Compliance Does Not Equal Security
March 1, 2016

Mac McMillan, Co-founder & CEO, CynergisTek, Inc.
Jay Adams, Director of Information Security, Tallahassee Memorial Healthcare

DISCLAIMER: The views and opinions expressed in this presentation are those of the author and do not necessarily represent official policy or position of HIMSS.
Conflict of Interest

Mac McMillan, FHIMSS, CISM
Jay Adams, CISSP, HCISPP
Have no real or apparent conflicts of interest to report.
Agenda

• Compliance ≠ Security
• Industry Examples
• Importance
• Questions & Answers
Learning Objectives

• Recognize why focusing on compliance will fall short of protecting information adequately.

• Develop sound security programs by building it on managing risk, protecting data, and detection, reaction and governance.

• Describe how breaches occur, using current examples, and why compliance alone will not stop them from occurring.

• Evaluate the types of security technologies that are emerging as critical to building a secure enterprise and supporting clinical innovation.

• Explain why people, and not just technology or controls, are key to successfully achieving security and how enhance their training.
A Summary of How Benefits Were Realized for the Value of Health IT

- Reliance of information increases satisfaction
- Knowing information is secure and having accurate info improves quality of treatment
- Going beyond security compliance requirements helps secure electronic data
- Secure data enhances patient engagement
- Proactive security reduces likelihood of a breach and helps reduce expenses
Compliance & Security
HIPAA Security Rule

• Security Standards for the Protection of Electronic Protected Health Information, found at 45 CFR Part 160 and Part 164, Subparts A and C. The Security Rule is designed to protect the privacy and security of certain health information.

• HIPAA was not intended to cover all forms of information or to be a complete standard for data protection.

• The Security Rule, as initially envisioned, only covered protected health information in electronic form, not on paper or transmitted verbally.

• The Security Rule initially conceived in 2001 did not envision cloud computing, the proliferation of mobile devices, BYOD, networkable medical devices, wearables and many other technology advancements seen since that time.
HIPAA Privacy Rule

• The Privacy Rule contains provisions requiring covered entities (CE) to adopt safeguards to protect PHI.
  – A CE must reasonably safeguard PHI from any intentional or unintentional use or disclosure, and
  – Must limit incidental uses or disclosures made pursuant to an a permitted use or disclosure.

• The Privacy Rule covers all forms of PHI, electronic, paper and voice.
## Sources of Hacking

<table>
<thead>
<tr>
<th>Source</th>
<th>Motivations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recreational</td>
<td>Used to be the primary motivation for many attackers</td>
</tr>
<tr>
<td></td>
<td>Still a motivator for those looking to prove themselves</td>
</tr>
<tr>
<td>Hacktivism</td>
<td>Want to call attention to their social or political causes</td>
</tr>
<tr>
<td></td>
<td>Often motivated by anti-establishment themes</td>
</tr>
<tr>
<td>Espionage</td>
<td>Sophisticated attacks against government, military, or industry targets</td>
</tr>
<tr>
<td></td>
<td>May be motivated by political or monetary gains</td>
</tr>
<tr>
<td></td>
<td>Goals may be theft of intellectual property or disruption of critical infrastructure</td>
</tr>
<tr>
<td>Cybercrime</td>
<td>Cybercriminals have built a huge black market for developing malware, conducting internet-scale operations, and laundering money</td>
</tr>
<tr>
<td></td>
<td>Stolen data can be used by criminals for identity theft and financial fraud</td>
</tr>
<tr>
<td></td>
<td>Extortion by attacking availability of assets or sensitive nature of data</td>
</tr>
</tbody>
</table>
Accidents, Mistakes & Deliberate Acts

• Neurologic institute *accidentally emails* 10,000 patient records to 200 patients
• Phishing/hacking *nets nearly $3M* from six healthcare entities
• 2200 physicians victims of *ID theft/tax fraud*
• *Stolen laptop* from nurse’s home with patient data
• *Printers* returned to leasing company compromise thousands of patient records
• 400 hospitals billings delayed as clearinghouse hit with *ransomware*
• *Failure to apply fix* to router results in compromise and loss of 4.5M records
• Mistake during *software upgrade test* results in 8000 letters mailed
• Physician held up at gunpoint, *turns over passwords* for computer and phone
• International hacking group uses *phishing* then *hacking* to steal information on 80M people
• Three hospital networks compromised by *medical device hack* called MedJack
• New York hospital *hacked by Pro-ISIS* supporters, website defaced redirected to ISIS propaganda
• *Hacking* of UCLA Medical nets 4.5 Million records, goes undetected for over 9 months.
• Two separate *hacks of third party vendors* compromises 26 Million background investigations of government workers.
• And, on and on it goes…

Attribution provided to various breach citations as identified by the U.S. Department of Health and Human Services
Closing The Gap

Security is the ceiling.

Leadership are the walls that bring security and compliance together.

Compliance is the floor.
Compliance ≠ Security

- Compliance and security are two different paradigms
- Certification is not a “magic” pill
- Compliance is a “floor” rating
- Compliance is point in time
- Manual processes are too slow
- Controls are not enough
- Treat compliance as a risk
# Cybersecurity Risk

<table>
<thead>
<tr>
<th>Category</th>
<th>Subcategory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategic</td>
<td>• Goals of the Organization</td>
</tr>
<tr>
<td>Operational</td>
<td>• Processes that Achieve Goals</td>
</tr>
<tr>
<td>Financial</td>
<td>• Safeguarding Assets</td>
</tr>
<tr>
<td>Compliance</td>
<td>• Laws and Regulations</td>
</tr>
<tr>
<td>Reputational</td>
<td>• Public Image</td>
</tr>
</tbody>
</table>
Industry Examples
Risk Management

• Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to PHI in the enterprise
• Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the Security Rule
• Conduct or review a risk assessment of the CEHRT as part of annual attestation at least once during the reporting period.

• Accurate and up-to-date inventory of applications that process PHI, including data storage locations this is critical.
• Rate of change in healthcare placing strain on internal security resources
• Relationships with outside experts to help with following
  – Risk assessments
  – Management of security tools
• Complexity of environment
• Internal and external vulnerability scanning followed by a repeatable patch management process
Information System Activity Review

- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
- Regularly is not defined
- Audit logs assume all systems processing PHI, but does not specify which logs
- No retention period for logs defined
- Matrix defining which systems have sensitive information
- Manual log review processes are too slow; millions of log events need to be analyzed.
- Ability to correlate events across the environment using a SIEM, process a large numbers of events down to a handful of events to be reviewed.
- Balance between internal and external experts
- Geo-IP blocking reduce the threat conduit
Access Management

• Organizations are to first determine access needs for each workforce member, and then limit their access to what is necessary for their job.

• The rule does not specify role based access, rule based access, how to treat elevated privileges, service accounts, remote access, vendor access, levels of authentication, etc.

• Role based access is a must.

• Administrators with elevated privileges can make changes to the environment.

• Manual process for account management is time consuming and leaves room for provisioning errors.

• Without good access management and accountability it’s hard to know who, what, and when.

• Identity and access management tools manage this process.

• Automated log monitoring tools alert when elevated access privileges are created and used.
Security Awareness & Training

• Implement a security awareness and training program for all workforce members (to include management), vague on periodicity
  – Periodic reminders
  – Protection from malware
  – Log in monitoring
  – Password management
• ISO, PCI, FISMA, GLBA, RedFlags, CobiT, NERC-CIP, State Laws
• There are more than 572 individual knowledge and skills areas in 30 categories identified for cybersecurity awareness and training.

• Traditional HIPAA training cannot address the changing threat environment.
• Recognize that education alone isn’t going to cut it anymore.
• Phishing is a practical exercise by putting the user in a real life simulated environment, but this one is penalty free.
• Social engineering is a reality - why go through a firewall when you can go through the front door.
• Security exercise simulations put people in a mock security incident to test the response process and procedures.
• Monthly security articles relevant to today’s threats.
Evaluation

- Perform a periodic technical and non-technical evaluation based on the standards within the Security Rule and in response to environmental changes.
  - Periodicity is not defined.
  - No standard set for type of testing, how often, what to test for, etc.

- Today’s complex environments require security testing during implement and for all system changes.

- Testing program should evaluate how effective we are at system hardening, patching, and following change control.

- Any changes in the environment need to be tested.

- If our processes are performing well then we will have a high degree of integrity.

- Two levels – testing vendors validating the systems then we use internal tools to validate.

- Change management cycle.

- Tools/applications to help organize data.
Business Associates

- CEs may permit vendors to create, process, store or transmit PHI on their behalf if the CE obtains satisfactory assurances that the vendor will appropriately safeguard the information.
- A Business Associate Agreement establishes the legal basis for these assurances.
- Specific requirements for due diligence are not identified.
- NIST, CobiT, PCI, FFIEC, FISMA, etc. all have very specific requirements for supply chain security.
- Vendor security management from a lifecycle approach.
- Need to make sure security requirements are baked in on the front end of the vendor selection process thru contract negotiation.
- SLA agreements for hosted solutions - do they meet the business requirements for uptime.
- Where is your data going to be stored?
- Monitoring requirement in the contract so the vendor can prove they have a security program.
- Language with respect to what happens to our data at the end of the agreement.
- Should a breach happen at a 3rd party, how will the notification process occur.
- Compliance and Security must work together.
Encryption

• HIPAA discusses encryption under Access Controls – “Implement a mechanism to encrypt PHI” as a means of limiting access to PHI to intended recipients or authorized users.

• HIPAA mentions encryption again under Transmission Security specifically as it relates to transmitting PHI over open networks (internet).

• The Breach Notification and subsequently the Omnibus Rule clarified encryption requirements and application.

• HIPAA only concerns itself with encryption of PHI.

• Time to think about data encryption across the environment.

• Anywhere we have PHI we need to determine if encryption should be applied.

• Encryption of privileged accounts across the environment.

• Compromised administrator credentials allow the attacker to own the environment.

• Email encryption.

• USB drives.

• All information encrypted prior to transmission.

• Mandate SSL for internal applications where possible.
Audit Controls

- Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use PHI.
- The Security Rule does not identify what information is important to collect.
- How often audit reports should be reviewed.
- The complex systems that we have today require automation technologies to react to events.
- Auditing based on compliance rules will not allow you to identify bad behavior.
- You need to look for anomalies, look for traffic it doesn't recognize – not just things that are broken.
- Sandboxing traffic allows analysis to determine if it is malicious or not.
- 60K new malwares were released last month that traditional signature based systems don't recognize.
- Categorize and prioritize all applications that contain PHI.
- Resource constraints/expertise is why it is important to partner with MSSP.
Person or Entity Authentication

- Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
- The Security Rule provides no further specifics.
- The Security Rule does not differentiate between users.
- Generally authentication is achieved by:
  - Something the user knows
  - Something the user possesses
  - Something unique to the user
- Identity and access management is critical to security – you have to know who they are and what they are accessing.
- Good oversight is key, and automation is the only way to accomplish this.
- Disparity of systems create a challenge.
- Two factor authentication enhances security. This make compromising that account much harder.
- Soft tokens on smart phones, biometrics, tokens.
- Remote access by computers that are untrusted.
- Healthcare is getting extended out to the home, the patients need to have the same level of confidence in providers as they do their bank.
- PHI, PII, and financial information in our systems.
What About…

- Mobile technologies (BYOD)
- Networked medical devices
- Cloud and SaaS solutions
- Big data
- Wearable technologies
- Whatever is next…

- The new threat landscape in which security is no longer just an internal concern.
- Standards lag behind the technology, whereas NIST and other standards bodies will develop standards and guidelines for security of these devices.
- To stay up with real risks in the environment we have to go beyond HIPAA.
- Mobile devices have caused us to address remote access with BYOD.
- Medical devices are of great concern due to lack of compliance requirements.
- We have to look to frameworks as we address security issues with these new technologies.
Importance
Compliance ≠ Security

“Being compliant does not make you safe, being certified does not mean you are protected, and neither of those things are going to save you from the impact or fall out associated with a breach.”

“The things that matter are discipline, vigilance, inspection and readiness.”
Frameworks Facilitate Metrics

- How secure are we?
- How effective are the controls we’ve put in place?
- Where are our biggest gaps?
- Where can we make the biggest difference?
- What do we need to educate senior management on with respect to business impact?
Example Incident Response

• Goal
  – Assess ability to detect, respond and recover from incidents

• Measurement
  – Mean time to discovery, eradication & recovery

• Presentation
  – Graph showing average times per incident by month
The Framework Provides a Common Taxonomy to...

• Describe an organization’s **current** cybersecurity posture
• Describe its **target state** for cybersecurity
• Identify and **prioritize** areas of improvement
• Employ a **repeatable** process for review
• Continuously **assess** its cybersecurity posture
• **Communicate** cybersecurity risks to both internal and external stakeholders
Why NIST Security Framework

- The NIST is a recognized federally funded standards institute dedicated to developing and testing information security standards.
- The NIST frameworks are considered industry best practice.
- The NIST frameworks are recognized by both private and public sector compliance standards.
- HHS only references NIST guidelines when providing baselines for regulatory standards.
- Demonstrates due diligence.
- Allows for risk based approach for determining controls.
- Complete flexibility to implement.
- Insures relevance with current threat issues.
- Meets definition of “standard of care”.
Compliance is Necessary

“It should be noted that it took many years to get the seatbelt usage up to its present level, and it takes a heavy hand from the police to persuade the stupid to do the obvious.”

- Peter N. Wadham
It’s Time...

Healthcare must think and act differently when it comes to data security and privacy.
A Summary of How Benefits Were Realized for the Value of Health IT

Reliance of information increases satisfaction

Knowing information is secure and having accurate info improves quality of treatment

Going beyond security compliance requirements helps secure electronic data

Secure data enhances patient engagement

Proactive security reduces likelihood of a breach and helps reduce expenses
Questions

Jay Adams
Director of Information Security
Tallahassee Memorial Healthcare
jay.adams@tmh.org

Co-founder & CEO
CynergisTek, Inc.
mac.mcmillan@cynergistek.com
@mmcmillan07