HEALTHCARE REGULATORY ROUND-UP #89

Proposed Changes to the HIPAA Security Rule:

Speak Now or Forever Hold Your Peace

February 26, 2025

Housekeeping

- Slides and handouts available in the **Resources Panel**
- Enter questions in the **Q&A Panel**
  - If question not addressed during webinar, will follow-up via e-mail
- Enlarge, rearrange, or close panels as you prefer
- For technical difficulties, try refreshing your browser first

Introductions

Barry Mathis
Principal
bmathis@pyapc.com

Erin Walker
Manager
ewalker@pyapc.com

pyapc.com
800.270.9629

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

Today's Agenda

1. Overview of Proposed HIPAA Security Changes
2. Compliance Implications
3. Potential Impact of The Proposed Changes
4. Strategies to Prepare for Compliance
5. Q&A

1. Overview Of Proposed HIPAA Security Changes

Proposed HIPAA Security Rule Changes

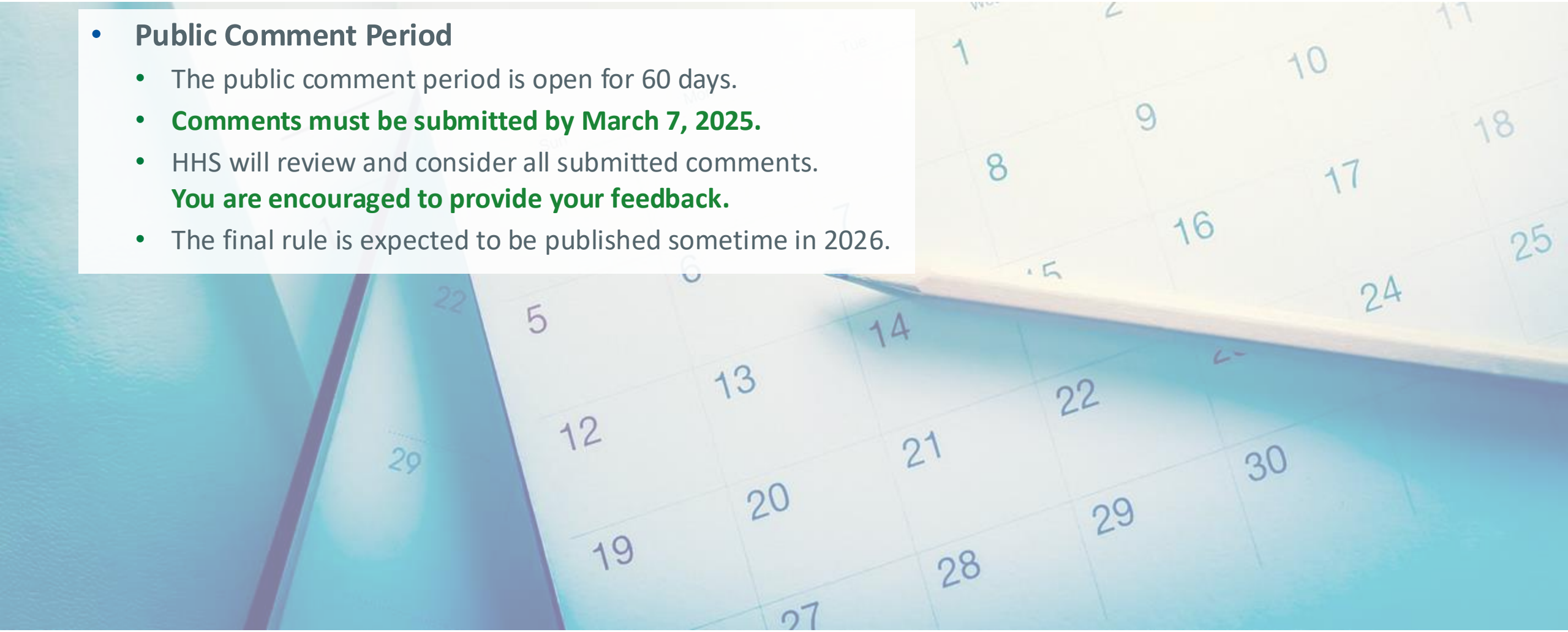
- **Uniform Implementation Specifications**
  - Elimination of distinction between “required” and “addressable” implementation specifications
- **Mandatory Documentation**
  - Maintain written records of all security-related policies, procedures, plans and risk analyses
  - Extends to contingency plans, incident response strategies and network configurations
- **Asset Inventory and Network Mapping**
  - Identify and catalog all devices, applications and systems involved in managing ePHI
  - Document the flow of data within networks
    - Includes smart devices and medical devices connected to the Internet of Things (IoT)
  - Include processes that involve movement of ePHI into and out of a regulated entity’s systems, including those that involve another entity
  - Process to routinely update the required inventory and network map

Proposed HIPAA Security Rule Changes (*cont.*)

- **Enhanced Risk Analysis**
  - Required to identify threats and vulnerabilities comprehensively, assess risk levels and document mitigation strategies
  - Conduct risk assessments of the cybersecurity threats of new Artificial Intelligence (AI) tools
    - Must include, among other things, the type and amount of ePHI accessed by the AI tool, to whom the data is disclosed, and to whom the output is provided
- **Access Termination Notifications**
  - Notify relevant workforce members within 24 hours of changes or terminations in their access to ePHI systems
- **Contingency Planning and Incident Response**
  - Establish procedures to restore lost systems and data within 72 hours of an incident
  - Create comprehensive security incident response plans
- **Annual Compliance Audits and Business Associate Verification**
  - Mandatory annual compliance audits for all covered entities
  - Business associates who play a crucial role in handling ePHI must verify annually that they have implemented the necessary safeguards

Timeline and Compliance

- **Public Comment Period**
  - The public comment period is open for 60 days.
  - **Comments must be submitted by March 7, 2025.**
  - HHS will review and consider all submitted comments.
    You are encouraged to provide your feedback.
  - The final rule is expected to be published sometime in 2026.



Timeline and Compliance (*cont.*)

- **Grace Period**
  - Once the final rule is published, there will be a six-month grace period for compliance.
- **Enforcement**
  - Full enforcement of the new requirements will begin after the grace period.

Resources:

- Proposed HIPAA Security Rule Article
- How To Prepare for HIPAA Security Rule Changes

2. Compliance Implications

Compliance Implications

Security Risk Assessments	Data Encryption	Incident Response and Reporting	Vendor/Third Party Risk
• Review and update risk assessment frameworks to ensure new threats and vulnerabilities are addressed.	• Upgrade existing encryption technologies or implement new ones to meet the updated standards.	• Update or implement new incident response procedures. • Revise reporting mechanisms to meet new timelines and requirements.	• Create training programs, increase training frequency, or ensure staff certification in relevant cybersecurity competencies.

Compliance Implications (*cont.*)

Access Controls	Audit Logs/Monitoring	Policies and Procedures	Increased Reporting
• Review and adjust access control policies, ensuring they align with the latest rules and best practices.	• Implement or update systems that monitor and log user activity. • Ensure logs are accessible for audit purposes.	• Formalize, document, and regularly review cybersecurity policies to ensure compliance with the updated standards.	• Update internal protocols for notifying HHS/OCR about breaches or security events within specific timelines and formats.

Compliance Implications (*cont.*)

Breach Notification	Business Associate Compliance	Emerging Threat and Vulnerability Management
• Ensure processes to meet accelerated timelines are developed and implemented.	• Review and amend business associate agreements to ensure they align with the updated cybersecurity rules.	• Adopt advanced threat detection systems and improve vulnerability management practices.

3. Potential Impact of the Proposed Changes

Potential Positive Impacts

Clearer Definitions:

The proposed HIPAA security rule enhances data protection by making addressable safeguards mandatory and clarifying definitions, ensuring stronger compliance and improved data security.

Audit and Reporting:

The proposed rule mandates greater specificity in documenting the risk analyses and requires the development and revision of a technology asset inventory and a network map.

Enhanced Preparedness:

The new rule includes requiring annual written analyses and certifications of compliance with technical safeguards, conducted by qualified cybersecurity professionals.

Relevant Standards:

By updating definitions and revising implementation specifications to reflect changes in technology and terminology, the proposed rule ensures that cybersecurity measures remain relevant and effective in the face of evolving threats.

Potential Challenging Impacts

Increased Costs:

Implementing the new requirements, such as developing a technology asset inventory and network map, could lead to significant financial and human resource investments.

Vendor Management:

This could complicate vendor relationships and necessitate additional administrative efforts to manage and monitor these partnerships effectively and adding to costs.

Non-Compliance:

Organizations that fail to meet the new standards could face increased scrutiny and potential penalties, adding to the overall burden of compliance.

Overwhelming:

The need for extensive documentation, enhanced cybersecurity measures, and continuous monitoring could overwhelm smaller entities with limited resources, potentially impacting their ability to provide care and maintain operations.

4. Strategies to Prepare for Compliance

Privacy and Security

Risk Assessments

Regularly update technology asset inventories and network maps to identify potential vulnerabilities and ensure all ePHI is adequately protected.

Use NIST SP 800-30 and HHS Guidelines.

Enhanced Training

Provide ongoing training for staff on the latest cybersecurity threats and best practices to ensure everyone is aware of their role in protecting ePHI.

This is an organizational effort and not just Compliance and IT.

Vendor Oversight

Establish robust and continuous processes for evaluating and monitoring third-party vendors to ensure they comply with the updated standards and do not pose a risk to your organization.

Privacy and Security (*cont.*)

Allocate Resources

Budget for the financial and human resources needed to implement the new requirements, including hiring qualified cybersecurity professionals if necessary.

Incident Response Plans

Create and regularly update incident response plans to quickly and effectively address any security breaches or incidents .

Engage Leadership

Ensure that organizational leadership and key stakeholders are informed and involved in the compliance process, fostering a culture of security and accountability.

5. Q&A

Our Upcoming Healthcare Regulatory Round-Up Webinars

- **March 5, 11 am – 12 pm ET**
  Tightening Your Belt: Prepare for Site Neutral Payment Reforms

Thank you for attending!

PYA's subject matter experts discuss the latest industry developments in our popular Healthcare Regulatory Roundup webinar series twice each month.

For on-demand recordings of this and all previous HCRR webinars, and information on upcoming topics and dates, please follow the link below.

https://www.pyapc.com/healthcare-regulatory-roundup-webinars/

pyapc.com | 800.270.9629

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

A national healthcare advisory services firm providing consulting, audit, and tax services