Montana Primary Care Association

Staying Ahead of Regulatory Changes:

Key Updates for Health Centers in 2025

> The latest HIPAA regulation changes, the impacts, what's next, and insight on protecting PHI in today's world.

Presented by:

MEDCURITY®

Overview

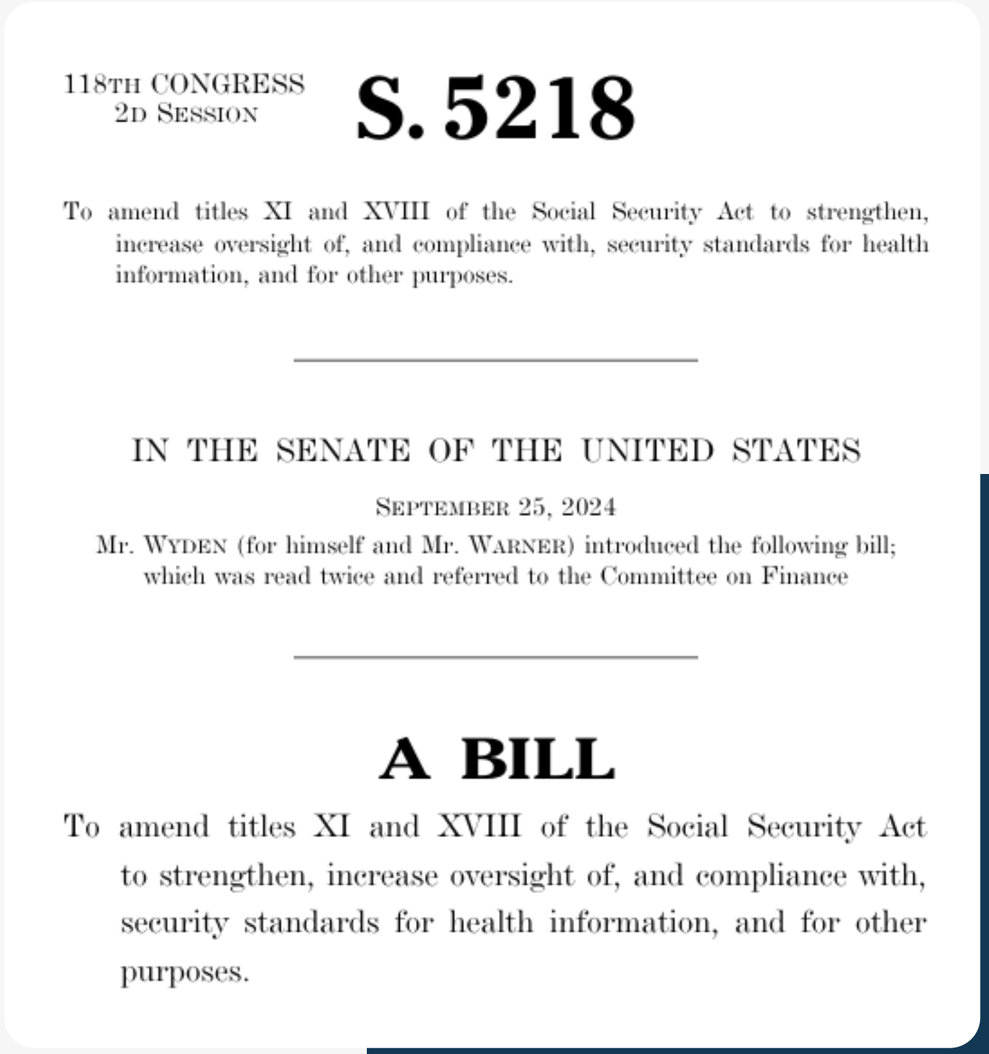
1. HISAA: 2024 Cybersecurity Bill
2. Proposed Security Rule Changes
3. Understanding Reproductive Rights and 42 CFR Part 2 SUD
4. Compliance Checklist
5. OCR News
6. Cybersecurity Performance Goals
7. Risk Mitigation

New Bill Introduced:

Health Infrastructure Security and Accountability Act of 2024

The Health Infrastructure Security and Accountability Act of 2024 (HISAA) is a legislative measure designed to enhance cybersecurity across the U.S. healthcare sector. The bill addresses the growing threat of cyberattacks, including ransomware incidents targeting hospitals, healthcare providers, and business associates handling sensitive patient data.

- **Strengthen Security Standards**
- **Increase Federal Oversight & Accountability**
- **Provide Funding & Incentives for Compliance**



118TH CONGRESS
2D SESSION

S. 5218

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

SEPTEMBER 25, 2024

Mr. WYDEN (for himself and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Finance

---

A BILL

To amend titles XI and XVIII of the Social Security Act to strengthen, increase oversight of, and compliance with, security standards for health information, and for other purposes.

TITLE I—STRENGTHENING AND INCREASING OVERSIGHT OF, AND COMPLIANCE WITH, SECURITY STANDARDS FOR HEALTH INFORMATION

SEC. 101. SECURITY REQUIREMENTS.

(a) IN GENERAL.—Section 1173(d)(1) of the Social Security Act (42 U.S.C. 1320d–2(d)(1)) is amended—

(1) in subparagraph (A), by redesignating clauses (i) through (v) as subclauses (I) through (V) respectively and indenting appropriately;

(2) by redesignating subparagraphs (A) and (B) as clauses (i) and (ii) respectively and indenting appropriately;

Proposed Requirements

In general, each covered entity and business associate shall at a minimum, on an annual basis —

- ☑ **Conduct and document a security risk analysis, including information on exposed to risk through business associates**
- ☑ **Document a plan for rapid, orderly resolution in the event of a technological failure of information systems**
- ☑ **Conduct a stress test to evaluate capabilities and planning necessary to recover essential functions.**
- ☑ **Provide a written statement signed by the CEO and chief information security officer (or equivalent) stating compliance with security requirements**
- ☑ **Publish publicly on a website whether minimum security requirements have been met (and enhanced, if applicable), and a copy of each sworn statement**

HIPAA Security Rule: Proposed Changes

HHS has proposed significant changes to the HIPAA Security Rule, aiming to strengthen cybersecurity protections for ePHI, some of the most notable include:

- **Removal of the distinction between "required" and "addressable" implementation specifications**
- **Enhanced Documentation and Security Risk Assessment Requirements**
- **Strengthened security measures (such as mandatory encryption and more robust technical controls)**
- **Improved incident response, such as requiring faster notification and enhanced contingency planning.**
- **Increased accountability with regular compliance audits**
- **Verification of Business Associate compliance with HIPAA**

Understanding Reproductive Health Privacy Rules

📅 When Did This Start?

The HIPAA Privacy Rule to Support Reproductive Health Care Privacy was finalized on April 22, 2024, by the Department of Health and Human Services (HHS) and the Office for Civil Rights (OCR).

- Final Rule Issued: April 22, 2024
- Effective Date: June 25, 2024

This timeline reflects a rapid regulatory response to concerns that personal reproductive health data could be misused, particularly following the overturning of Roe v. Wade in June 2022, which led to varying state laws regarding reproductive rights.

🔍 Why Was This Put in Place?

The rule was created to address growing concerns about the security and use of reproductive health data in a rapidly changing legal landscape.

- Protects Sensitive Reproductive Health Information
- Prevents Unauthorized Data Disclosures
- Strengthens Patient Privacy Protections

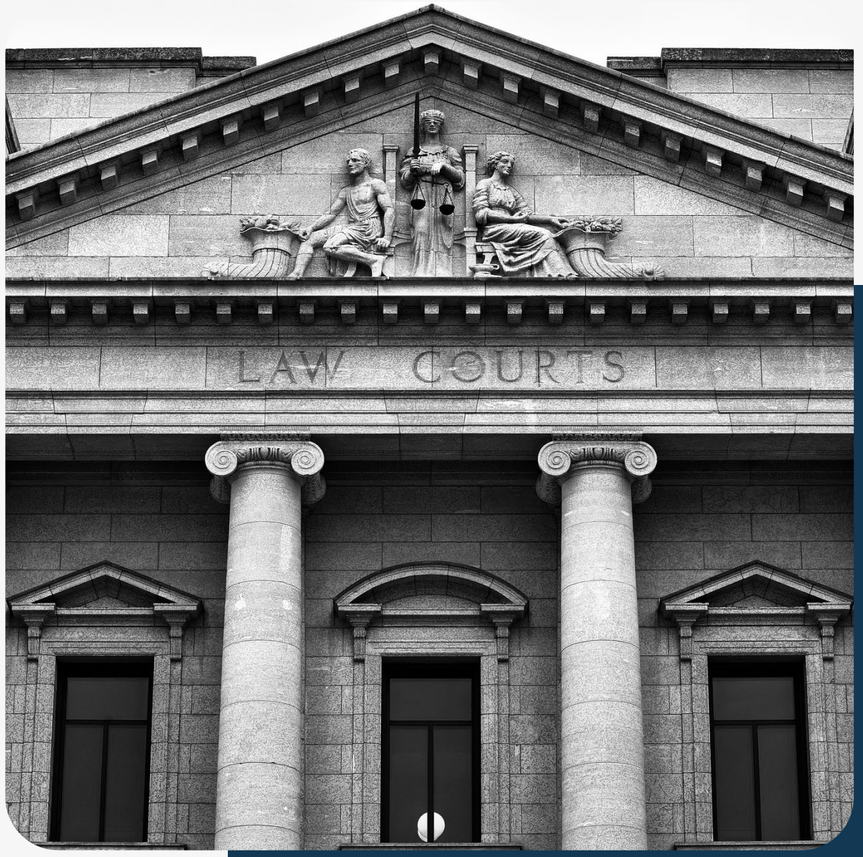
📢 The Bottom Line

This rule was introduced to ensure that reproductive health information remains private and protected, particularly in states with conflicting laws. Patients, providers, and business associates must now follow stricter guidelines to avoid unauthorized data sharing.

HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy

Key Federal Compliance Requirements

- **Prohibition:** Covered entities and business associates cannot use or disclose PHI for investigations or legal actions related to reproductive health care that is lawful under state or federal law.
- **Presumption of Lawfulness:** When a covered entity receives a request for PHI related to reproductive health care, the law presumes the care was lawful unless the requester provides substantial evidence proving otherwise.
- **Attestation Requirement:** Before disclosing PHI for oversight, legal, or law enforcement purposes, covered entities must obtain a signed attestation confirming the information will not be used for prohibited investigations.
- **Notice of Privacy Practices (NPP) Updates:** All Covered Entities must update their NPPs to reflect new federal reproductive health privacy protections.



HIPAA Privacy Rule Final Rule to Support Reproductive Health Care Privacy

Key State Compliance Requirements

- **Montana voters approved a constitutional amendment**

  In November 2024, Montana voters affirmed the right to abortion, strengthening state-level privacy protections for reproductive health care.

  This reinforces Montana's long-standing legal precedent that reproductive health decisions are protected under the state's constitutional privacy clause.

- **Montana's law aligns with the new HIPAA reproductive health rule**

  Montana's legal framework supports and complements the new HIPAA rule on reproductive health privacy.

  Providers and business associates must comply with both federal and state laws, ensuring reproductive health PHI remains protected.

Understanding 42 CFR Part 2 Changes

The recent updates to 42 CFR Part 2 were made to balance patient privacy protections with better care coordination for individuals receiving Substance Use Disorder (SUD) treatment. The goal is to reduce barriers that previously made it difficult for healthcare providers to share critical SUD treatment information while still maintaining strong privacy protections. These reasons include:

- **Aligning with HIPAA**
- **Improving Care Coordination**
- **Reducing Stigma While Protecting Privacy**
- **Addressing Public Health Needs**
- **Standardizing Enforcement**

Regulatory Changes: SUD Patient Records

The Confidentiality of Substance Use Disorder Patient Records (42 CFR Part 2) regulations were revised. Some key changes include:

- **Consent for Use and Disclosure, Consequences of refusal**
- **Restrictions on Use and Disclosure in Legal Proceedings**
- **Alignment with HIPAA: Enforcement and Breach Notification**
- **Permitted Redisclosure**
- **Public Health Disclosures**
- **Desegregation of SUD Records**
- **Updated Patient Rights & Notices**

What Can I Do to Make Sure My Organization Is Compliant?

- ☑ Review & Update Privacy Policies
- ☑ Train Staff on New Privacy & Disclosure Rules
- ☑ Update Notice of Privacy Practices (NPP)
- ☑ Ensure Proper Patient Consent Forms Are Used
- ☑ Implement Updated Breach Notification Procedures
- ☑ Review Business Associate Agreements (BAAs)
- ☑ Integrate SUD & Reproductive Health Records into EHR (If Applicable)
- ☑ Develop Procedures for Attestation & Legal Requests
- ☑ Monitor State & Federal Privacy Law Updates
- ☑ Conduct Regular Security & Privacy Risk Assessments

*“Healthcare entities need to ensure that they are **proactively monitoring** who is in their information systems, and that they have **backup procedures in place** to **be able to create exact copies of the electronic PHI** they hold, in the event health information is held for ransom or deleted.”*

MELANIE FONTES RAINER
OCR DIRECTOR

OCR Settles HIPAA Security Rule Investigation with USR Holdings, LLC

January 8, 2025

The OCR announced a $337,750 settlement to resolve a breach investigation concerning the deletion of ePHI by an unauthorized third party. Potential violations were:

- **Unauthorized third party/parties individuals were able to access a database containing the ePHI of 2,903 and delete**
- **Failure to conduct an accurate, thorough risk analysis**
- **Failure to regular review information system activity**
- **Procedures to create and maintain retrievable exact copies of ePHI were not established or implemented**

Essential: Cybersecurity Performance Goals

- Mitigate Known Vulnerabilities
- Email Security
- Multifactor Authentication
- Basic Cybersecurity Training
- Strong Encryption
- Revoke Credentials for Departing Workforce Members,
- Including Employees, Contractors, Affiliates, and Volunteers
- Basic Incident Planning and Preparedness
- Unique Credentials
- Separate User and Privileged Accounts
- Vendor/Supplier Cybersecurity Requirements

Enhanced: Cybersecurity Performance Goals

- [x] Asset Inventory
- [x] Third Party Vulnerability Disclosure
- [x] Third Party Incident Reporting
- [x] Cybersecurity Testing
- [x] Cybersecurity Mitigation
- [x] Detect and Respond to Relevant Threats and Tactics,
- [x] Techniques, and Procedures
- [x] Network Segmentation
- [x] Centralized Log Collection
- [x] Centralized Incident Planning and Preparedness
- [x] Configuration Management

Security Measures that Help Reduce RIsk

INTERNAL

- Employee Training
- Strong Access Controls
- Regular Security Audits
- Incident Response Plans
- Data Encryption
- Regular Backups

EXTERNAL

- Network Security Measures
- User Access Controls
- Data Protection
- Employee Training & Awareness
- Incident Response Planning (IRP)

Recommended Actions for Protecting Against Breaches

When the OCR investigates or audits an organization, they begin by asking for and reviewing security risk analysis reports and related documentation. Corrective action plans for violations often may include:

- **Workforce Training**
- **Security Risk Analysis and Risk Management**
- **Network Vulnerability Assessments**
- **Risk Management Plans**
- **Policy and Procedure Updates**
- **Third-Party Audits and Monitoring**
- **Business Associate Agreements**

Measures That Can Help Mitigate Risk

- Strong Authentication and Authorization
- Data Encryption
- Regular Security Audits
- Penetration Testing
- Clear and Transparent Data Use Policies
- Obtaining Informed Consent
- Continuous Monitoring and Risk Management
- Up-to-Date Business Associate Agreements
- Routine HIPAA and security awareness training

Security and Risk Management is an Ongoing Process

This is the best way to ensure PHI is protected. Also, covered entities and third-party vendors can both be held accountable for a breach of PHI.

Covered entities are ultimately responsible for the confidentiality, integrity, and availability of Protected Health Information (PHI).

Healthcare organizations can be fined for failing to adequately oversee their business associate and ensuring appropriate safeguards are in place, regardless of who is at fault.

CONTACT OUR TEAM

Ready to conduct your annual security risk analysis?

www.medcurity.com

Get in Touch

509-867-3645

support@medcurity.com

meln@medcurity.com

Any Questions?

Thank you!

MEDCURITY®

meln@medcurity.com

Upcoming Events

Navigating the 2025 HIPAA Security Rule Proposed Changes

As healthcare technology evolves, so do the regulations that govern patient data protection. Join Online Business Systems for an in-depth webinar with Adam Kehler from Online Business Systems that explores the proposed changes to the HIPAA Security Rule in 2025. Whether you are a healthcare provider, IT professional, or compliance officer, this session will provide the latest updates on how these changes will affect your organization's security practices and patient data privacy.

Wednesday, March 12th at 11:00 a.m. **REGISTER**

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

2025 Montana Policy & Issues

Helena, MT

March 18th 6pm – March 19th 5pm

Two ways to register!

https://cvent.me/3e1BOP

Montana Primary Care Association