rkl ADVISORS for WHAT'S NEXT

Unveiling the Intersection of Cybersecurity and HIPAA Rules

Presented by:

Michael McAllister | Partner, IS Assurance and Advisory Services

rkl ADVISORS for WHAT'S NEXT

Welcome and Meet Your Facilitator

Michael McAllister, CPA.CITP, CISA

Partner / IS Assurance and Advisory Services

As Partner and Leader of RKL's IS Assurance and Advisory Services Practice, his focus lies in supporting the accounting world and helping clients navigate through the issues and concerns that may keep them up at night.

With more than 30 years of experience in accounting and computer science, Michael builds the knowledge bridge between the financial aspects of accounting, and the information technology systems and controls that support each process.

Together with his IS Assurance & Advisory Services team, he serves clients in a variety of industries, ranging from healthcare, manufacturing to retail, and technology and, creating an extensive background of linking information security and operational risks.

Objectives

- Gain an in-depth understanding of the HIPAA Security and Privacy Rules, their intent, and their application in the healthcare environment.
- Identify the basic principles of cybersecurity, including types of threats, common vulnerabilities and the role of risk management.
- Understand how implementing strong cybersecurity measures can help prevent breaches of protected health information.

"To err is human, but to really foul things up you need a computer."

Paul R. Ehrlich

Understanding the HIPAA and Privacy Rules ›

HIPAA Overview

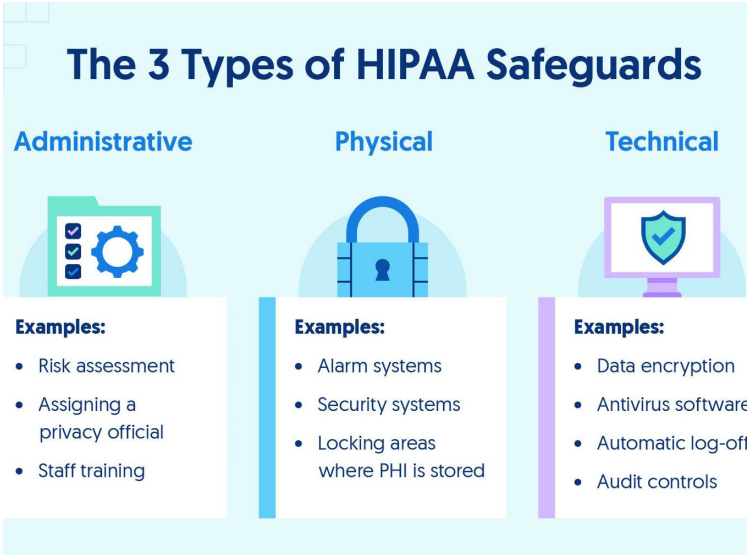
- HIPAA enacted – 1996
- 1998 Proposed rule -> Final Rule – 2003
- HITECH Act – 2009
- 2010 Proposed rule -> Final Rule 2013
- 2024 Proposed rule -> Comment period closed

rkl ADVISORS for WHAT'S NEXT

HIPAA Overview – Security Rule Safeguards

Additional considerations

- Organizational requirements
- Breach notification rule



rkl ADVISORS for WHAT'S NEXT

HIPAA Overview – Consistent Approach

- Confidentiality, integrity, and availability of ePHI
- Reasonable and appropriate safeguards
- Risk analysis and risk management
- Flexible, scalable, and technology neutral requirements

rkl ADVISORS for WHAT'S NEXT

HIPAA Overview – 2024 Proposed Rule Overview

- Notice of Proposed Rulemaking – December 27, 2024
- Comment period ended March 7, 2025
- Highlights of some of the recommended changes:
  - Remove distinction between "required" and "addressable"
  - Required written documentation
  - Greater specificity regarding risk analysis
  - Require regulated entities to perform compliance audit – every 12 months

rkl ADVISORS for WHAT'S NEXT

The Principles of Cybersecurity ›

rkl ADVISORS for WHAT'S NEXT

Cybersecurity Principles

- **Confidentiality:** Ensuring that information is accessible only to those authorized to have access.
- **Integrity:** Safeguarding the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that authorized users have access to information and associated assets when required.

rkl ADVISORS for WHAT'S NEXT

Cybersecurity Principles - Components

- **Network Security:** Protecting the network infrastructure from unauthorized access, misuse, or theft.
- **Application Security:** Keeping software and devices free of threats, often during the development stage.
- **Information Security:** Protecting the integrity and privacy of data, both in storage and in transit.
- **Operational Security:** Processes and decisions for handling and protecting data assets.
- **Disaster Recovery and Business Continuity:** Strategies for responding to and recovering from incidents that disrupt operations.
- **End-user Education:** Training users to recognize and avoid potential threats, such as phishing attacks.

rkl ADVISORS for WHAT'S NEXT

Cybersecurity Principles – Types of Threats

- Social Engineering / Phishing Attacks
- Ransomware / Malware
- Insider Threats
- Unsecured Devices / outdated software and system

rkl ADVISORS for WHAT'S NEXT

Cybersecurity Principles – Threat Trends

- Zero-Click Exploits (No interaction required)
- Internet of Things (IoT)
- Artificial Intelligence
- Quantum Computing

Cybersecurity Principles – Common Vulnerabilities

- Weak passwords
- Lack of encryption
- Inadequate access controls
- Unpatched software
- Improper disposal of data
- Lack of training / personal devices
- Third-party vendor risks

Cybersecurity Principles – Role of Risk Management

- Identification of risks
- Assessments and prioritization
- Implementation of mitigation strategies
- Continuous monitoring and review
- Training and awareness
- Incident response planning
- Compliance with regulations

rkl ADVISORS for WHAT'S NEXT

Managing Risks and Avoidance of Overreliance

- The need to be realistic
- Continually evolving
- Avoid over reliance on the typical cybersecurity practices
- Learning from the "stumbles"

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures ›

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - Strategies

- Strong password policies
- Two-factor authentication
- Regular software updates and patch management
- Data encryption
- Access controls
- Incident response plan
- Vendor management

rkl ADVISORS for WHAT'S NEXT

Ownership of Cyber Risks

Not just an IT concern anymore, everyone has a role and it takes a village, including:

- Executives / C-Suite
- Business / Process owners
- Information Technology team
- Vendors / Contactors

rkl ADVISORS for WHAT'S NEXT

Ownership of Cyber Risks - Executives / C-Suite

- Strategic planning
- Risk acceptance
- Budget
- Regulatory compliance concerns
- Oversight of entire business

rkl ADVISORS for WHAT'S NEXT

Ownership of Cyber Risks – Business / Process Owners

- Following the expectations / directives of the organization's leadership
- Maintaining quality data
- Ensuring proper communication channels are followed and maintained

rkl ADVISORS for WHAT'S NEXT

Ownership of Cyber Risks – Information Technology Department

- Maintaining proper information technology controls
- Creating awareness of emerging threats
- Communicating the risk levels across the organization

rkl ADVISORS for WHAT'S NEXT

Ownership of Cyber Risks – Vendors / Contractors

- Communicating risks / issues
- Staying compliant with security expectations
- Managing additional risk associated with subcontractors / vendors

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - Prevention

- Training specific to the entity and job responsibilities – reinforce protecting privacy
- Device Security Protocols / Data Encryption and proper disposal
- Incident Response – lessons learned
- Vendor / contractor relationship – appropriate breach / security
- Regular Third-party Security Assessment
- Establish an Information Security Framework

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - NIST CSF 2.0

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - NIST Frameworks

Fig. 5. Using the CSF to improve risk management communication

- **NIST (National Institute of Standards and Technology)**
  - Federal agency – part of the U.S. Department of Commerce
  - Established in 1901
- **Cyber Security Framework (CSF) 2.0**
  - February 2024
  - The Cybersecurity Framework (CSF) 2.0 is designed to help organizations of all sizes and sectors — including industry, government, academia, and nonprofit — to manage and reduce their cybersecurity risks.

rkl ADVISORS for WHAT'S NEXT

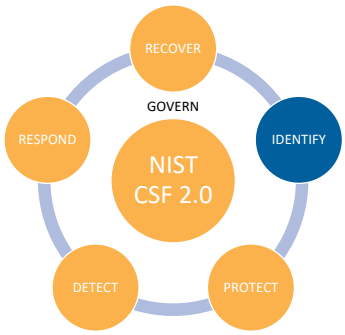
Implementing Cybersecurity Measures - NIST CSF - Govern

The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

- Organizational context
- Risk management strategy
- Roles, responsibilities and authorities
- Policy
- Oversight
- Cybersecurity pully chain risk management

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - NIST CSF - Identify



The organization's current cybersecurity risks are understood

- Asset management
- Risk assessment
- Improvement

rkl ADVISORS for WHAT'S NEXT

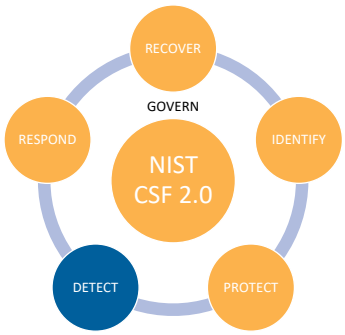
Implementing Cybersecurity Measures - NIST CSF - Protect

Safeguards to manage the organization's cybersecurity risks are used

- Identity management, authentication, and access control
- Data and platform security
- Technology infrastructure resilience

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - NIST CSF - Detect



Possible cybersecurity attacks and compromises are found and analyzed

- Continuous monitoring
- Adverse event analysis

rkl ADVISORS for WHAT'S NEXT

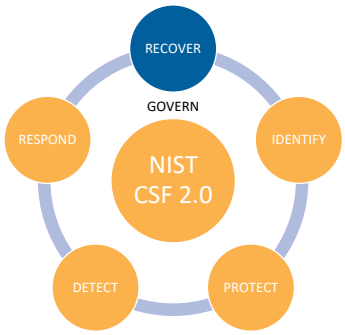
Implementing Cybersecurity Measures - NIST CSF - Respond

Actions regarding a detected cybersecurity incident are taken

- Incident management
- Incident analysis
- Incident response reporting and communication

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - NIST CSF - Recovery



Assets and operations affected by a cybersecurity incident are restored

- Incident recovery plan execution
- Incident recovery communication

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures - Challenges

- Limited resources
- Rapidly evolving threat landscape
- Lack of skilled professionals
- Integration of third-party services

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures– Compliance Issues

According to the Office for Civil Rights, Recurring HIPAA Compliance Issues:

- Individual rights of access
- Risk analysis
- Business associate agreements
- Access controls
- Audit controls
- Information system activity review

rkl ADVISORS for WHAT'S NEXT

Implementing Cybersecurity Measures – Recent OCR Enforcement Actions

Just a few examples of enforcement actions that happened in 2024

Date	Entity	Fine
Dec-24	Immediata Health Group	$250,000
Oct-24	Gum Dental Care	$70,000
Oct-24	Providence Medical Institute	$240,000
Sept-24	Cascade Eye and Skin Centers	$250,000
Aug-24	American Medical Response	$115,200
July-24	Heritage Valley Health System	$950,000

Recent OCR Settlements

Deer Oaks – The Behavioral Health Solution (July 2025)

- $225,000 fine and 2-year surveillance
- Breach and failed to conduct an accurate and thorough risk analysis

Northeast Radiology (April 2025)

- $350,000 fine and 2-year surveillance
- Breach and failed to conduct an accurate and thorough risk analysis

Solara Medical Supplies (January 2025)

- $3,000,000 fine
- Breach and failed to implement security measures and timely notification

Top Patient Safety Concerns - 2025

Insufficient Governance of AI in Healthcare

- Only as good as the algorithms that were used for training
- It will be a challenge to establish policies that can adapt to rapidly changing AI technology

Medical Error & Delay in Care Resulting from Cybersecurity Breach

- 88% reported some level of cyberattack in the past year
- Patient can experience poor outcomes from delays, prescription medications can be compromised – leading to missed doses, resulting in poor outcomes

Let's Recap and Talk About Key Takeaways ›

Recap of Key Points

- Importance of keeping HIPAA Security Rule in line-of-sight
- There are various ways that a covered entity could be exposed
- The role that all team members play in keeping the covered entity secure
- Strategies for enhancing cybersecurity

rkl ADVISORS for WHAT'S NEXT

Continuous education

Encourage the concept of "See something, Say something"

Challenge the current cybersecurity practices

Don't be afraid of an assessment

rkl ADVISORS for WHAT'S NEXT

How Would You Answer These Questions?

Leadership

- How do you stay current in the cyber landscape?
- How has the cybersecurity been improved within the past year?
- What might be the biggest cyber threat (who and what)?

Strategic Posture

- What is the cyber risk tolerance? Does it align with the business tolerance?
- Who is ultimately responsible for cybersecurity and how are they supported?
- Any cybersecurity initiatives that go unfunded, and has the risk been analyzed and accepted?

How Would You Answer These Questions?

Visibility of the cybersecurity program

- How is management staying aware of the volume of attacks? Are they increasing or decreasing?
- What is the escalation process in the event of a cyber event? Who would be the first to know and who would be the last?
- How does the company learn from past issues or adapt to what is happening within the industry?

Skill Sets

- What is your biggest strength and weakness regarding cybersecurity?
- Have external resources been contracted in the event of a cyber issue, and if so, how would they coordinate with internal resources?
- Have internal resources been assessed to determine their ability to address a concern and if not, has a plan been developed?

Do You Have Questions?

rkl ADVISORS for WHAT'S NEXT

Thank You for Joining Us

Whatever your next move, we're here to help.

Michael McAllister
mmcallister@rklcpa.com