%</td>
</tr>
</tbody>
</table>

2014 PHI Data Breaches by Source/Device

<table>
<thead>
<tr>
<th>Device</th>
<th># of Incidents</th>
<th>%</th>
<th># of Records</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>22</td>
<td>13.4%</td>
<td>5,120,480</td>
<td>57.5%</td>
</tr>
<tr>
<td>Multiple devices</td>
<td>2</td>
<td>1.2%</td>
<td>2,030,000</td>
<td>22.8%</td>
</tr>
<tr>
<td>Laptops and other portable devices</td>
<td>41</td>
<td>25.0%</td>
<td>4,754,911</td>
<td>5.3%</td>
</tr>
<tr>
<td>Email</td>
<td>25</td>
<td>15.2%</td>
<td>468,873</td>
<td>5.3%</td>
</tr>
<tr>
<td>Paper</td>
<td>36</td>
<td>22.0%</td>
<td>340,961</td>
<td>4.1%</td>
</tr>
<tr>
<td>Other</td>
<td>21</td>
<td>12.8%</td>
<td>219,003</td>
<td>2.3%</td>
</tr>
<tr>
<td>Desktops</td>
<td>14</td>
<td>8.5%</td>
<td>204,138</td>
<td>2.3%</td>
</tr>
<tr>
<td>Electronic Medical Records</td>
<td>3</td>
<td>1.8%</td>
<td>20,764</td>
<td>&lt;0.1%</td>
</tr>
<tr>
<td>Total</td>
<td>164</td>
<td>100%</td>
<td>8,899,610</td>
<td>100%</td>
</tr>
</tbody>
</table>

Objectives

- Overview of HIPAA
- Impact of HITECH
- Meaningful Use (CMS) versus Office of Civil Rights Audits
- Future of HIPAA, Meaningful Use and Audits
HITECH Act Has Teeth

The HITECH Act has significantly modified and strengthened many aspects of the HIPAA Security Rule, including imposition of penalties

- Widens the scope of protections available under HIPAA
- Increases potential liability for non-compliance
- Provides for more enforcement
- Affects Covered Entities and Business Associates

Modifications to the HIPAA Privacy, Security, Enforcement and Breach Notification Rule 2013

  - Most interim rules of ARRA were moved from Interim to Final
- March 26, 2013 – Effective Date
- September 23, 2013 – Compliance Date

Still Waiting for Final Rules…

- Accounting and Disclosures/Access Reports
- Guidance on Minimum Necessary
- Distribution of penalties and settlements to harmed individuals
Breach Notification Changes

- Risk of Harm analysis replaced with more objective Risk Assessment analysis:
  - Show evidence of evaluating
    - Nature and extent of PHI involved – Types and likelihood of re-identification
    - Unauthorized person(s) who used the PHI or whom it was disclosed to
    - If the PHI was acquired, viewed, disclosed or re-disclosed – interim rule specified if the PHI was accessed, disclosed, used, or acquired
    - The extent to which the risk to PHI has been mitigated
- Eliminates the exception in interim rule that limited data sets were not included in breach investigation

Updated Breach Definition

BREACH – an impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates there is a low probability that the PHI has been compromised

Examples of a Breach

- Fax containing PHI sent to the wrong fax number
- Email containing PHI sent to wrong recipient
- Employee inappropriately accessing co-workers chart or celebrity’s chart
- Release of information sent to wrong person
- Using social media to blog about specific patient diagnoses that can link to a patient
Changes to Business Associates – Final Rule

• Business Associates Definition
  – Old: An individual or organization who uses or discloses PHI on behalf of the covered entity
  – New: An individual or organization that creates, receives, maintains, or transmits PHI on behalf of a covered entity (HIE, data transmission services, offers a personal health record)
  – Mere Conduits: Very narrow definition; only applies to courier services (Postal Service, Internet Service Provider)

Covered Entities and Business Associates

• CE must enter into business associate agreements with contractors
• Contractors must enter into a business associate agreement with subcontractors
  – Subcontractor: A person to whom a business associate delegates a function, activity or service, other than in the capacity of a member of the workforce of such a business associate
  • These agreements with subcontractors follow the line down as far as it goes; each subcontractor who subcontracts any part of the work needs a business associate agreement

Impact of Changes on Business Associates

• They must comply with the administrative, physical and technical safeguards of the Security Rule, including policies and procedures
• They must comply with components of the Privacy Rule; not required to designate a privacy officer or provide a Notice of Privacy Practices
• They must comply with items a covered entity adds into business associate agreement
Other Changes to Final Rule

- Patient Access to Electronic Health Records
- Patient Access – Technical Safeguards
- Fundraising and PHI
- Research
- Access to Immunizations
- Access to Deceased Patient’s Records
- Marketing and PHI
- Selling PHI
- GINA Act

Objectives

- Overview of HIPAA
- Impact of HITECH
- Meaningful Use (CMS) versus Office of Civil Rights Audits
- Future of HIPAA, Meaningful Use and Audits

Privacy and Security
Meaningful Use (CMS) versus OCR Audits

<table>
<thead>
<tr>
<th>Meaningful Use (CMS)</th>
<th>OCR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meaningful Use Core Measure:</td>
<td></td>
</tr>
<tr>
<td>Eligible Professional (EP)</td>
<td></td>
</tr>
<tr>
<td>Core Measure 13, Stage 1</td>
<td></td>
</tr>
<tr>
<td>Core Measure 7, Stage 1</td>
<td></td>
</tr>
<tr>
<td>Eligible Hospital (EH)</td>
<td></td>
</tr>
<tr>
<td>Core Measure 7, Stage 1</td>
<td></td>
</tr>
<tr>
<td>EP/EH must conduct Security Risk Analysis on CEHRT</td>
<td></td>
</tr>
<tr>
<td>Figliozzi requests copy of Security Risk analysis</td>
<td></td>
</tr>
<tr>
<td>Failure of audit = return of incentive payment</td>
<td></td>
</tr>
<tr>
<td>Much deeper dive into EHR Security Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>Business Associate audit</td>
<td></td>
</tr>
<tr>
<td>Focus on EHR cloud service providers and EHR vendor</td>
<td></td>
</tr>
<tr>
<td>On-site audit (2-3 weeks)</td>
<td></td>
</tr>
<tr>
<td>Interviews</td>
<td></td>
</tr>
</tbody>
</table>
| Failure of audit = fraud?
OCR Phase 1 Findings
2011 – 2012

115 Covered Entities Audited
• Level 1 entities (26 total)
  – Large provider/health plan/clearinghouse
  – Revenue/assets > $1 billion
• Level 2 entities (31 total)
  – Larger regional hospitals/health plans/clearinghouses
  – Revenue/assets $300 million to $1 billion
• Level 3 entities (22 total)
  – Community hospitals, regional pharmacy/self-insured entities/clearinghouses
  – Revenue/assets $50 to $300 million
• Level 4 entities (36 total)
  – Small provider practices, community/rural pharmacies/clearinghouses
  – Revenue/assets < $50 million

OCR Phase 1 Findings/Observations
• None found for 11% of those audited
• Healthcare providers represented 53% of covered entities audited
• Healthcare providers accounted for 65% of findings/observations; smallest covered entities struggled with non-compliance for all HIPAA standards
• Findings by rule:
  – Privacy = 10%
  – Security = 60%
  – Breach = 10%

Meaningful Use (CMS)
Stage 1:
• Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process
Meaningful Use (CMS)
Stage 2 Core Measure:
• **Conduct or review a security risk analysis** in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data stored in CEHRT in accordance with requirements under 45 CFR 164.312(a)(2)(iv) and 45 CFR 164.306(d)(3), and **implement security updates as necessary and correct identified deficiencies** as part of the provider’s risk management process for EPs/EHs.

Meaningful Use (CMS)
Findings/Observations
• No analysis publicized
• Figliozzi and Company does Medicare audits
• State Medicaid agencies do Medicaid audits

REACH Experience
Who
• Small/medium hospitals and providers
Findings
• No/incomplete security risk analysis
• No/incomplete mitigation plan
• No/incomplete policies and procedures
Attested for Meaningful Use
**Barriers**

- Complexity of HIPAA
- Privacy and Security roles and responsibilities are added on to current job duties
- Lack of staff time and resources
- Understanding meaningful use requirements to complete the Security Risk Assessment with each attestation period

**Objectives**

- Overview of HIPAA
- Impact of HITECH
- Meaningful Use (CMS) versus Office of Civil Rights Audits
- Future of HIPAA, Meaningful Use and Audits

**OCR Phase 2**

- Selection of Audit Recipients
  - Covered Entities
  - Business Associates
  - Random selection of 550-800 recipients through National Provider Identifier database and America’s Health Insurance Plans’ database
  - Mandatory pre-audit screening survey will be sent
  - Selection of 350 covered entities; data requests will be sent; covered entities to provide list of business associates and OCR will select from the list
  - 232 healthcare providers
  - 109 health plans
  - 9 healthcare clearinghouses
OCR Phase 2

Audit Process
- 100 covered entities/50 business associates—compliance with security standards
- 100 covered entities—compliance with privacy standards
- 100 covered entities—compliance with breach notification standards
- Two weeks to respond to requests—failure could lead to a referral to applicable OCR Regional office
- Desk reviews—not on-site audit
- Covered entity targets: Risk analysis/risk management; content and timeliness of breach notification; Notice of Privacy Practices; individual access; privacy standards' reasonable safeguard requirement; training; device and media controls; and, transmission security
- Business associate targets: Risk analysis/risk management and breach reporting to covered entities
- Draft audit report will be presented for comment from management—OCR will review comments and issue final report

How to Prepare
- Complete a comprehensive Security Risk Analysis/review a previous analysis
- Have a mitigation plan
- Have a complete list of Business Associates
- Have an updated/compliant Notice of Privacy Practices, not only a website notice
- Have reasonable and appropriate safeguards in place for paper, verbal and electronic PHI
- Train workforce
- Have an inventory of information system assets, including mobile devices

Resources
- OCR Audit Protocol
- McDermott Will Emery OCR Phase 2 HIPAA Audit Program
- Redspin HIPAA Resources
- IDTC 2015 Breach Report
- Redspin 2014 Breach Report
- HIMSS 2015 Handouts
- www.khareach.org
- www.hipacow.org
Security Risk Analysis Resources

- NIST
- OCR Security Rule Final Guidance
- HealthIT.gov Security Risk Assessment
- EHR Incentive Program Security Risk Assessment Fact Sheet
- http://www.hipaaone.com/

Contact Information

Patti Kritzberger, RHIT, CHPS
HIT/Quality Specialist
pkritzberger@qualityhealthnd.org
701-500-7216