Pitfalls and Benefits of Telehealth and Cybersecurity in the Digital Age

IHA Legal Forum for Hospital Executives and Counsel
September 16, 2016

What We Will Cover:

• Cybersecurity in Healthcare
  – Cybersecurity risks and tools
  – HIPAA enforcement
  – Mitigating risk

• Telehealth
  – Why we are doing it
  – What’s involved
  – Legal considerations
Cybersecurity in Healthcare

• What is cybersecurity?
  – Protection of systems that use the Internet and computers

• Why is cybersecurity so important in health care?
  – Dependent on electronic equipment and communications
  – Vast amount of ePHI

• Why is health care a cybersecurity target?
  – Critical infrastructure
  – Valuable information
  – Soft target
Cybersecurity in Healthcare

• Cyber-criminal motives
  – Monetization
  – Espionage
  – Hacktivism

• Types of attacks
  – Social engineering
  – Phishing
  – Ransomware
  – Persistent attacks

Cybersecurity in Healthcare

• Areas of risk
  – EMR
  – Mobile devices
  – Medical devices
  – Web-based applications
Cybersecurity in Healthcare

- Cybersecurity tools
  - Firewalls
  - Authentication
  - Anti-virus software
  - Encryption
  - Updated software and patches
  - Training
Cybersecurity in Healthcare

• Current State
  – Health care continues to have the highest per capita breach costs:

  ![Graph showing cost per capita by industry classification](image)

  Source: Ponemon Institute 2015

• Current State
  – The more robust the data, the more it is targeted:

  ![Bar chart showing patient data targeted](image)

  Source: Ponemon Institute 2015
Cybersecurity in Healthcare

• Current State
  – Malicious/criminal attacks are top cause of data breaches:

  ![Pie chart showing distribution of data breach root causes](image)
  - Malicious or criminal attack: 47%
  - System glitch: 25%
  - Human error: 28%

  Source: Ponemon Institute 2015

• Current State
  – Impact of root cause on the cost of a breach:

  ![Bar chart showing per capita cost of breaches](image)
  - Malicious or criminal attack: $230
  - System glitch: $210
  - Human error: $198

  Source: Ponemon Institute 2015
Cybersecurity in Healthcare

• Current State
  – Factors that impact the cost of a breach:

| Factor                        | Cost Impact
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident response team</td>
<td>$12.6</td>
</tr>
<tr>
<td>Extensive use of encryption</td>
<td>$12.3</td>
</tr>
<tr>
<td>Employee training</td>
<td>$8.0</td>
</tr>
<tr>
<td>BCM involvement</td>
<td>$7.1</td>
</tr>
<tr>
<td>CISO appointed</td>
<td>$5.6</td>
</tr>
<tr>
<td>Board-level involvement</td>
<td>$5.5</td>
</tr>
<tr>
<td>Insurance protection</td>
<td>$4.4</td>
</tr>
<tr>
<td>Consultants engaged</td>
<td>$4.5</td>
</tr>
<tr>
<td>Rush to notify</td>
<td>$9.0</td>
</tr>
<tr>
<td>Lost or stolen devices</td>
<td>$9.0</td>
</tr>
<tr>
<td>Third party involvement</td>
<td>$16.0</td>
</tr>
</tbody>
</table>

Source: Ponemon Institute 2015

HIPAA

• Enforcement
  – Historical Performance:
    • As of today, $52M in OCR settlements and CMPs
      – 39 enforcement actions
      – $1.2M average settlement
      – Wide variety in terms of entity type, nature of alleged violation, number of individuals affected and geography
      – Two of last five settlements pertained to lack of business associate agreements.
      – New catchphrase: “Widespread noncompliance”
        » lack of risk analysis, remediation, policies and procedures, training, etc.
## Recent OCR HIPAA Actions

<table>
<thead>
<tr>
<th>Type of Entity</th>
<th>Amount</th>
<th>Individuals Affected</th>
<th>State</th>
<th>Year</th>
<th>Key Facts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health System</td>
<td>$5,500,000</td>
<td>4,000,000</td>
<td>IL</td>
<td>Aug 2016</td>
<td>• Failure to perform risk analysis for all ePHI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of facility access controls on data center</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of Business Associate Agreement</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to safeguard laptop</td>
</tr>
<tr>
<td>University Medical Center</td>
<td>$2,750,000</td>
<td>10,000</td>
<td>MS</td>
<td>July 2016</td>
<td>• Failure to manage and remediate risks and vulnerabilities to ePHI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to implement unique user access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to implement workstation physical safeguards</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to notify all affected individuals</td>
</tr>
<tr>
<td>University Medical Center</td>
<td>$2,700,000</td>
<td>3,000</td>
<td>OR</td>
<td>July 2016</td>
<td>• Risk analyses were not enterprise-wide</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to address identified risks and vulnerabilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of C-Suite involvement in HIPAA compliance</td>
</tr>
<tr>
<td>Business Associate</td>
<td>$650,000</td>
<td>412</td>
<td>MN</td>
<td>June 2016</td>
<td>• Theft of unencrypted iPhone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of mobile device policy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• No risk analysis or risk management plan</td>
</tr>
<tr>
<td>Hospital</td>
<td>$2,200,000</td>
<td>2+</td>
<td>NY</td>
<td>April 2016</td>
<td>• Disclosure of PHI to Media</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of patient authorizations</td>
</tr>
<tr>
<td>Physician Group</td>
<td>$750,000</td>
<td>17,300</td>
<td>NC</td>
<td>April 2016</td>
<td>• Lack of business associate agreement</td>
</tr>
<tr>
<td>Medical Research Institute</td>
<td>$3,900,000</td>
<td>13,000</td>
<td>NY</td>
<td>March 2016</td>
<td>• Stolen unencrypted laptop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of policies and procedures related to accessing ePHI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Inadequate security management process</td>
</tr>
<tr>
<td>Health System</td>
<td>$1,550,000</td>
<td>9,497</td>
<td>MN</td>
<td>March 2016</td>
<td>• Stolen unencrypted laptop</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to institute an organization-wide risk analysis</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Failure to have compliant business associate agreements</td>
</tr>
<tr>
<td>Physical Therapy Provider</td>
<td>$25,000</td>
<td>Numerous</td>
<td>CA</td>
<td>Feb 2016</td>
<td>• Posted PHI on website</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Lack of patient authorizations</td>
</tr>
<tr>
<td>Infusion and Equipment Provider</td>
<td>$239,800</td>
<td>278</td>
<td>FL</td>
<td>Feb 2016</td>
<td>• Failure to safeguard PHI</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• Employee left PHI in former resident</td>
</tr>
</tbody>
</table>
Recent OCR HIPAA Actions

<table>
<thead>
<tr>
<th>Type of Entity</th>
<th>Amount</th>
<th>Individuals Affected</th>
<th>State</th>
<th>Year</th>
<th>Key Facts</th>
</tr>
</thead>
</table>
| Teaching Hospital| $750,000   | 90,000               | WA    | Dec 2015 | • Malicious malware compromised IT system  
• Lack of organization-wide risk analysis |
| Insurance        | $3,500,000 | Exact number not provided | PR    | Nov 2015 | • Multiple reported breaches  
• Failure to implement comprehensive wide compliance program |
| Teaching Hospital| $850,000   | 599                  | MA    | Nov 2015 | • Stolen laptop  
• Widespread non-compliance  
• No thorough risk analysis  
• Lack of policies and procedures related to safeguarding workstations |
| Physician Group  | $750,000   | 55,000               | IN    | Sept 2015 | • Stolen unencrypted backup media  
• Lack of enterprise-wide risk analysis  
• Failure to implement a comprehensive wide device and media control policy |
| Hospital         | $218,200   | 498                  | MA    | July 2015 | • Lack of safeguards for internet applications |
| Pharmacy         | $125,000   | Numerous             | CO    | April 2015 | • Failure to securely dispose of paper medical records |

HIPAA

• Audits
  – Phase II Audits:
    • 167 covered entity desk audits have begun
      – Audited for either Privacy, Security or Breach Notification Rule compliance
        » Privacy: Access and notice of privacy practices  
        » Security: Risk analysis and risk management  
        » Breach: Content and timing of notice
    – Business Associates
      » 33 will be chosen from lists provided by covered entities
    – Revised audit protocol
HIPAA

• What to Do?

—HIPAA Privacy fundamentals:
  » Policies and Procedures
  » Training
  » Sanctions
  » Documentation

HIPAA

• What to do?

—HIPAA Security fundamentals:
  » Risk analysis
  » Policies and Procedures
  » Training
  » Sanctions
  » Documentation
HIPAA

• What to Do?

—HIPAA Breach Notification fundamentals:
  » Policies and Procedures
  » Training
  » Sanctions
  » Risk assessment
  » Documentation

—Document, Document, Document
  » Document all HIPAA compliance activities
  » HIPAA requires that documentation be maintained for 6 years
  » Better to over-document than to under-document
  » Consider when to utilize attorney-client privilege
HIPAA

- Entities can mitigate risk of violations and penalties by:
  - Good faith effort at HIPAA compliance
    - Risk analysis
    - Policies and procedures
    - Training
    - Audits
  - Meaningful response to breach
    - Don’t give an affected individual a reason to sue you
  - Meaningful discipline
    - Don’t give a jury a reason to doubt your commitment to privacy

Telehealth – Why are we doing it?

Boldly going where no one has gone before...

or keeping up with the Joneses.
Telehealth – What is involved

- Understanding the deal
  - IT solution
  - Clinical Services
  - Billing arrangement
  - Allocating the risk
  - Mission alignment

Telehealth - Patient Flow
Telehealth- Documents

The documents:

• IT Services/license agreement
  – Vendor Terms of Use
  – Vendor Privacy Policy
  – Vendor click through

• Clinical Services Agreement
  – Notice of Privacy Practices
  – Consent to treatment
  – HIPAA Notice

• Third party Payor Agreement
• Joint Marketing Agreement

• Medical Staff By-Laws
• Delegated Credentialing Agreement
• Medical Malpractice policies
• Hospital website
  – Terms of Use
  – Privacy Policy
  – Consent to Treatment
  – HIPAA Notice
• Advanced Beneficiary Notice

Telehealth – Legal considerations

• Stark (Where are the financial relationships? Do we have an exception?)
• Anti-Kickback (Watch for technology fee structures which could be viewed as incentivizing referrals in a particular direction)
• Medicare Claims Processing Manual (know your MAC, their guidance varies)
• HIPAA (who is responsible for obtaining consent, what is the scope of use of PHI, when will it be shared, and are consents to use PHI valid)
• Medical Staff Credentialing and Privileging (only applies to hospital based services)
• Third Party Payor Agreement
• Licensure (certification needed for out of state providers)
• Malpractice Insurance (Are you covered?)
Telehealth - Ind. Code 25-1-9.5-6

Ind. Code 25-1-9.5-6 "telemedicine" means the delivery of health care services via:
(1) secure videoconferencing; (2) interactive audio-using store and forward technology; or
(3) remote patient monitoring technology; between a provider in one (1) location and a patient in
another location.

Telemedicine does not include health care services provided via:
(1) Audio-only communication; (2) A telephone call; (3) Electronic mail; (4) An instant messaging
conversation; (5) Facsimile; (6) Internet questionnaire; (7) Telephone consultation; and (8)
Internet consultation.

Telehealth – Indiana Standard of Care

The provider-patient relationship:
1. Obtain the patients name and contact information
2. Disclose the provider’s name, and type of provider (physician, PA APN)
3. Obtain informed consent
4. Obtain patient’s medical history and other information necessary for
diagnosis
5. Discuss diagnosis, evidence of diagnosis, and risks and benefits of
treatment options
6. Create and maintain record of treatment, notify primary care provider of
any prescriptions
7. Provide follow-up care instructions
8. Provide visit summary to patient including prescription.
Telehealth – Indiana Prescription Authority

IC 25-2-9.5-8 Permits Physicians, PAs and APNs to prescribe non-controlled legend drugs via telemedicine provided:

- provider-patient relationship is established and
- prescription is issues with the same standard of care as in-person services.

— Overrides prior law prohibiting physicians from prescribing without having “personally physically examined and diagnosed”.


Please visit the Hall Render Blog at http://blogs.hallrender.com for more information on topics related to health care law.

Michael T. Batt | (317) 977-1417 | mbatt@hallrender.com
Elizabeth Callahan-Morris | (248) 457-7854 | ecallahan@hallrender.com

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.