online business systems

Navigating the 2025 HIPAA Security Rule Proposed Changes

Adam Kehler
Director of Health Cybersecurity

Results. Guaranteed.

AGENDA

01 HIPAA Security Rule

02 Proposed Administrative Changes

03 Proposed Technical Changes

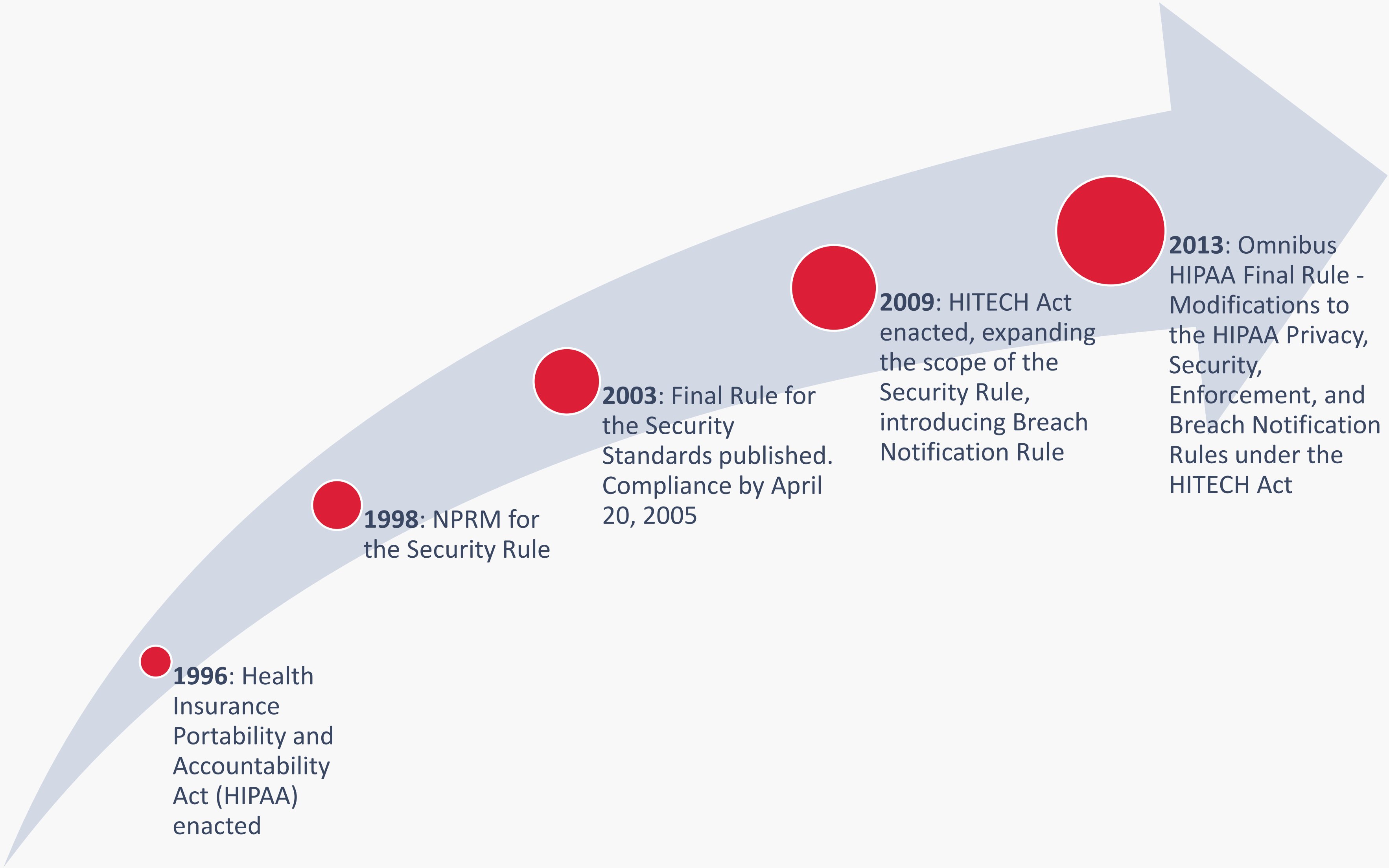
04 Proposed Continuity Changes

05 Implications

06 HIPAA, 405(d), CPG

07 Next Steps

HIPAA Security Rule History



1996: Health Insurance Portability and Accountability Act (HIPAA) enacted

1998: NPRM for the Security Rule

2003: Final Rule for the Security Standards published. Compliance by April 20, 2005

2009: HITECH Act enacted, expanding the scope of the Security Rule, introducing Breach Notification Rule

2013: Omnibus HIPAA Final Rule - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH Act

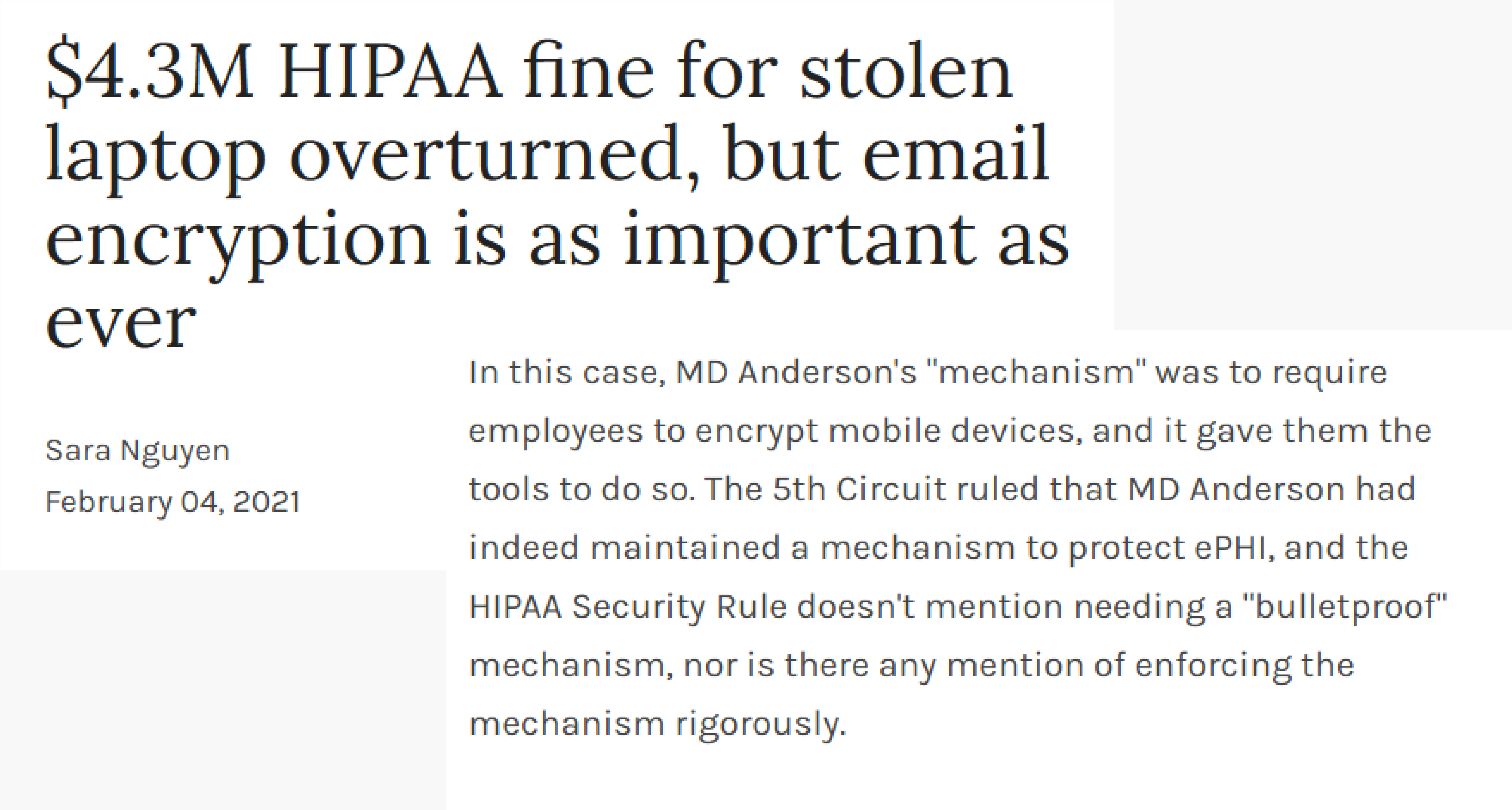
Jan 6, 2025
HIPAA Security Rule NPRM

HIPAA Security Rule Challenges

- Lacked the specificity to know when an organization is “compliant”
- Misunderstanding of “Addressable” vs “Required”
- Lack of understanding of “Security Risk Analysis”
- Increase in Third-Party Risk not fully addressed by Business Associate Requirements
- Some language is unenforceable

HIPAA Security Rule Challenges

PAUBOX



$4.3M HIPAA fine for stolen laptop overturned, but email encryption is as important as ever

Sara Nguyen
February 04, 2021

In this case, MD Anderson's "mechanism" was to require employees to encrypt mobile devices, and it gave them the tools to do so. The 5th Circuit ruled that MD Anderson had indeed maintained a mechanism to protect ePHI, and the HIPAA Security Rule doesn't mention needing a "bulletproof" mechanism, nor is there any mention of enforcing the mechanism rigorously.

online business systems

HIPAA Security Rule NPRM

- Notice of Proposed Rule Making (NPRM) for HIPAA Security Rule
  - Comment Period open for 60 days (ended March 7, 2025)
- Alignment with 405(d) and CPGs
- Emphasizes written documentation – especially of plans and analysis
- Removal of “Addressable” and “Required”
- Added specificity to the frequency of controls
- Updates definitions and revises implementation specifications to reflect changes in technology and terminology

HIPAA Security Rule – *Proposed Administrative Changes*

Technology asset inventory and network map

Maps your ePHI and how it flows throughout the environment. Updated annually.

Increased specificity of Risk Analysis

Leverages technology inventory and asset map, documents threats to CIA, vulnerabilities and “predisposing conditions,” risk levels

Notification Requirements

Require notification of certain regulated entities within 24 hours when a workforce member’s access to ePHI or certain electronic information systems is changed or terminated.

Compliance Audits

Regular review of P&P to see if they are working as intended

Third-Party Management

Require BAs verify they have deployed ”technology safeguards” by a “Subject Matter Experts” on an annual basis

Reviews and tests of security measures

Test for effectiveness at least every 12 months.

HIPAA Security Rule – *Proposed Technical Changes*

Requires Network Segmentation

Implement different network segments to separate sensitive data from other systems.

Extension to Portable Devices

Technical safeguard for portable devices extended to mobiles, tablets, and other portable devices.

Technical Security Enhancements

Require anti-malware protections, "extraneous" software removal, disable network ports in accordance with Risk Analysis.

Requires MFA to access ePHI

With limited exceptions.

Encryption

Requires encryption of data at rest and in transit.

Technical Testing

Require vuln scanning at least every 6 months and pen test every year.

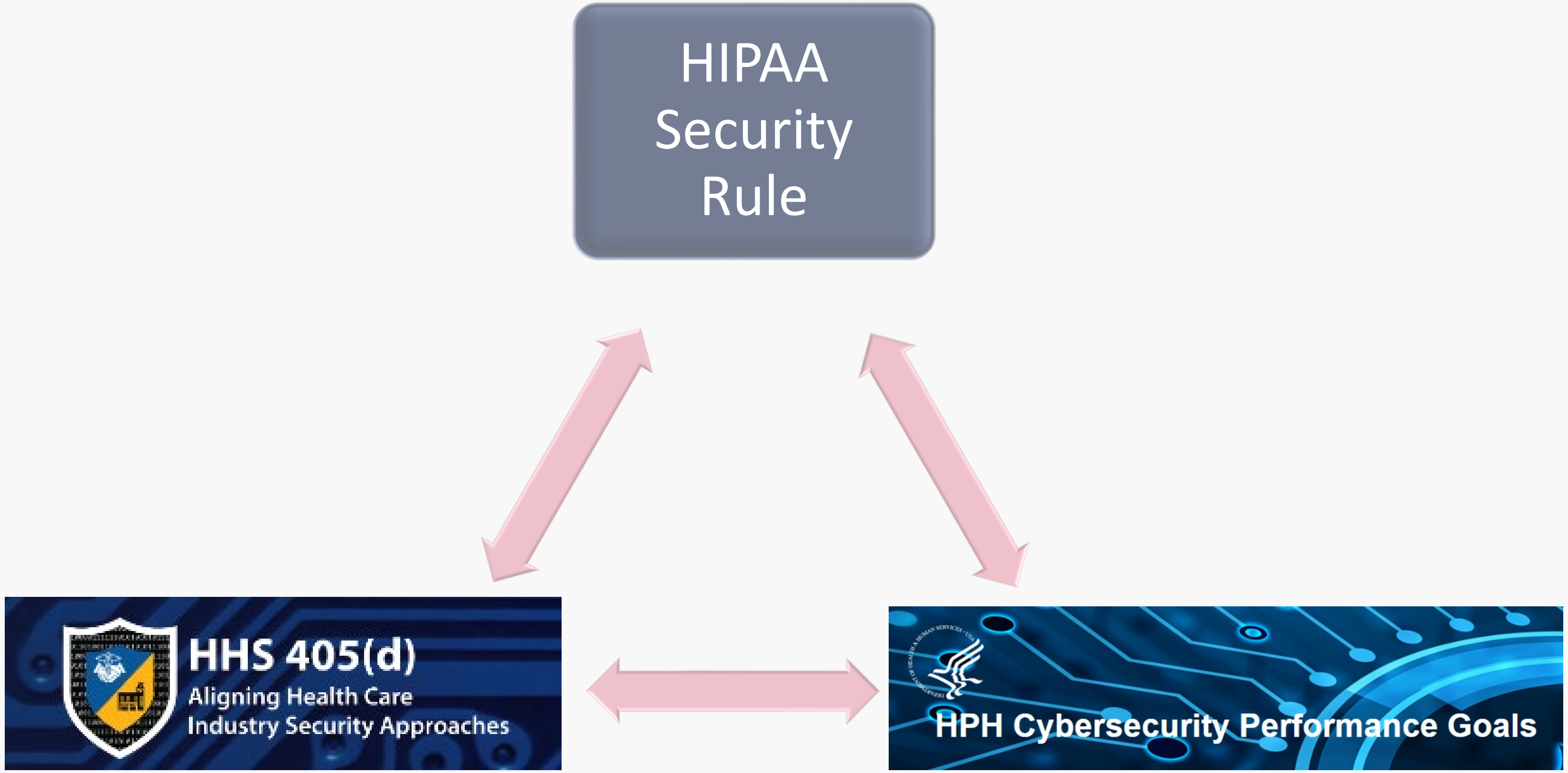
HIPAA Security Rule – *Proposed Continuity-Related Changes*

- Strengthens requirements for contingency planning and incident response to restore loss of data of “certain relevant” data within **72 hours**
- Requires organizations to perform an analysis of the relative criticality of their relevant electronic information systems and technology assets to determine the priority for restoration
- Requires written procedures for incident response, as well as testing, and revising incident response plans
- Requires separate technical controls for backup and recovery of ePHI and relevant electronic information systems.
- Require BAA to notify CE (and subcontracts to notify BAs) upon activation of contingency plans within 24 hours

HIPAA Changes - Implications

- Resource concerns (both time and people)
- Potential for new policies, procedures, and safeguards
  - Procurement considerations for new tools or services
    - Third-party management, technical testing, MFA, recovery
- Staff training and knowledge sharing
- Increased alignment with 405(d) and HPH Cyber Performance Goals

HIPAA, 405(d), & CPG



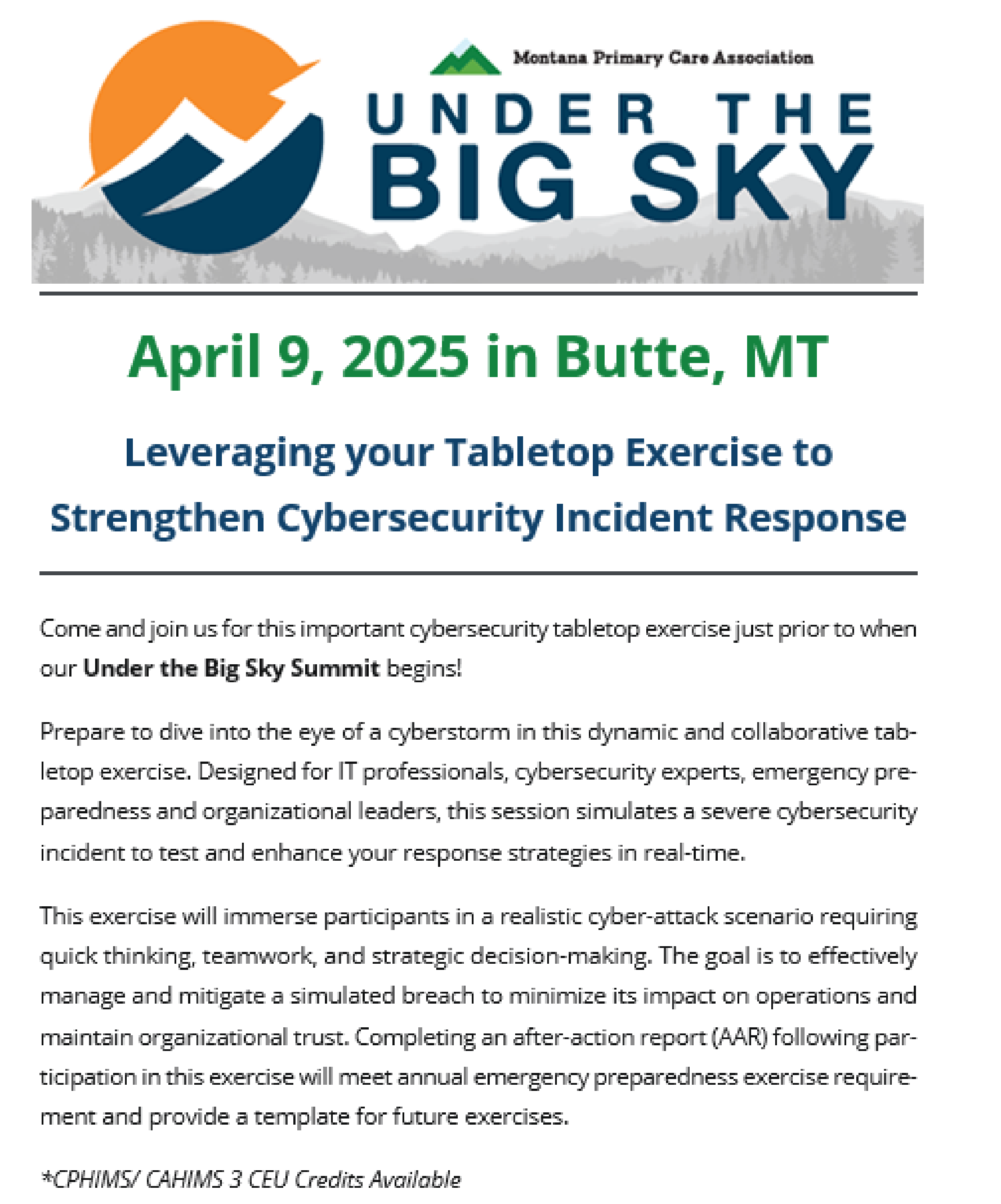
HIPAA Security Rule

HHS 405(d)
Aligning Health Care Industry Security Approaches

HPH Cybersecurity Performance Goals

Next Steps

- Build out security controls using 405(d) as a baseline
- Develop complete and accurate asset and data flow diagrams
- Collect and review inventory of Business Associates
- No need to jump now!
  - Final Rule will have changes
  - Compliance not required until after Final Rule is published
  - Will have time to comply
- Most changes align with industry security frameworks, so aligning with one will increase security posture and minimize required changes



Montana Primary Care Association

UNDER THE BIG SKY

April 9, 2025 in Butte, MT

Leveraging your Tabletop Exercise to Strengthen Cybersecurity Incident Response

Come and join us for this important cybersecurity tabletop exercise just prior to when our **Under the Big Sky Summit** begins!

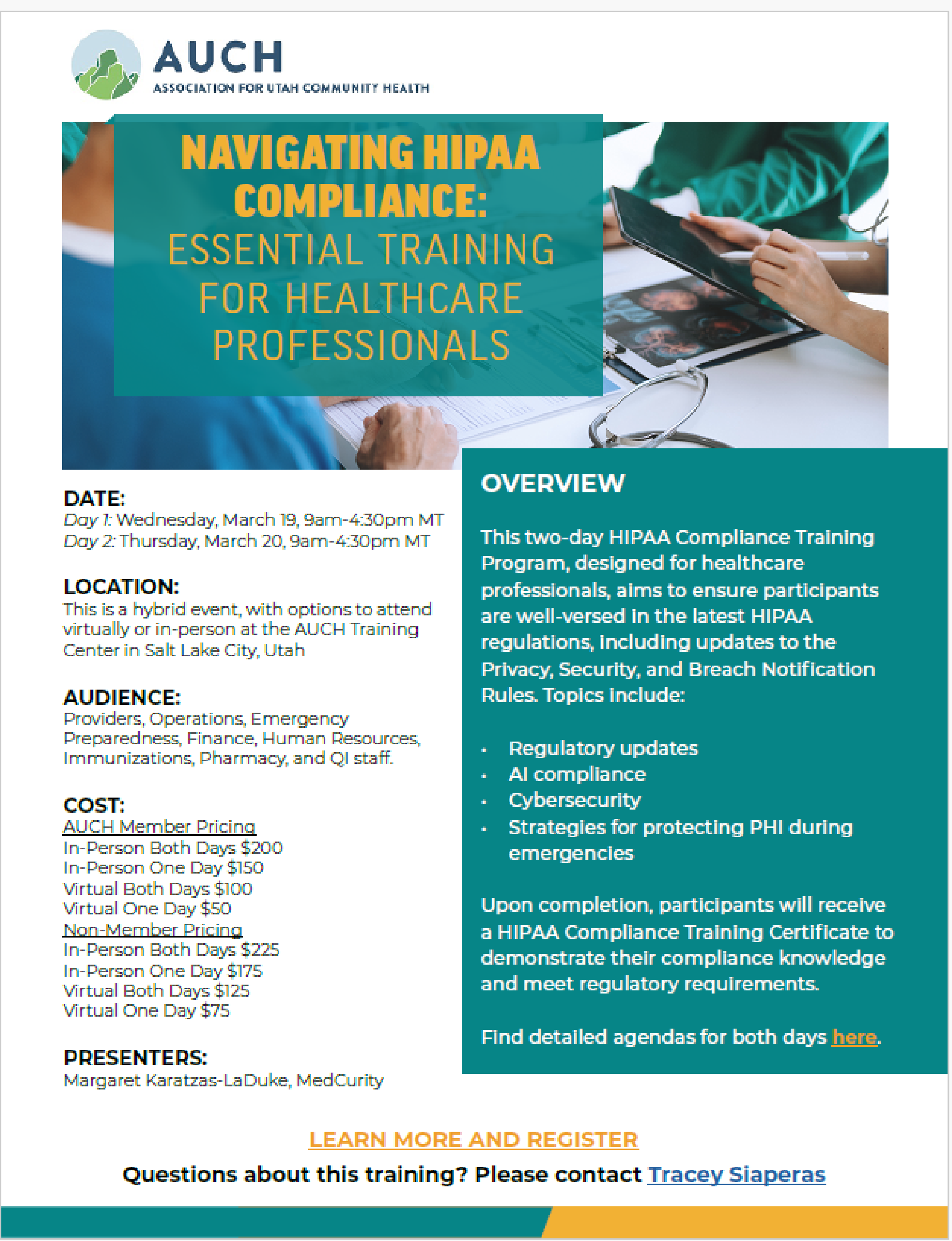
Prepare to dive into the eye of a cyberstorm in this dynamic and collaborative tabletop exercise. Designed for IT professionals, cybersecurity experts, emergency preparedness and organizational leaders, this session simulates a severe cybersecurity incident to test and enhance your response strategies in real-time.

This exercise will immerse participants in a realistic cyber-attack scenario requiring quick thinking, teamwork, and strategic decision-making. The goal is to effectively manage and mitigate a simulated breach to minimize its impact on operations and maintain organizational trust. Completing an after-action report (AAR) following participation in this exercise will meet annual emergency preparedness exercise requirement and provide a template for future exercises.

**CPHIMS/ CAHIMS 3 CEU Credits Available*

HCCN Health Center Controlled Network

MPCA



AUCH
ASSOCIATION FOR UTAH COMMUNITY HEALTH

NAVIGATING HIPAA COMPLIANCE: ESSENTIAL TRAINING FOR HEALTHCARE PROFESSIONALS

DATE:
Day 1: Wednesday, March 19, 9am-4:30pm MT
Day 2: Thursday, March 20, 9am-4:30pm MT

LOCATION:
This is a hybrid event, with options to attend virtually or in-person at the AUCH Training Center in Salt Lake City, Utah

AUDIENCE:
Providers, Operations, Emergency Preparedness, Finance, Human Resources, Immunizations, Pharmacy, and QI staff.

COST:
AUCH Member Pricing
In-Person Both Days $200
In-Person One Day $150
Virtual Both Days $100
Virtual One Day $50
Non-Member Pricing
In-Person Both Days $225
In-Person One Day $175
Virtual Both Days $125
Virtual One Day $75

PRESENTERS:
Margaret Karatzas-LaDuke, MedCurity

OVERVIEW

This two-day HIPAA Compliance Training Program, designed for healthcare professionals, aims to ensure participants are well-versed in the latest HIPAA regulations, including updates to the Privacy, Security, and Breach Notification Rules. Topics include:

- Regulatory updates
- AI compliance
- Cybersecurity
- Strategies for protecting PHI during emergencies

Upon completion, participants will receive a HIPAA Compliance Training Certificate to demonstrate their compliance knowledge and meet regulatory requirements.

Find detailed agendas for both days here.

LEARN MORE AND REGISTER

Questions about this training? Please contact Tracey Siaperas

HCCN
Health Center Controlled Network

MPCA

THANK YOU

Enjoy the rest of your day.