Cyber Risk Management in Healthcare

Presented to: San Antonio TMGMA

February 17, 2016
The information and opinions in this course and the supplemental materials should not be used or referred to as primary legal sources. The information presented should be used as a resource, selected and adapted with the advice of your attorney. It is distributed with the understanding Cathy Bryant, Texas Medical Liability Trust, nor Texas Medical Insurance Company is engaged in rendering legal services.
Upon completion of this program, participants should be able to:

• Recognize that data breach vulnerabilities in healthcare are numerous.
• Identify what healthcare providers should do to mitigate their cyber risks
• Understand the importance of appropriate risk transfer.
THE YEAR OF THE HEALTH CARE BREACH

- 264 breaches involving >500 patient health records
- 113,208,516 patient records breached (73% of all records breached since 2009)
- 897% increase in the number of records breached 2015 vs. 2014
- 98% of the breaches were due to hacking attacks/IT incidents
- 20% of all breaches involved a business associate
- 26% of the large breaches involved paper or x-ray films
HIPAA Circa 2003

What I See

Here – What I Hear

Here – Let it

Be Here When I leave

Here!
Cyber criminals are going to find way to blow a hole in your defenses
Pathway to compliance and risk management

- Organizations are at a crossroads, deciding which path to take for compliance with HIPAA and cybersecurity
- Your decision will be the foundation of the organization’s culture on medical privacy and security
- Being well informed, making good choices can help provide peace of mind
Technology & devices have great benefits have brought us opportunities --- but their use also exposes us to significant risk.
Cyber Risk Management Process

Risk Identification

Risk Assessment

Risk Management & Administration

Risk Transfer
RISK IDENTIFICATION
Where do you create, maintain, transmit or store PHI/ePHI?
Cyber Risk Management Process

Risk Identification

Risk Assessment

Risk Management & Administration

Risk Transfer

RISK MANAGEMENT PROCESS
Do we have an effective enterprise risk management process in place and are cyber risks fully integrated into the process?
### Healthcare Organizations’ Perceptions About Privacy and Data Protections

<table>
<thead>
<tr>
<th>Perception</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies and procedures effectively prevent or quickly detect unauthorized patient data access, loss or theft</td>
<td>58%</td>
</tr>
<tr>
<td>Personnel has technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data</td>
<td>53%</td>
</tr>
<tr>
<td>Technologies effectively prevent or quickly detect unauthorized patient data access, loss or theft</td>
<td>49%</td>
</tr>
<tr>
<td>Resources prevent or quickly detect unauthorized patient data access, loss or theft</td>
<td>33%</td>
</tr>
</tbody>
</table>

Ponemon Institute 2015
Top Security Technologies Ranked by IT Security Staff

Ponemon Institute: 2015 Global Study on IT Security Spending and Investments
Office was burglarized October, 2013
OCR compliant was filed (October 30, 2013) stating the practice failed to notify patients of the “breach”
  • Physician initially OCR’s compliant investigation letter (November 20, 2013)
  • OCR found the response incomplete and requested additional information/documents

October 29, 2015 the OCR conducted a site visit at the office

Conclusion:
  • After two years under investigation, the office will not be subject to fines or penalties.
  • The investigator was positive about the progress made by the practice to come into compliance, despite the fact they did not have records of compliance for six years
  • A plan of correction for remaining issues will be required
All cyber liability policies have a reporting requirement
• claims must be reported within 60 days of knowledge of the claim
Failure to report in a timely manner can result in a coverage
“HHS is serious about enforcing individual rights guaranteed by the HIPAA Privacy Rule and ensuring provider cooperation with our enforcement efforts”
What to do if you get a letter from the OCR

Random HIPAA Audit
- Call TMLT Product Development & Consulting for a free Mini Assessment

Complaint Investigation
- Call TMLT Claims
- Report the incident within 60 days!

Breach Investigation
- Call TMLT Claims
- Report the incident within 60 days!
- NAS’ claims team will assist
Appoint a Privacy Officer
Appoint a Security Officer
Add the duties to the job description
Make sure they have knowledge necessary to do the job
The first Implementation Specification of the Security Rule requires covered entities and business associates to conduct a security risk analysis.

Meaningful Use requires participants to attest that have conducted or reviewed a SRA annually.

“The one unforgiveable in the eyes of the OCR is failure to conduct a risk assessment”
Common Issues We Find with Clients

MISSING OR OBSOLETE
P&P and Documents
- PRIVACY
- SECURITY
- BREACH NOTIFICATION

HIPAA Policies & Procedure
Common Issues We Find with Clients

Texting PHI via SMS

Know who your Business Associates are and have current agreements to protect you!
NETWORK ISSUES

- Hardware out of date (antiquated networks)
- Weak, unchanged passwords
- Unsecure wireless networks
- Software not updated, unpatched for known vulnerabilities
- Unsecure Communications
- Unencrypted mobile devices
December 2015 Settlement agreement with University of Washington Medicine

- November 2013—ePHI of 90,000 individuals was accessed after an employee downloaded an email with malicious malware
- $750,000 settlement, corrective action plan and annual reports of compliance efforts
- Organization’s security policies required its affiliated entities to have up-to-date, documented system-level risk assessments and to implement safeguards in compliance with the Security Rule.

“All too often we see covered entities with a limited risk analysis that focuses on a specific system such as the electronic medical record or that fails to provide appropriate oversight and accountability for all parts of the enterprise,” said OCR Director Jocelyn Samuels. “An effective risk analysis is one that is comprehensive in scope and is conducted across the organization to sufficiently address the risks and vulnerabilities to patient data.”
November 30, 2015

- Puerto Rico insurance holding company
- $3.5 million and a robust corrective action plan
- OCR Director Jocelyn Samuels.

“This case sends an important message for HIPAA Covered Entities not only about compliance with the requirements of the Security Rule, including risk analysis, but compliance with the requirements of the Privacy Rule, including those addressing business associate agreements and the minimum necessary use of protected health information.”
**TMLT’s Comprehensive Risk Assessment**

**HIPAA PRIVACY RULE**
“To protect an individual’s health information in all formats, verbal, written, or electronic”

**HIPAA SECURITY RULE**
“To protect the confidentiality, integrity, and availability of electronic protected health information”

**BREACH NOTIFICATION**
“A breach is an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of protected health information”

**THE TEXAS MEDICAL PRIVACY ACT & THE TEXAS IDENTITY THEFT, ENFORCEMENT, AND PROTECTION ACT**

**TMLT MEDICAL PRIVACY, SECURITY & BREACH NOTIFICATION RISK ASSESSMENT**
The second Implementation Specification of the Security Rule requires covered entities and business associates to develop a risk management plan.
HHS/OCR SETTLEMENT AGREEMENT: November 25, 2015

- Burlington, Massachusetts--Theft of an unencrypted laptop from an unlocked treatment area on August 11, 2011
- $850,000
- Facility **address its history of noncompliance** with the HIPAA Rules by **providing OCR with a comprehensive, enterprise-wide risk analysis and corresponding risk management plan**
- Encryption is an “Addressable” – HIPAA does not require encryption per se
- Addressable does not mean optional
- OCR underscores unencrypted portable devices pose a significant risk to PHI
- Encryption is now considered a basic risk management tool in data security and there is an expectation that organizations use this tool
The Problem with Unencrypted Devices

August 2015 OCR Settlement with Cancer Care Group

- Laptop and backup media (unencrypted) was stolen from employee’s vehicle.
- Cancer Care was “in widespread non-compliance with the HIPAA Security Rule.”
- Had not conducted an enterprise wide risk analysis.
- Did not have written P&P specific to removal of hardware and electronic media.
- Did not encrypt.

An exclusion endorsement may be added due to the failure to encrypt data on mobile devices, if disclosed in the Cyber Insurance Application.

$750,000
Written Policies & Procedures

HIPAA
Policies & Procedures
Beware of P&P templates

December 2014 Anchorage Community Mental Health Services OCR Settlement Agreement

- 2012 ePHI was compromised due to malware compromising the security of its IT services
- $150,000 fine and adopt a plan of correction
- Organization had adopted sample P&P in 2005 but never followed them
- The breach was a direct result of failing to identify and address basic risks
Employee education is paramount
“See Something – Say Something”

- Texas – new employees must be trained within 90 days of employment
- Federal – as soon as possible
Jocelyn Samuels: “It is critical that entities take a comprehensive and thorough approach to assessing and addressing the risk to all of the protected health information they maintain.”

“have comprehensive policies and procedures for compliance with the HIPAA Rules, but also the P & P must be clearly communicated to and implemented by all workforce members”
As the forms of connected technology used by healthcare providers increases—so will their cybersecurity risks.

Therefore, providers will need assistance in mitigating the proliferation and diversity of their cyber risks, including help with their:

- IT Systems;
- Privacy, Security, & Breach Risk Assessments;
- Staff Privacy Training; and
- Risk Transfer (cyber insurance).
DATA BREACHES…

A MAJOR SOURCE OF MEDICAL IDENTITY THEFT
“Your Medical Records Could Be Sold on Black Market”

HEALTHCARE BREACH CAN COST $363 PER RECORD

- COST OF NOTIFYING PATIENTS
- CREDIT MONITORING
- CALL CENTER
- FORENSICS
- LEGAL FEES
- PUBLIC RELATIONS/CRISIS RESPONSE

5th Annual Benchmark Study on Patient Privacy and Data Security – The Ponemon Institute
Impact of Data Breaches on Physicians & their Practices

- Loss of revenues/loss of business
- Loss of patient goodwill
- Damage to reputation
- Time and productivity loss
- Cost of outside consultants/lawyers
- Remediation expenses/technology & training
- Government fines and penalties
- Lawsuits
- Poor employee morale

Each staff member has a responsibility for their actions
Cyber Risk Management Process

- Risk Identification
- Risk Assessment
- Risk Management & Administration
- Risk Transfer

RISK MANAGEMENT PROCESS
Cyber Liability Coverage

Are you covered? Are you sure?

1. Privacy Breach Response
2. Privacy and Security Liability Coverage
3. Regulatory Defense and Penalty Coverage
4. Network Asset Protection Coverage
5. Multimedia Liability Coverage
6. Cyber Extortion Coverage
7. Cyber Terrorism Coverage
8. Technology Services Errors & Omissions Coverage
Cyber Risk Management and Risk Transfer
1. Do a comprehensive risk assessment
2. Develop a risk management plan
3. Have policies and procedures that reflect your practices
4. Make sure your staff is educated
5. Ask for help, when needed
Cathy Bryant

[cathy-bryant@tmlt.org](mailto:cathy-bryant@tmlt.org)

512-425-5910