Evolution of Cyber Security in Healthcare

Spencer L SooHoo, PhD
Director, Scientific Computing & Chief Security Officer
Enterprise Information Services
Healthcare and Security

How we got here
- Healthcare ecosystem
- Different business models
- Example of one model to demonstrate differing requirements
- Regulatory Environment
  - HIPAA

Where we’re at

Paradigm Shift

Where we’re going
Background – Healthcare Ecosystem

- **Patients** (consumers)
- **Insurance** - Private, Public
- **Government**
- **Medical**
  - Tech & Pharma
- **Regulatory Agencies**
  - PHI (Billing, A/P, coding, etc.)
- **Healthcare Providers** (Hospitals/Health Systems)
  - Physicians, Nurses, etc.
  - Reimbursements
  - Medical devices, Rx
  - Business Associates
- **Regulatory Agencies**
- **Physician referrals**
- **Premiums**
- **Grants, other funding**

CEDARS-SINAI
Background—Models of Healthcare

Hospitals/Health Systems are distinguished by their Ownership

**proprietary (for-profit)** businesses, owned either by corporations or individuals such as the physicians on staff

**not-for-profit** corporations, religious organizations operated by federal, state, or city governments

Scope of services

- **Acute care** – community hospitals
- **Long-term care/rehab/behavioral health**
- **Teaching hospitals** -- academic affiliations
- **Tertiary hospitals** – specialized care

**Academic Medical Center** – Teaching and Tertiary care with research mission
Cedars-Sinai: Overview

- Not-for-profit academic medical center
- Established in 1902 and located in Los Angeles, California
- 866 licensed beds, Level 1 Trauma Center
- Primary service area includes 3.3 million people
- Focus on Healthcare Delivery, Education, and Research
  - 230 Emergency Patients, 1400 Outpatient visits per day
  - >600 medical students, >600 residents/fellows
  - ~1000 engaged in research, 1180 sponsored research projects/year
Is healthcare more heavily regulated than the nuclear power industry?

1996 HIPAA (Health Insurance Portability and Accountability Act) HIPAA is the 900 pound gorilla in terms of impact on cyber security

Pre-HIPAA – Healthcare gave little attention to cyber security

Immediately after HIPAA’s Security Rule was being enforced, cyber security efforts started getting traction at the C-suite level.
Regulatory Environment
1996 HIPAA (Health Insurance Portability and Accountability Act)

**Privacy Rule** -- Protected Health Information (PHI)---both paper and electronic
**Security Rule** -- Electronic Protected Health Information (E PHI)

- 3 types of safeguards: Administrative, Physical, Technical
- Required specifications must be adopted
- Addressable specifications are flexible—can evaluate and determine best way to implement
- Compliance date 2005 for most covered entities

Jan 2013—HIPAA updated via Final Omnibus Rule
- Includes changes in Security Rule and Breach Notification of the HITECH Act.
  - Expansion to cover business associates
  - Have to prove harm due to a breach did not occur.

**Self-Reporting Requirements**
- Notification to affected individuals within 60 days of discovery
- Any breach involving >500 individuals must be reported to HHS within 60 days of discovery
- California has a 15 business day reporting requirement
Paradigm Shift

- Up to 2010 -- we were worried about giving away our data
- After 2010 -- we are worried about someone taking away our data

From the Health and Human Services “Wall of Shame” (breaches involving > 500 Patients)
Healthcare Slow to Adapt to Security Challenges

- Transition from proprietary network/operating system to off-the-shelf approach—Some developers still have a “proprietary” mindset.
- Niche market players
- FDA Medical Device Regulations (now used more as a stalling tactic)
- Inertia – complex, heterogeneous environment → long time lag to patch/upgrade
- Diverse business models (difficult to control workforce, devices, access)
- Funding
- Culture -- Focus on patient care, ease of access to information
• Things that kept the CISO awake at night
  ○ Losing an unencrypted laptop or USB drive
  ○ Putting PHI into a cloud-based file sharing system
  ○ Loss of PHI involving >500 patients
  ○ Passing a HIPAA audit
Shift in Use of Technology

Traditional Uses
- ADT (Admission, Discharge, Transfer)
- Billing
- Payroll
- Office Automation
- Standalone systems for labs, images, pharmacy, etc.

EMR (Electronic Medical Record)
- Physician Ordering
- Scheduling
- Labs
- Medication
- Remote Access
- Patient Access
- Integration with other systems (labs, images...)

Device Integration
- Data flows directly into EMR
- Reduce errors
- Faster response
- Increased efficiency

Analytics
- Metrics allow more efficient and effective delivery of healthcare
EMR (Electronic Medical Record) rollout
• Deployed hundreds of workstations as part of the rollout.
• Mobile workstations on carts -- COWs(Computers on Wheels)
• Evolving shift in focus from workstations to mobile devices

Putting COWs out to pasture
Mobile device technology for better delivery of patient care

- Arrhythmia monitors
- Bedside monitors, telemetry
- ‘emergency’ pull cord, pillow speaker/mic
- Medical devices (via the aux port)
- I’m in pain

Alerts from Nurse Call system & bedside medical devices

Cardiac Monitoring Center
- 6 stations, up to 288 patients
- (all alerts require user intervention)

Nurses Station
- (some alerts require user intervention)

Critical Lab Results

CEDARS-SINAI
Increased use of technology for better patient safety

8. Review results in flow sheets and validate in EMR

7. Verify correct programming of pump

6. Scan channel

1. Scan the patient

2. Verify correct patient

3. Scan medication

4. Verify correct med, time, dose, route

5. Document medication

6-rights plus:
- Auto program the pump with order detail
- Auto download infusion volumes into EMR

CEDARS-SINAI
Modeling ion transport through a cell membrane

Research
- Funding from grants
- Keep ‘till it stops working
- Computers imbedded in instruments
- One-of-a-kind configurations
- Assets may move with a grant
- Decentralized workforce management

High Performance Computing Cluster

Clinical/Administrative
- Funding from operational budget
- Upgrade every few years
- Easy to identify computers
- Deploy standard image
- Assets remain at institution
- Centralized (mostly) workforce management

Genomics

Translational Research Informatics

Inflammatory Bowel Disease Research

MS PROGRAM

Skeletal Dysplasia

Cedars-Sinai
Where are the security challenges in healthcare?
Technical Vulnerabilities--How secure is the technology?

Harder to manage environment
- 10X more devices
- 3-5X more types of devices
- BYOD push for mobile devices

Security on application platforms and medical devices
- Lack anti-virus software
- Weak security controls
- Long lag in certifying patches
- Operating system upgrades can be a really big deal

2003-- Blaster RPC Worm
- Better patch management
- Better AV Deployment
- Internal Firewalls

2009-- Conficker
- Isolated networks
- Internal IPS/IDS
- Workstation Firewalls
- Workstation Images

2009-- Stolen laptop with PHI
- Encrypt all laptops/desktops

2011-- #1 Ranking on SPAMRANKING.NET
- Anti-Phishing Awareness
- Malware Detection
- Better monitoring
- Frequent Security Scans

2014-- Heartbleed
- Better Inventory
- Better Scanning

Technical Vulnerabilities

Harder to manage environment
- 10X more devices
- 3-5X more types of devices
- BYOD push for mobile devices

Security on application platforms and medical devices
- Lack anti-virus software
- Weak security controls
- Long lag in certifying patches
- Operating system upgrades can be a really big deal
<table>
<thead>
<tr>
<th>Rank</th>
<th>Concern</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Successful Phishing Attack</td>
</tr>
<tr>
<td>2</td>
<td>Curiosity $\rightarrow$ HIPAA violation</td>
</tr>
<tr>
<td>3</td>
<td>User access management (employees, staff MD, attending MD, volunteers, students, researchers)</td>
</tr>
<tr>
<td>4</td>
<td>Unencrypted PHI on USB drive, cloud storage or personally owned computer</td>
</tr>
<tr>
<td>5</td>
<td>What happens at home doesn’t stay at home</td>
</tr>
</tbody>
</table>
Business Associates

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Pre-implementation

- **External Party Risk Assessment**
  - EPRA filled out by external party and CSMC sponsor--becomes part of the HIPAA BAA (Business Associate Agreement)

- **Tech Review Worksheet**
  - Review to ensure the application/services comply with architectural standards

Post Implementation Risk: PHI sent to BA, or BA has direct access into network.
Evolution of Patient Access Portals

Information
- Parking Maps
- Physician lookup and referral
- Marketing/PR Questions, etc.

Financial Transactions
- Statements, bill pay

Personal Health Record
- Schedule visits
- Lookup labs
- Medical history
- Refill prescriptions
- Communicate with physician

Minimal Security (secure website)
- Depend on collections vendor for security
- Financial transaction grade security needed

Patients
Post 2010

Things that keep the CISO awake at night

- Everything from 2010
  - Losing an unencrypted laptop or USB drive
  - Putting PHI into a cloud-based file sharing system
  - Loss of PHI involving more than 500 patients
  - Passing a HIPAA audit

Plus

- Notice from a government agency that our systems have been compromised

- Finding indications that data is being stolen but not knowing how much or for how long.

- Actual or threatened Denial of Service attack
New Worries

Vulnerabilities in medical devices
• Infusion pumps
• Implantable devices
• X-ray machines, CT scanners, etc.

Mergers and Acquisitions
• Range in size from small hospital to a 2-3 physician practice
• Replace or remediate decision
• Culture
• Resources
• Many don’t have full-time IT staff, much less a dedicated security officer
New Worries

Migration to cloud-based services
• HIPAA BAA (Business Associate Agreements)
• Know where data is
• How to get data back
• Monitoring– need unified security view of on-site and off-site access to data
Unintended Consequences of Self-Reporting Requirement

Not all breaches are equal in terms of harm to patients.

Self-reporting requirements and penalties may discourage some from proactively looking for unreported breaches.

Most reported breaches are accidental

Encourage “blame-free” self-reporting for process improvement.

Hacking into an EMR to steal ePHI

Incidental potential exposure of ePHI

Harm to patient

Proactively looking for breaches vs External report or complaint about a breach
What More Can We Do?

Senior Leadership buy-in \(\rightarrow\) sufficient budget (make up for lost time)

Need **Dual focus---compliance and operations**

**Compliance**
- Encrypt everything
- Proactive monitoring for privacy breaches (snooping)
- Frequent HIPAA risk assessments
- Effective security awareness education—especially anti-phishing training

**Operations**
- SOC to monitor SEIM 24x7
- **Advanced malware analysis** to detect/stop APTs (Advanced Persistent Threats)
- Aggressive anti-virus and patching program
- Network Segmentation for legacy applications
- Frequent penetration tests
- Subscribe to threat-intelligence feeds
What More Can We Do?

- Pressure on medical device and application vendors to prioritize security
  - “FDA regulated” excuse is wearing thin
  - No excuse for a vendor’s application to require deprecated operating system or software
What More Can We Do?

What is the Single greatest threat to Cyber Security in Healthcare?

Our workforce

Effective workforce education

- Anti-phishing training
- Culture of security and privacy – Information Security and Privacy need to get the same focus as patient safety does

Harm Report

Report Date 9/11/2014

<table>
<thead>
<tr>
<th>Harm Event</th>
<th>Week Ending Date</th>
<th>8/9-8/15</th>
<th>8/16-8/22</th>
<th>8/23-8/29</th>
<th>8/30-9/5</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central Line-Associated Blood Stream Infections (CLA-BSI)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Ventilator-Associated Pneumonia (VAP)</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>MRSA Blood Stream Infections (MRSA-BSI)</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Preventable Pressure Ulcers</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Medication Errors Causing Harm</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Never Events excluding HAPUs</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Focus on Workforce

Curiosity & Poor Judgment

Human Error

While not as dramatic as an airplane crash, a major factor in most security breaches is human error.

Cyber Security has to be part of Patient Safety Initiatives
Spencer L. SooHoo
Spencer.SooHoo@cshs.org