℞

Prescribing Privacy

When the Dx is an OCR Audit or Potential Noncompliance, Prescribe Privacy as the Solution

Cybersecurity & Privacy Compliance

HCCA- 2016

Your Speakers

Ellen Giblin

Privacy Officer
Boston Children's Hospital & Foundations

Ken Mortensen

Senior Managing Director
Cybersecurity and Privacy
PwC

Mike Parisi

Director
Risk Assurance
PwC

2

Agenda - Prescribing Privacy

Framing Your Business Issues

- Business Issues
- Regulatory Trends

Framing the Solution to the Needs

- Industry Trends
- Process

The "One-Size-Fits-All" Framework

- Single Framework Solution
- HITRUST

3

Framing your Business Issues

Selecting an appropriate framework to address your business needs as a crucial step for sustaining compliance.

Business Issues and Challenges

Changing information security and privacy requirements continue to challenge healthcare organizations.

- Healthcare regulatory requirements are relatively subjective and are often interpreted and applied differently across organizations
- Applicability (to the organization and its affiliates/partners) is not clear;
- Baseline controls may differ across an organization
- Unclear/inconsistent definition of sensitive data
- Risk of data breach and exposure
- Growing risk and liability associated with information protection
- Increased risk that critical systems may not have appropriate controls
- Preparing the organization for inspections/audits by regulators

5

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996:
  - Encourages efficiencies in exchange of health information.
  - Requires HHS to adopt standards for electronic transmission of certain health information
- Title II, Subtitle F, Section 264, *Recommendations with Respect to Privacy of Certain Health Information*:
  - Requires Secretary of HHS to establish standards with respect to privacy of individually identifiable health information.

6

Regulatory Trends - Omnipresent Challenge

Organizations that handle Protected Health Information (PHI) face a complex landscape of regulation at both the state and federal level.

NRS: Chapter 603A – State of Nevada *Security of Personal Information*	NIST/HITSP Standards for Certified EHR	Final HIPAA Omnibus Rule - 2013 *Security, Privacy and Breach Notification*
Texas General Laws 181: TX HB 300	HITECH Act - Encryption/ Destruction Guidance – 2009	Federal Register 21 CFR Part 11 – Electronic Records/Signatures
FTC - Identity Theft Red Flags	NIST Special Publication 800-53 Revision 3 - *Recommended Security Controls for Federal Information Systems and Organizations*	NIST Special Publication 800-66 Revision 1 - *Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*
Payment Card Industry (PCI) Data Security Standard Version 3.0	The Joint Commission Hospital Accreditation Standards (JCAHO) *Information Management (IM) Standards, Elements of Performance, and Scoring*	MA 201 CMR 17.00 : Standards for the Protection of Personal Information

7

Regulatory Trends - HIPAA Privacy Rule

HIPAA privacy is a set of fair information practices to ensure that:

- Personal information is accurate, relevant, and current;
- All uses of information are known and appropriate; and
- Personal information is protected.

Privacy rules require that:

- Employees collect, access, use, and disclose personal information only for reasons that are for a legitimate job function and are allowed by law;
- Safeguard personal information, whether it be in paper or electronic format;
- Properly dispose of documents containing PHI; and
- Report suspected privacy violations or incidents.

8

Regulatory Trends - HIPAA Security Rule

Establishes a national set of security standards for ePHI

- Protects certain health information held or transmitted in electronic form by a HIPAA- covered entity
- Requires the administrative, physical, and technical safeguards that covered entities must put in place to secure individuals' ePHI
- Does not apply to PHI transmitted orally or on paper
- Supports the Privacy Rule requirement to reasonably safeguard PHI in all forms

The three cornerstones of the HIPAA security standards for ePHI are confidentiality, integrity, and availability (CIA).

- Confidentiality – means that ePHI is not made available or disclosed to unauthorized persons or processes
- Integrity – means that ePHI has not been altered or destroyed in an unauthorized manner
- Availability – means that ePHI is accessible and usable upon demand by an authorized person

9

Industry Trends

Insights from the Field:

Understanding the current drivers that inform framework development can help prepare you for the road ahead.

Industry Trends

- Information security and privacy policies exist but are **specific to each requirement**
- Information security and privacy risk assessments, control self assessments, and internal audits attempt to **validate each requirement and control separately and in uncoordinated manner.**
- **A repository of all information systems does not exist** or is not kept up to date.
- **Ownership** of information security and privacy controls **exists only with the CISO or CPO.**
- **Basic information security and privacy governance programs** exist, but lack clear direction and **organizational clout.**
- General **understanding** and agreement **about information asset risk** does not exist.
- **Total cost of compliance** has not been quantified.

Key Point: *Organizations are missing out on opportunities to streamline and integrate information security and privacy efforts.*

11

Industry Trends - Competing priorities and focus

Focus: Adherence of privacy and security policies to regulatory requirements (e.g., HIPAA; PCI)

Legal/Compliance

Focus: Ensuring comply with corporate policy business units (e.g., CoBIT)

Audit

Information Technology

Focus: Implementing and maintaining minimum levels of control that achieve best practice standards. (e.g., ISO)

Building an integrated approach to privacy and security requirements assists by:

1. Ensuring efforts are prioritized across key functional areas, including Legal, Compliance and IT
2. Changes to the policies/procedures and environment do not create unexpected conflict
3. Waste (time/resources) from poorly aligned strategies is reduced.

12

Industry Conclusions - Integrate

An integrated privacy and security framework helps to consolidate requirements, which may be leveraged throughout the organization.

Such a framework can:

- Establish a single benchmark for an organization to facilitate internal and external measurement which incorporates the requirements of applicable standards and regulations including ISO, PCI, CoBIT, HIPAA, HITECH, and NIST.
- Increase trust and transparency among business partners and consumers **(e.g., carry "street value")** by incorporating best practices and building confidence through framework inclusiveness and visibility.
- Contain the cost of compliance while reducing the number, complexity, and degree of variation in risks and controls.
- Enable an organization to quickly identify and integrate new requirements.

13

Balancing Business Enablers vs. Business Risks

Mobility & Social Media	Mobile devices, mobile applications, social media, and accelerated product life cycles are just the latest contributors to risk of an enterprise.
Third Party Vendors & Cloud Computing	While risks associated with third parties and cloud computing continue to increase, many companies are less prepared to defend their data.
Insider Threats	Organizations need to focus on the insider threat along with the cyber threat.
Cyber Threat Intelligence	Cyber security will have to integrate all threat intelligence sources in a state of perpetual analysis to enhance and safeguard operations.
Incident Response Management	While breaches and incidents continue to rise organizations need to focus on creating a comprehensive Incident Response Management Program.
Threat & Vulnerability Management	Companies need to stay informed about the constantly changing threat environment, processes to identify potential vulnerabilities, and processes to resolve potential exposures.
Privacy & Data Protection	Organizations looking to improve privacy management in the event of a breach have to continually plan and prepare.
Big Data Analytics for Cybersecurity	Big Data is only getting bigger. Organizations will learn to assess and mitigate the risks along with using big data to enhance threat intelligence mechanisms.
Engaging with the Boards	Obtaining board level and executive level support for security initiatives is imperative for an organization to maintain an effective security program.

14

Lessons learned from recent cyber events

Recent breaches in retail and consumer industry challenges apply to a broader set of companies and industry sectors

- Attack Method - **organized and coordinated efforts** to exploit a known technical vulnerability in the core infrastructure
- Awareness - adversaries **tested and enhanced** their approach **over the course of months** before executing their campaign; intelligence sources communicated threat elements
- Detection - **technical indicators were undetected** during the attack sequence; additionally, as is often the case, third parties (e.g. law enforcement or the banks) detect the compromise, ***not*** the company
- Security Posture **- known companies compromised** were assumed to be **compliant** with industry standards (e.g. HIPAA, ISO/NIST, PCI DSS) -- compliance does not equal security
- Industry Exposure – attacks are often **not limited to a single company**; many companies within an industry sector share the same / similar profile and it is highly likely there are other targets and victims

15

HIPAA Compliance does not equal Security

Meeting the HIPAA Privacy and Security Rules may not be sufficient to prepare an organization for today's threats.

- HIPAA - The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is implemented by **covered entities (and there business associates)** through adoption of the **HIPAA Privacy Rule** and the **HIPAA Security Rule**;
- The HIPAA Privacy Rule - **only applies to individually identifiable health information**, used or disclosed by a covered entity for healthcare purposes, known as protected health information or PHI;
- The HIPAA Security Rule - applies only to that **subset of PHI** that is created, received, maintained, or transmitted in **electronic form** (ePHI);
- Limitations of scope
  - **Data** - other types of critical data, for example, **intellectual property, authentication credentials, or non-public financial information**, are **not** necessarily protected, even if an organization meets the HIPAA rules;
  - **Threats & Vulnerabilities –** requirements do not address evolving threats and vulnerabilities, and as such, **The controls required to meet the Security Rule a few years ago are insufficient** to address the APTs of today.

16

Impacts of Cyberattack and Breaches

- Security and data breach response has been a security and compliance activity – **it's starting to become a board level and audit committee issue**
- The industry has faced regulatory scrutiny for data loss / breaches previously; however these cybersecurity attacks are significantly different in their objectives, execution and impact. For instance these new cyber attackers are:
  - Seeking PHI/PII data for resale on black market for fraudulent access to healthcare products and services (i.e. Medicare, which is not reimbursable)
  - Targeting intellectual property including clinical trial data for new pharmaceuticals
  - Utilizing sophisticated threat actors with exceptional technical skills and experience
  - Employ advanced persistent threats to avoid detection and propagate your network seeking valuable information including intellectual property, trade secrets, etc.
- While some companies are thinking about proactive actions and some will operate reactively; PwC belief is to lead your response with a **business risk based approach**

Risks

- **Financial**: fines, remediation, cost to defend
- **Reputational**: brand impact, loss of confidence
- **Regulatory**: active regulators, increasing enforcement
- **Legal**: lawsuits, class action
- **Compliance**: evolving domestic & international laws
- **Contractual**: compliance with "promises" made – yours and your vendors/third parties

17

The value of integrating a framework

Benefits to Management

- Increased confidence in the organizations ability to address information privacy and security challenges comprehensively.
- Reduces risk through the incorporation of best practices into the framework.
- Gives management and internal audit the ability to assess the organizations compliance with information security requirements efficiently and in a coordinated matter.
- Provides clarity on information security requirements and expectations for all those charged with information security and privacy.
- Improves understanding of compliance requirements increases individual ability to apply safeguards and spot/report issues.
- Reduces expenses associated with information security assessments.

Benefits to the Community

- Increased trust throughout the healthcare system from all stakeholders.
- Can help improve organizations image to consumers and influence how their choices are made.

Benefits to the Regulators and Auditors

- Allows organizations to demonstrate compliance with MU requirements around information privacy and security.
- Reduces the complexity and ambiguity when working with auditors attempting to assess compliance.

18

The process of integrating a framework

Taking Requirements…

- MA-201/CMIA
- HIPAA
- PCI
- ISO
- NIST

Identifying Common Controls or Processes…

- Access Control
- Passwords
- Encryption
- Training
- Risk Assessment

Execute integrated program…

- Identify Data Sources
- Define & Assess Risk
- Develop & Implement Controls
- Audit and Correct
- Enforce, Monitor & Support

Document policy, controls and criteria that meet minimum requirements across standards…

- Integrated Control Framework

19

The One-Size-Fits-All Framework

Privacy + Security = Success

HITRUST
Health Information Trust Alliance

Single Solution - HITRUST

HITRUST
Health Information Trust Alliance

Basic Facts:

- Security Framework (CSF) which brings together the following standards into a single framework specific to the health care industry
  - ISO 27001, 27002 and 27799
  - NIST 800-53 and 800-66
  - Health Insurance Portability and Accountability Act (HIPAA)
  - CoBIT
  - PCI Data Security Standard (PCI DSS)
  - Considers federal and state regulations
- Office of Civil Rights (OCR) refers to the HITRUST CSF as resource to use when defining risk analysis and assessment programs
- Offers Varying Levels of Certification

21

Single Solution - HITRUST

The HITRUST CSF:

- Maps to compliance frameworks and maps to reporting (parts) initiatives like components of SOC1/2 principles etc.
- What drives the business issues/ what do I assess against/ pros and cons
- What about this concept of streamlining against 1 (CSF)

Single Framework, Cohesive Compliance

- Reduced Incidence of Noncompliance
- Qualifies as a Risk Assessment

22

Single Framework - Overview

The CSF provides a benchmark for the organizations' adoption of information security and privacy. The CSF is:

- Healthcare focused
- Updated at least annually
- Incorporates requirements from numerous frameworks and regulations, addressing many industry segments

Certifiable compliance, common understanding and acceptance

- Provides accreditation and certification process to drive transparency and adoption of baseline information security controls
- Follows a risk-based approach to allow security controls to be prioritized based on risk

23

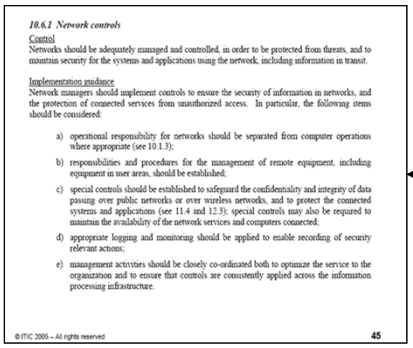
Single Framework - Categorical Composition

The HITRUST CSF addresses the following 14 information security and privacy areas of focus, referred to as Control Categories:

Information Security Management Program	Security Policy	Physical and Environmental Security
Access Control	Organization of Information Security	Communications and Operations Management
Human Resources Security	Business Continuity Management	Information Systems Acquisition, Development and Maintenance
Risk Management	Compliance	Information Security Incident Management
Privacy Practices	Asset Management	

24

HITRUST CSF – Control mapping example



10.6.1 Network controls

Control

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

Implementation guidance

Network managers should implement controls to ensure the security of information in networks, and the protection of connected services from unauthorized access. In particular, the following items should be considered:

a) operational responsibility for networks should be separated from computer operations where appropriate (see 10.1.3);

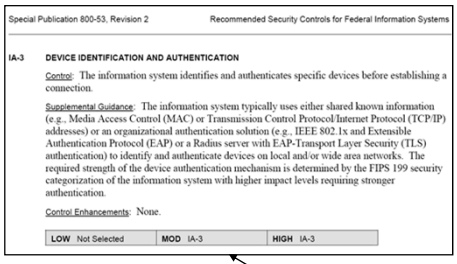
b) responsibilities and procedures for the management of remote equipment, including equipment in user areas, should be established;

c) special controls should be established to safeguard the confidentiality and integrity of data passing over public networks or over wireless networks, and to protect the connected systems and applications (see 11.4 and 12.3); special controls may also be required to maintain the availability of the network services and computers connected;

d) appropriate logging and monitoring should be applied to enable recording of security relevant actions;

e) management activities should be closely co-ordinated both to optimize the service to the organization and to ensure that controls are consistently applied across the information processing infrastructure.

 45



Special Publication 800-53, Revision 2 Recommended Security Controls for Federal Information Systems

IA-3 DEVICE IDENTIFICATION AND AUTHENTICATION

Control: The information system identifies and authenticates specific devices before establishing a connection.

Supplemental Guidance: The information system typically uses either shared known information (e.g., Media Access Control (MAC) or Transmission Control Protocol/Internet Protocol (TCP/IP) addresses) or an organizational authentication solution (e.g., IEEE 802.1x and Extensible Authentication Protocol (EAP) or a Radius server with EAP-Transport Layer Security (TLS) authentication) to identify and authenticate devices on local and/or wide area networks. The required strength of the device authentication mechanism is determined by the FIPS 199 security categorization of the information system with higher impact levels requiring stronger authentication.

Control Enhancements: None.

LOW Not Selected	MOD IA-3	HIGH IA-3

ISO controls for network security

NIST controls for network security enhanced beyond ISO

Level 2 Implementation Requirement

HITRUST CSF leverages ISO as the base and is improved with the more stringent requirements of NIST

25

Contacts

Ellen Giblin
Privacy Officer- Boston Children's Hospital
(617)
ellen.giblin@childrens.harvard.edu

Kenneth Mortensen
Managing Director
Cybersecurity & Privacy
(617) 530-5137
kenneth.p.mortensen@pwc.com

Michael Parisi
Director
Risk Assurance
(860) 241-7194
michael.p.parisi@pwc.com

26

Thank You!

Q&A

Cybersecurity & Privacy Compliance

HCCA- 2016