HIPAA Compliance is not a Cybersecurity Strategy

Presented by:
Hector Rodriguez, WW Health CISO, Microsoft
Jay Trinckes, Director, Coalfire
Speaker Introductions

Hector Rodriguez, WW Health CISO, Microsoft

Jay Trinckes, Director, Coalfire
Agenda

• Timeline – how did we get here?
• Why does this matter?
• What’s the problem?
• Coalfire: Risk versus compliance assessments
• Coalfire: Managing cybersecurity risk in a HIPAA-compliant world
Timeline
HOW DID WE GET HERE?
HIPAA Compliance ≠ Cybersecurity

**HIPAA compliance**
- An audit process
- Focused on ePHI and code sets
- A yearly report of security and compliance policies & procedures and ability to meet a specific set of defined requirements at a point in time

**Cybersecurity**
- A process
- Holistic
- Always On
- Built on modern technology
- Layered Security
- Security-in-Depth
- Critical “must have”
- Everyone’s responsibility

**Compliance + Cybersecurity**
- Not mutually exclusive
- Must be integrated
- “Always On” together
- Applied to everyone and everything
- Include security, privacy, and compliance
- Foundational
Timeline – from HIPAA to Cybersecurity
The Internet Came First But…

Timeline – from HIPAA to Cybersecurity …HIPAA Compliance Out of Sync

1991-1st Web Page
1998-2002-HIPAA NPRMs Progress
2007-NPID Compliance
2012-HIPAA 5010
1/2013-HITECH W/Breach Notification Final Rule
2/2014-NIST CSF Published
8/1996-HIPAA Enacted
2003-2005-Compliance & Deadlines
2/2009-HITECH/ARRA Signed
2012-MA Eye&Ear, BCBSTN - $1.5M HIPAA Violation Fines
2/2014-NIST CSF Published

The “HIPAA Compliant” covered entities thought they were secure

2015-2017-Ransomware, Cyberattacks, etc.

“HIPAA has Teeth” – more fines, lack of risk assessment

The "HIPAA Compliant" covered entities thought they were secure
Timeline – from HIPAA to Cyber Security
Attacks on “HIPAA Compliant” Entities Continue

Ransomware moved from nuisance to epidemic in 2016: IMB study
The year 2016 saw 400% increase in spam; 44% of spam emails contained malicious attachments. Ransomware made up 85% of those malicious attachments

Ransomware attacks on Hospitals put Patients at Risk

Hackers steal personal data of thousands of hospital staff
Information on staff accessed through attack on IT contractor’s server.

By Danny Palmer | March 13, 2017 -- 12:51 GMT (00:51 PDT) | Topic: Security

The Internet of Things is making hospitals more vulnerable to hackers
The attack potential grows exponentially as IoT technologies are implemented, warns European cyber security agency.
Regulations – what regulations?

No Matches Found 😞

- Cloud
- Cybersecurity

*Note: HITRUST CSF and NIST CSF Fill the Gap
WHY DOES THIS MATTER?
Start with Why: 86% of CEOs consider Digital their #1 priority

CEOs believe technology will transform their business more than any other global trend

Top 5 Concerns Keeping Hospital Executives Up

1. Engaging physicians in reducing clinical variation (53%)
2. Redesigning health system for Population Health (52%)
3. Meeting increasing consumer expectations for services (47%)
4. Implementing Patient Engagement strategies (45%)
5. Controlling avoidable utilization (44%)

Trends that will transform business, next five years (%)

- The Advisory Board Company’s Annual CEO Survey, April 2016

Source: PWC CEO Survey
Scenarios for Healthcare
Digital Transformation Pillars in Healthcare

Digital Transformation Pillars

- ENGAGE MEMBERS
- EMPOWER CARE TEAMS, UTILIZATION
- OPTIMIZE CLINICAL & OPERATIONAL EFFECTIVENESS
- TRANSFORM THE CARE CONTINUUM

Scenarios

- More Efficient Access
- Virtual Care
- Quality Improvement
- Remote Monitoring/Rural Health
- More Efficient Engagement
- Care Team Collaboration & Productivity
- Population Health
- Precision Health
- More Continuous Engagement
- Care Coordination
- Operational & Financial Efficiency
- Managing Devices & Facilities
- More Efficient Engagement
- Care Coordination

Trusted Technology – enabling Security, Privacy, & Regulatory Compliance

Must be built on an end-to-end Cybersecurity Foundation
Role: Security, Privacy, and Compliance are Foundational to Healthcare Digital Transformation

- Not mutually exclusive, required across the extended enterprise
- Success in today's economy requires that organizations establish and operationalize a culture of security and privacy to ensure consistent and continued protection of sensitive data

"Companies need to rethink their approach to security... The approach we recommend is really founded on the fact that security is part of the entire life cycle. It should be catered to at the start of the digital transformation..."

Raymond Teo
SVP NTT Security’s APAC Field Operations
Role: Digital Transformation Enables “New Designs”

The Institute for Health Improvement states that new designs must be developed to simultaneously pursue the three dimensions of healthcare transformation called the “Triple Aim”.

1. Improving the patient experience of care (including quality and satisfaction)
2. Improving the health of populations
3. Reducing the per capita cost of health care

Microsoft defines digital transformation in health as "technology enabled care, health promotion and disease prevention that advances the triple aim in a trusted mobile-first, cloud-first world."
WHAT’S THE PROBLEM?
Covered Entities Believe They are Secure

Common Myths and Misunderstandings

- Our EMR vendor will make us HIPAA Compliant
- Our Cloud Services Provider is HIPAA Compliant
- We’re HIPAA Compliant so therefore…”We’re secure”
- We don’t run cloud services…on premise so it doesn’t apply to us
- There’s no ePHI…so it doesn’t apply
- …
Covered Entities Believe They are Secure
But...Here’s a Perfect Example...

Denver-Based FQHC Will Pay $400,000 HIPAA Settlement

April 12, 2017 by Heather Landl

The U.S. Department of Health and Human Services, Office for Civil Rights (OCR) announced that a Denver-based provider, Metro Community Provider Network, has agreed to pay $400,000 and to implement a corrective action plan to settle potential noncompliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules.

The settlement is based on the lack of a security management process to safeguard electronic protected health information (ePHI), according to OCR.

- Breach took place in December 2011.
- Hacker accessed employees’ email accounts and obtained 3,200 individuals’ ePHI through a phishing incident.
- OCR then investigated the incident and the agency found that MCPN took necessary corrective action related to the phishing incident.
- Investigation also revealed that MCPN failed to conduct a risk analysis until mid-February 2012.
- Prior to the breach incident, MCPN had not conducted a risk analysis to assess the risks and vulnerabilities in its ePHI environment.
- Had not implemented any corresponding risk management plans to address the risks and vulnerabilities identified in a risk analysis.
- When MCPN finally conducted a risk analysis, it was insufficient to meet the requirements of the Security Rule.
Risk Assessment vs. Compliance Assessment

WHAT’S THE DIFFERENCE?
Compliance Versus Risk – HIPAA Compliance is not a Cybersecurity Strategy

HITRUST is a risk-based assessment that covers the security, privacy, and compliance posture overall and the HITRUST CSF fully integrates the requirements of the HIPAA Security Rule with the standards of ISO, NIST and many other federal, state, and business requirements listed in the whitepaper. One of the statements that we made last year and still holds true is that HIPAA compliance is not a cyber-security posture or plan.

In the US, covered entities need to work with cloud and solution vendors who do both (and more).
HOW DO YOU MANAGE CYBERSECURITY RISK IN A HIPAA-COMPLIANT WORLD?
Visit the Coalfire booth in the exhibitor area to get the paper.
Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight