IT SECURITY, HIPAA PRIVACY AND DISASTER RECOVERY
The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Presented By:

Lori Laubach, CPA
Partner

Kevin Villanueva, CISM, CISA, CISSP, MCP, PCI QSA
Senior Manager
Objectives

- Review the HIPAA Privacy Rule changes under HITECH
- Consider how to update privacy practices
- Review methods to meet the security requirement under HIPAA
- Understand threats and attacks in health care IT security
- Examine how organizations are changing their approaches to IT security
- Disaster Recovery plan

LTC IT Industry Trends
Systems for Residents

- Kiosks
- Point of sale
- Dining
- Facilities
- Resident billing
- Clinical and EMR
- Tablets/BYOD
- Internet access
- Safety
- Health and wellness
- Social interaction

Resident Care

- Wireless point of care systems
- Personal health records
- Remote monitoring
- Fall detectors
- First alert responders
- Motion sensors in living space
- Telehealth monitoring
- Caregiver network accessibility
- Videoconferencing
- Cognitive fitness
Administration

• Medical billing system
• Wireless connectivity
• Remote connectivity
• HIPAA policies and procedures
• Centralized data repositories
• Multifunction copiers/scanners/printers
• Badge systems
• Screen protection filters

Emerging Trends

• Software as a Service (SaaS)
• Tablets
• Mobility
• BYOD
• Big Data
• Security and privacy
• Green technology/Sustainability
• Data, information, and knowledge management
• Changes to the HIPAA compliance obligations comprise four rules wrapped into one:
  – Modifications to HIPAA privacy, security, and enforcement rules mandated by HITECH Act.
  – Increased and tiered civil money penalty structure
  – A final rule on breach notification for unsecured PHI
  – GINA requirements
Key Provisions

• Expanded definition of “business associate”
• Direct compliance obligations and liability of business associates.
• Modified definition of “marketing”
• Prohibition on sale of PHI without authorization
• Clear and conspicuous fundraising opt-outs
• Right to electronic copy of PHI
• Right to restrict disclosures to health plans

Key provisions (continued)

• GINA changes for some health plans
• Provision for compound authorizations for research
• Required changes to Notice of Privacy Practices (NPP)
• Broader disclosure of decedents’ PHI
• Disclosure of proof of immunizations to schools
• Tiered and enhanced enforcement provisions
The Final Rule

Business Associates
- Direct Liability
- Subcontractors
- Transitional Relief

Notice of Privacy Practice
- Required Notice Items
- Distribution of New Notice

Examples of How the Rule Works
Authorization is not required when PHI is provided for:

- Treatment:
  - Nursing home charge nurse provides PHI to triage nurse at the Emergency Department
  - OR

- Required by Law:
  - Notification of SSI recipient admission to SNF
The Final Rule (cont.)

Breach Notification and Reporting

- Breach Determination
- Notification Requirements for Business Associates
- Notification to Affected Individual and the Media
- Notification to the Secretary

Individual Access to PHI

- Providing PHI directly to a third party
- Distribution of PHI via e-mail
- Timing requirement

Imposition of Fees

- HHS clarified that labor costs can include compiling, extracting, scanning, and burning PHI to media, skilled technical staff time spent to create and copy the electronic file, and distributing the media.
Protected Health Information

- Deceased individuals
- Genetic information
- Proof of immunizations

Restriction on Disclosure of PHI

- HHS has clarified under the final rule that this requirement applies only to covered entities that are covered health care providers

Disclosure Restrictions

- Healthcare provider’s responsibility:
  - Assist when needed
  - Encouraged to alert:
    - All care team members
    - Pharmacy
- Patient’s responsibility
  - The patient is ultimately responsible for:
    - Requesting additional disclosures restriction
    - Clinician of other practices, OT/PT
    - Pharmacy
Examples of How the Rule Works

Restrict Disclosure of PHI to Health Plans and/or healthcare provider(s)

- Diabetic Patient had a Benign Lesion removed
- Consultations
  - Alternative treatment(s)
    - Malignancy
    - Osteoporosis

Final Rule (continued)

Marketing

- Face-to-face communications;
- Promotional gifts of nominal value;
- Communications promoting health in general and not promoting a product or service from a particular provider;
- Communications about government and government-sponsored programs; and
- Communications about a drug or biologic currently being prescribed and drug refill reminders.
Examples of How the Rule Works

Authorization is required when PHI is provided for:

- Marketing
  - Assisted Living Facility requests a list of discharged residents from local SNF.
  - DME Vendor requests a list of discharge residents with electric wheelchairs and/or scooters.

The Final Rule (continued)

Sale of PHI

- Exceptions to required authorization
- Future disclosure of remuneration
### Increased Civil Penalties

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Penalty for Each Violation</th>
<th>Penalty for All Violations of the Identical HIPAA Provision Occurring With the Same Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know and by Exercising Reasonable Diligence, Would Not Have Known of the HIPAA Violation</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to Willful Neglect but Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Due to Willful Neglect and is Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

### Estimated Total Implementation Cost

- 1st year - $114 million to $225.4 million
- Each year thereafter approximately $14.5 million

It is predicted that the true compliance costs for both covered entities and business associates will be far in excess of these HHS estimates.
Mitigate Your Risk

Prepare now by tightening up your rule-required oversight areas before September 23, 2013:

• Update Policies and Procedures
• Privacy Notice
  o Patient’s new right to “restrict certain disclosures of PHI”
  o Electronic copy of medical record
  o Response time
• E-mailed Records
  o Encryption requirement

Mitigate Your Risk

• Know The New Breach Definition
  o Proof of Harm Not Required
• Liability Insurance
  o Verify Coverage in Current Plan
• Insulate Business Associate Agreements
  o Keep a List
  o Keep a Safe Distance
  o Prepare for Pushback
HIPAA Security

HIPAA Security Rule

- Legislation designed to protect the confidentiality, integrity, and availability of ePHI
- Comprised of three main categories of “standards” pertaining to the administrative, physical, and technical aspects of ePHI
- Applies to the security and integrity of electronically created, stored, transmitted, received, or manipulated personal health information
HIPAA Omnibus Rule – Highlights

- Omnibus Rule released January 17, 2013 increased privacy and security provisions
- Effective date of March 26, 2013 with compliance for both Covered Entities and Business Associates required by September 23, 2013
- Expansion of Privacy and Security Rules for Business Associates
- Increase in penalties for non-compliance
- New standard for determining whether a PHI breach requires notification

Data Breaches - By The Numbers

- **538** breaches of protected health information (PHI)
- **21,408,505** patient health records affected
- **21.5%** increase in # of large breaches in 2012 over 2011 *but... a 77% decrease in # of patient records impacted*
- **67%** of all breaches have been the result of theft or loss
- **57%** of all patient records breached involved a business associate
- Historically, breaches at business associates have impacted **5 times** as many patient records as those at a covered entity
By the Numbers (continued)

- 38% of incidents were as a result of an unencrypted laptop or other portable electronic device
- 63.9% percent of total records breached in 2012 resulted from the 5 largest incidents
- 780,000: number of records breached in the single largest incident of 2012

Biggest Breaches for 2012

- Utah Department of Health - 780,000 records
- Emory Healthcare - 315,000 records
- S.C. Dept. of Health and Human Services - 228,435 records
- Alere Home Monitoring, Inc. - 116,506 records
- Memorial Healthcare System, Fla. - 102,153 records
- Howard University Hospital - 66,601 records
- Apria Healthcare - 65,700 records
- University of Miami - 64,846 records
- Safe Ride Services - 42,000 records
- Medical Integration Services, Puerto Rico - 36,609 records
Breaches Affecting LTC

- December 2012 - Data breach affects 14,000 Medi-Cal providers
- May 2012 – Personal IHSS data missing, affecting 700,000 individuals who provide or receive home care under California’s In-Home Supportive Services

Security Risks

- Going Mobile
  - In 2011 39% of breaches occurred on laptop or other portable device.
  - In 2012 that number was 37.7%
  - BYOD is biggest concern

<table>
<thead>
<tr>
<th>Device Type</th>
<th>2009-2011</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop and other portable device</td>
<td>151</td>
<td>55</td>
</tr>
<tr>
<td>Paper</td>
<td>82</td>
<td>31</td>
</tr>
<tr>
<td>Computer</td>
<td>56</td>
<td>20</td>
</tr>
<tr>
<td>Server</td>
<td>38</td>
<td>15</td>
</tr>
<tr>
<td>Other</td>
<td>18</td>
<td>18</td>
</tr>
<tr>
<td>Email</td>
<td>7</td>
<td>4</td>
</tr>
<tr>
<td>Electronic Health Record</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>X-Ray</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>Backup Tapes</td>
<td>4</td>
<td>1</td>
</tr>
<tr>
<td>Hard Drives</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Mail, Postcards</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>CD / DVD</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>385</strong></td>
<td><strong>146</strong></td>
</tr>
</tbody>
</table>
Security Risks

- Unauthorized Access ePHI
  - 3rd largest breach in 2012 due to employee e-mailing himself 228,000 patient records
  - Identify who has access to what?

- Hackers or Employees
  - Most breaches occur due to our employees, whether malicious or not, not hackers

- Physical Access
  - Where is data stored? Servers, workstations, laptops, smartphones, backup tapes
  - Who has physical access to these storage locations?

- Workstation Left Unattended
  - Is workstation in a public area?
  - Are there controls to lock the workstation after a certain amount of inactivity?

- Mobile Computing and BYOD
  - Adds a whole new level of complexity to protecting ePHI
  - Are smart phones and tablets considered workstations under HIPAA?
Security Risks

• Business Associates (BA)
  – Partners who have access to your ePHI
  – How many records and what types of ePHI does each BA have access to?

• BA HIPAA Compliance
  – Are all of your BAs compliant?
  – How do you perform your due diligence?

• Omnibus Rule Impact
  – Extends compliance requirement further downstream
  – Chain of assurances is needed

Protect Yourself

• Conduct a HIPAA Security Risk Analysis
• Perform regular vulnerability scanning and remediation
• Encrypt data on ALL devices
• Perform due diligence on business associates
• Perform regular security awareness training for all employees and vendors
• Require an SSAE 16 or similar assessment of security controls of cloud computing service providers
Security Rule Recommendations

• Identify and be cognizant of how ePHI is being used
• Apply a risk-based approach toward protecting ePHI and conduct a risk assessment
• Follow a best practice standard for information security
• Review and revise contracts/agreements with BAs
• Put monitoring controls in place to identify and respond to security breaches
• If taking the BYOD plunge, use a combination of MDM, MAM, policy, and training

(Note: See NIST Special Publication 800-66 for guidance, including a framework for managing risk.)

Disaster Recovery: How Do You Get Started?

• Identify critical data
• Conduct a Business Impact Analysis (BIA)
• Document your data backup and recovery process
• Determine resources needed during a recovery effort
• Identify alternate processing facilities
Business Impact Analysis (BIA)

- **Purpose**: To help organizations identify the business units, operations and processes essential to the survival of the business.
- **Considerations**:
  - Life or death situation
  - Potential for significant loss of revenue
  - Obligations to external parties may be jeopardized
- **RTO** – Recovery time objective
- **RPO** – Recovery point objective
- **Critical**: for determining the order and priority of system recovery

Disaster Recovery Plan Structure

- **Assumptions** (communications infrastructure in place, primary location still available, primary IT staff available)
- **Roles and Responsibilities**
- **Declaration of a Disaster**
- **Equipment Salvage** (procurement)
- **System Recovery Process** (alternate site)
- **Resumption at Primary Site**
- **Declare End of Disaster** (debrief)
Disaster Recovery Testing

1. Table top test
2. Structured walk-through
3. Parallel simulation
4. Live production simulation

- Test on an annual basis
- Keep your plan current

Closing

- Review the HIPAA Privacy Rule changes under HITECH
- Consider how to improve a resident’s privacy practices
- Review methods to meet the security requirement under HIPAA
- Understand threats and attacks in health care IT security
- Examine how organizations are changing their approaches to IT security, especially those who are “in the cloud”
- Review how to monitor and manage compliance with cloud computing best practices
- Disaster recovery plan development is a multi-step process
Questions

Lori Laubach, CPA
Partner
(253) 284-5256
lori.laubach@mossadams.com

Kevin Villanueva, CISM, CISA, CISSP, PCI QSA
Senior Manager
(206) 302-6542
kevin.villanueva@mossadams.com