How to align governance with the practical aspects of information Security and Privacy compliance

Ryan Dobbins  GSLC, HCISPP | Director, Advisory Services  Infolock Technologies

Karen Pagliaro-Meyer  
Chief Privacy Officer  
Columbia University Medical Center

Robert Lord  
Co-Founder  
protenus.com
Learning Objectives

- Understanding the difference between compliance and information security/privacy
- Understanding what a security control is
- How to align security controls and corporate policy
- How to create reportable metrics that support security, privacy, and compliance.
What is the problem at hand?

- Compliance is defined as conforming to a rule

- IT Organizations struggle to effectively comply with Security and Privacy governance if the ‘rules’ are not completely understood or measured

- The effect is a reactive posture to Security and Privacy
Reactive Compliance

Inefficient, Ineffective, Expensive

Imagine a home builder who does not understand building codes and relies on visits from the Inspector to be compliant.
How to align governance with the practical aspects of information Security and Privacy compliance

RESULTS OF COMPOUNDING INEFFICIENCIES

The real world impact of unaligned governance

Understanding

IT understands 70% of the compliance requirements

Implementation

Around 60% of requirements are fully implemented.

Scope

Change reaches 80% of the target audience.

Effect

Governance is 33% effective.
Using controls to solve the issue

What is a technical control?

A sequential building block for information and infrastructure security that a computer can execute.

Fundamentally privacy does not exist without security

By using Technical Control language in Governance, IT is mandated to build secure environments in language they understand. This in turn can ensure privacy and subsequently compliance in a holistic sense.
How to align governance with the practical aspects of information Security and Privacy compliance

Technical Controls
A language and context that all can understand and measure - examples

- Data Inventory
- Data Classification and Risk
- Data Use

• Hardware Inventory
• Software inventory
• Secure Configurations

Align Governance with fundamental security concepts
What it looks like
Control requirements specified in Governance that are measured

Control – Data Inventory

Governance – A policy stating that protected data is defined, identified and cataloged

Measurement – Scheduled Data at Rest scans with the results compared to the known data inventory

Measurement and reporting allows leadership to make informed decisions.
How to align governance with the practical aspects of information Security and Privacy compliance

RESULTS OF COMPOUNDING INEFFICIENCIES
The real world impact of unaligned governance

Understanding
IT understands 95% of the compliance requirements

Implementation
Around 80% of requirements are fully implemented.

Scope
Change reaches 95% of the target audience.

Effect
Governance is 72% effective.
Technical Controls are a universal language to bridge the gap between Governance and Information Technology.

By using technical controls when producing governance, information professionals are empowered to build fundamentally secure environments which in turn meet compliance requirements efficiently and effectively.

Technical Controls are easily measured.
THANK YOU
The Trustees of Columbia University in the City of New York
Columbia University Medical Center (CUMC)

• Accounting for roughly half of Columbia University's nearly $3 billion annual budget, Columbia University Medical Center (CUMC) provides global leadership in scientific research, health and medical education and patient care

• Columbia University Medical Center is a Hybrid Entity
  • Excludes schools of Business, Law, Journalism, General Studies, Arts and Sciences etc.
  • Includes several internal business associates i.e. General Counsel, Treasury, Procurement, Information Technology etc.
  • 3,500 faculty members
  • 2,000 students (Medical, Nursing, Dental and Public Health)
  • 14,000 staff members

• Columbia University Medical Center is also in an OHCA with NewYork Presbyterian Hospital and Weill Cornell Medical Center
Governance

- The governance structure at the medical center has evolved over time.
- Committee membership, roles, and responsibilities are periodically reviewed and updated.
- Communication and support between the Privacy Officer and the Information Security Officer is crucial for an effective HIPAA Compliance Program.
- Support from Administration and Clinical Leadership is also critical.
- Regular communication with OHCA Privacy and Information Security Officer is important.
- Development and monitoring of key indicators is one of the essential measures of an effective compliance program.
Monitoring

- Daily audit reports of EMR access including:
  - High access volume
  - Consecutive MRN access
  - Hours of access
  - IP conflict
  - VIP access

- Privacy complaint audit

- DLP
Detailed Structure

**HIPAA Risk Management Committee**

- Serves as the authoritative source for risk management decisions for high level risks
- Evaluates privacy and security initiatives and balances these against other operational imperatives
- Membership includes representatives from Office of the General Counsel, CFO, CIO, CMO and CISO, CPO

**Privacy and Security Workgroup**

- Provides an effective mechanism for all of the CUMC schools and departments to review and approve information relating to the HIPAA Privacy and Information Security Program
- Provides support, direction and guidance to the Privacy and Information Security Officers
- Provides periodic updates to the Risk Management Committee
- Ad Hoc subcommittees created as needed
- Membership includes key stakeholders from each of schools and departments

**Incident Response Team / CAP Task Force**

- Membership includes Chief Information Security Officer, Chief Privacy Officer and General Counsel
- Reviews reports privacy and information security incidents and reports findings including corrective action plans to the Risk Management Committee
- Manages the development and implementation of the CAP/Resolution Agreement
- Provides regular updates to the Risk Management Committee
- Ongoing review of new and potential risks
Chief Information Officer (CIO)

- Directs centralized IT functions, including Information Security
- Chairs HIPAA Risk Management Committee

Chief Information Security Officer (CISO)

- Responsible for the day to day operations of the Information Security Program
- Chairs the Certified IT Group Committee
- Ongoing review of potential risks including overseeing the organizations Risk Management Plan

Chief Privacy Officer (CPO)

- Responsible of the day to day to operations of the HIPAA Privacy Program
- Investigates and reviews potential Breach reports in consultations with the Incident Response Team
- Chairs the Privacy and Security Workgroup
CISO & CPO Roles & Responsibilities

What is the difference in Compliance Responsibilities between the Information Security and the Privacy Role?

• Security is an essential component to ensure privacy

• Security is the technical strategy and privacy is the goal/outcome

• Security must be actively involved in privacy issues and policy development and Privacy must be actively involved in Security events/issues and policy development

• Security is not purely technical and privacy is not only HIPAA Breach reports or complaints. These roles must be integrated and interact frequently. Every privacy training session should include security
HIPAA: PRIVACY vs. SECURITY

What’s the Difference?

SECURITY
Refers to **HOW** private information is safeguarded—Insuring privacy by controlling access to information and protecting it from inappropriate disclosure and accidental or intentional destruction or loss.

PRIVACY
Refers to **WHAT** is protected — Health information about an individual and the determination of **WHO** is permitted to use, disclose, or access the information.
CISO & CPO Roles & Responsibilities

• The privacy officer role has changed immensely since it was first mandated by HIPAA in 2003

• Protecting patient health information has become much more complex since 2003, when nearly all healthcare organizations were primarily protecting paper records

• Privacy officers have seen their jobs grow as new regulations, technology, and data-sharing initiatives have reshaped the landscape

• Risks have shifted as organizations transitioned to use of multiple electronic systems including EMR’s, billing systems, quality, HIE and research

• Regular/frequent interaction of privacy and security is essential to evaluate risk, develop mitigation strategies including security controls in addition to responding to audit reports
Governance – Communication Plan

• Training
  – New workforce
  – Annual
  – Remedial
  – Risk focused

• Periodic email reminders / information

• Annual Management Briefing

• Departmental and risk focused training

• Briefings at other management meetings

• Participation at IRB / Research Orientation

• Regular participation in other management meetings to identify potential privacy and security risks
Trust as a Strategic Priority: Privacy Program Maturity

Robert Lord
Fellow, ICIT
Co-Founder, Protenus
Privacy Programs as a Continuum

Privacy programs mature through four incremental steps, all requiring different resources, and one paradigm-shifting leap.
Where Does Your Program Fall?
Survey Results from Recent HCCA Webinar

Percentage

Nothing | Spot Audits | Rules-Based Audits | Privacy Intelligence | Privacy Insight
---|---|---|---|---
0 | 37.5 | 25 | 12.5 | 0
Phase 1: Nothing

- Unfortunate truth is many institutions don’t have the time to really perform audits of their EHR audit logs in any substantive way.
- Often times, hard-working teams don’t have the executive buy-in and staff to build out a monitoring program, despite what 45 CFR 164.308(a)(1)(ii)(D) and 45 CFR 164.312(a-d) mandate.
Phase 2: Spot Audits

- Really just a “snapshot”
- Once per month, year, or quarter taking a sample of users and auditing their work
- Maintain credibility and potentially put one just within the bounds of compliance
- Unlikely to yield much, given the huge number of accesses per year and the time it takes to investigate
Phase 3: Rule-Based Audits

- A wide array of potential tools
- Simplistic, but can get the job done
- Often require a lot of up-front rules specification
- Drowning in false-positives
Phase 4: Privacy Intelligence

- A wide array of tools purport “intelligence”
- Often adds a ROI component or dashboards
- Key is how the tools work together, move beyond more data, truly provide insight
Phase 5: Privacy Insight

• Clinical context
• Data Science
• Machine learning-driven evolution
• Ability to integrate data sources from throughout enterprise
• Use of ensemble anomaly detection
• Dynamic and interactive visualizations
• Supports privacy professionals
Average Time Spent on One Case

Minutes

Traditional Investigations  Privacy Insight

0  20  40  60  80
Useful Features and Sources

- Relationships between users (who collaborates frequently with whom?)
- Patterns of activity (how do individuals traverse the medical record)
- Patterns of treatment (what types of activities do people perform from a clinical perspective)
- What type of patient is being treated (so which types of providers should see them?)
- Typical anomaly detection tools (frequencies and times of day)
One “Under the Hood” Example

Time and Activity of 1 Employee in 26 Medical Records
Considerations for a Privacy Platform

• Ease of data extracts
• Any number of sources to enrich data (PACS, HR, pharmacy, etc.)
• Wide array of analytical techniques
• Natural language explanations of alerts and evidence
• Few false positives
• Visualization to speed investigations
• Reporting to demonstrate ROI
Whatever You Implement Should…

• Track categories of breaches to understand sources
• Create standardized collaboration workflows
• Automate portions to overcome non-human scale problem
• Communicate platform to workforce
• Inform targeted education
Data-driven privacy insights mean you always see the entire picture.