

Center for Improvement

CIHQ

in Healthcare Quality

HIPAA Final Rule Update

What's Enforceable, What's in Flux

October 22, 2025

Carrie Levake - RN, BSN, HACP-CMS
CIHQ Generalist Surveyor

Presentation Objectives

-  **Spot the Shifts:** Identify finalized vs. proposed HIPAA changes from 2024–2025, including 42 CFR Part 2 alignment and vacated rules.
-  **Decode the Impact:** Understand how changes affect documentation, redisclosure, and breach handling across departments.
-  **Prep for Compliance:** Recognize deadlines and operational updates needed for February 2026 readiness.
-  **Train with Tools:** Explore mock survey Q&A, crosswalks, and real-world examples to support staff education.
-  **Anticipate What's Next:** Preview upcoming cybersecurity and privacy proposals—and what to flag for IT, HIM, and policy teams.

HIPAA Final Rule (2024–2025) – Quick Overview

Why It Was Created

-  **Protect sensitive health data**
-  **Improve cybersecurity safeguards**
-  **Support safe and efficient data sharing across system.**

What It Aims to Do

-  **Align behavioral health records with HIPAA**
 - Enables smoother care coordination across providers & systems
-  **Strengthen cybersecurity rule**
 - Improves encryption, access controls, and breach response protocols
-  **Update privacy language to support CMS data-sharing goals**
 - Simplifies how PHI moves between hospitals, insurers, and platforms
 - Clarifies redisclosure rules and consent boundaries for interoperability

What's New vs. What's Staying the Same



Staying the Same:

- Core Privacy Rule protections
- Minimum necessary standard
- Patient rights to access records



Changing:

- Consent language for redisclosure
- Security Rule technical safeguards
- Behavioral health record alignment

Departmental Touchpoints for Final Rule

 **Clinical Staff:** Consent handling, verbal PHI disclosures

 **IT Teams:** Encryption, access controls, breach response

 **Policy Teams:** Documentation workflows, redisclosure protocols

 **Education/Training:** Staff prep, updated scripts, mock survey tool

Timeline of Key Changes

Date	Action	Status
2024	Reproductive Health Privacy Rule issued	✗ Vacated (2025)
2024	42 CFR Part 2 Alignment Finalized	✓ Finalized
Early 2025	Security Rule Modernization (Proposed)	⌚ Pending
Mid 2025	Privacy Rule Adjustments (Proposed)	⌚ Pending

Reproductive Health Rule – Vacated

This rule was designed to prevent PHI from being used in investigations related to reproductive care. Basically, the rule had required providers to get a signed statement (attestation) before sharing patient info related to legally provided reproductive services. But it's been vacated nationwide!

 **Vacated nationally in June 2025 by federal court**
( **Purl v. HHS, N.D. Tex., June 18, 2025**)

The court said this rule went too far and conflicted with state laws—especially in states that require reporting certain types of care

***ACTION: Remove any attestation language from your policies and workflows—especially those tied to law enforcement or oversight disclosures.**

42 CFR Part 2 Alignment – What It Means



Compliance deadline: February 2026

Substance use disorder (SUD) records now follow HIPAA rules

- This means fewer barriers to sharing records for treatment, payment, and operations



Consent is easier

- No need for separate consent every time



Redisclosure is allowed

- If a provider gets SUD records under HIPAA rules, they can share them again—just like other health records. *Example: If a hospital receives SUD records for treatment, it can now share them with a specialist under HIPAA rules.*



Action: Begin documentation crosswalks

- Compare old vs. new consent language
- Update redisclosure policies
- Train staff on what's change

42 CFR Part 2 – Key Updates Recap

One-Time Consent

- Patients can sign **one form** that covers future use for treatment, billing, and operations
- No need for repeated consent

Redisclosure Allowed

- HIPAA-covered entities and business associates can share SUD records as needed
- Same rules as other PHI

Public Health Sharing

- De-identified data can be sent to public health agencies
- No patient consent required

Court Use Restrictions

- SUD records need patient consent or a court order before use in legal cases

Official Guidance

- HHS Fact Sheet: [HHS.gov – 42 CFR Part 2 Final Rule](https://www.hhs.gov/42-cfr-part-2-final-rule)

Compliance Pathways – 42 CFR Part 2 Final Rule

1. Update Consent Forms – What That Means

One form covers future care

Patients only need to sign one consent form that allows their substance use records to be used for treatment, billing, and care coordination—no need to sign again each time.

Patients can change their mind

The updated form must explain how patients can take back their consent if they choose to later.

Wider sharing options

The form can now name groups of people (like “billing staff” or “referring providers”) instead of listing every person by name.

Extra protection for counseling notes

If a provider writes private therapy-style notes during substance use counseling, those need separate consent—just like psychotherapy notes under HIPAA.

Compliance Pathways (Continued)

2. Update How Records Can Be Shared

Who can share records now?

Hospitals, clinics, and their business partners (like billing companies) can now share substance use records under HIPAA rules—just like other health information.

What needs to go with the records?

When sharing these records, include a copy or summary of the patient's consent so everyone knows what's allowed.

What must be protected?

Add a reminder to all shared records:

“42 CFR Part 2 prohibits unauthorized use or disclosure.”

– This helps prevent misuse and keeps everyone compliant.

Compliance Pathways (Continued)

3. What to Do If Substance Use Records Are Mishandled:

Follow HIPAA Breach Rules

If substance use disorder (SUD) records are lost, shared by mistake, or accessed without permission—it's treated like a HIPAA breach.

Train Staff to Speak Up

Staff must know how to report any unauthorized use or sharing of SUD records

*This includes verbal disclosures, emails, or system access

Update Your Internal Steps

Review what your team considers a “breach”

*Make sure your reporting and escalation process includes SUD records

*Add SUD examples to your training and incident response guides

Compliance Pathways (Continued)

4. Update Policies, Procedures, and Audit Tools **Make sure your internal documents match the new 42 CFR Part 2 rule!**

Policy Manuals

- Remove outdated language that blocks redisclosure
- Add new guidance aligned with HIPAA and Part 2
- Include required consent language for SUD records

Staff Training Guides

- Explain how one-time consent works
- Clarify when redisclosure is allowed
- Add examples of what counts as a breach

Compliance Checklists & Audit Tools

- Ensure tools check for proper consent
- Include redisclosure tracking steps
- Flag missing or outdated forms during audits

Compliance Pathways (Continued)

Using Crosswalks to Update Your Documents

Compare old vs. new to stay compliant!

Use a simple format:

Old Rule → New Rule → What to Fix

*Then apply it to policies, training, and audit tools **before**
February 16, 2026*

Policy Language Example

- Old: “Redisclosure of SUD records is prohibited under all circumstances.”
- New: “Redisclosure is permitted under HIPAA if the patient’s consent includes redisclosure language.”

...Another Crosswalk Example

Current Practice	New Requirement	Gap	Action Needed
Consent form allows one-time disclosure	New rule allows broader redisclosure with patient consent	Form is too restrictive	Update consent form language and retrain staff

Compliance Pathways (Continued)

Step 5: Educate Staff on the New Rules

 *Use real tools and examples to make training stick!*

How to Train on the New Consent Rules

Example: Show a side-by-side of old vs. new consent forms

Tool: Use a visual crosswalk with callouts for “*What Changed*”

Tip: Include a sample one-time consent form in your training packet.

Compliance Pathways (Continued)

How to Explain Redisclosure

 ***“Can I share this SUD record again?”***

Example: Walk through a scenario: “Can I send this record to billing?”

Tool: Create a decision tree or flowchart for redisclosure steps.

“Is it a Part 2 record?” → “Do we have consent?” → “Does consent allow redisclosure?” → “Is billing HIPAA-covered?”
→  **Send it**

Tip: Add redisclosure examples to your mock survey
Q&A

Compliance Pathways (Continued)

How to Teach Breach Handling

Example: “A staff member emailed SUD records without consent—what now?”

Tool: Use a laminated breach response checklist at nurse stations

1.  **Stop and assess – Was the record shared without proper consent?**
2.  **Secure the record – Remove from email, shred printed copies, or lock access**
3.  **Notify your supervisor immediately**
4.  **Complete the incident report – Include what was shared, when, and to whom**
5.  **Send to Compliance or Privacy Officer within 24 hours**
6.  **Do not attempt to fix it alone – Follow official breach protocol**

Tip: Include breach scenarios in your annual HIPAA refresher

Compliance Pathways (Continued)

How to Verify Part 2 Program Status

***Before redisclosing SUD records, check if the provider is covered by 42 CFR Part 2*

Why It Matters

- Only records from **Part 2 programs** are protected under the new rule. If you redisclose without checking, it could trigger a **HIPAA breach!**

How to Verify

- Use SAMHSA's official Treatment Locator: <https://findtreatment.gov>

Steps:

- Search by provider name, city, or ZIP code
- Look for programs offering SUD treatment, detox, or MAT (Medication-Assisted Treatment).
- Confirm federal assistance (e.g., Medicare, Medicaid, grants)

Tip: Add a link or QR code to your handouts for quick access

Security Rule Modernization (Proposed)

What's Changing (Proposed Updates)

- Stronger requirements for encryption, access controls, and breach response
- Clearer rules for role-based access—who can see what, based on job duties
- More detailed expectations for incident response plans and breach reporting

What You Need to Know

- These changes will affect IT, Risk, HIM, and frontline workflows
- Staff access must be justified by role—“curious clicks” could trigger violations
- Breach response must be documented, rehearsed, and fast
- **Final Rule expected in 2026—but prep starts now**

Action Plan

- Flag this for IT and Risk teams

Privacy Rule Adjustments (Proposed)



What's Changing (Proposed Updates)

- Easier sharing of patient data between hospitals, insurers, and health systems
- Smoother, more consistent data flow—while maintaining privacy protections
- Proposed updates aim to reduce friction in care coordination and billing



What You Need to Know

- ***Changes are still in draft form—not final yet***
- May impact how your organization documents, stores, and shares patient records
- Could affect frontline workflows, HIM protocols, and policy language



Action Plan

- Flag for Policy and HIM teams

! Real-World HIPAA Violations – What Went Wrong

Examples, lessons learned, and potential penalties under the Final Rule.....

Example 1: Unauthorized Access by Staff

What Happened: A hospital employee accessed SUD records without a treatment relationship

Violation: HIPAA + 42 CFR Part 2 breach

Final Rule Tie-In: Reinforces role-based access—staff must only access data needed for their job

Potential Penalty:  **Up to \$100,000 per violation**

Criminal charges possible for willful misuse

 Action: Audit access logs & retrain on role-based permissions

! Real-World HIPAA Violations – What Went Wrong (Continued)



Example 2: Redisclosure Without Consent

What Happened: A behavioral health clinic shared SUD records with a billing vendor without redisclosure language in the consent.

Violation: Redisclosure without proper authorization

Final Rule Tie-In: Redisclosure is allowed only if consent includes redisclosure language

Potential Penalty: 💰 **\$10,000–\$50,000 per record**



Corrective action plan required by OCR



Action: Use updated consent templates and decision trees

⚠️ Real-World HIPAA Violations – What Went Wrong (Continued)



Example 3: Emailing Records to the Wrong Recipient

What Happened: A nurse emailed a patient's SUD summary to the wrong provider

Violation: Breach of protected health information

Final Rule Tie-In: SUD breaches must be treated as HIPAA breaches

Potential Penalty: 💰 **\$141 to \$2.1 million per violation**, depending on severity and intent



Mandatory breach notification and retraining



Action: Use laminated breach response checklists and secure messaging protocols



Compliance Resources



OCR – HIPAA & Privacy Rule Updates

- **Website:** <https://www.hhs.gov/hipaa>
- **Subscribe to Updates:** Scroll to bottom of page for email alerts



CMS – Interoperability & Data Exchange

- **Website:** <https://www.cms.gov>
- **Interoperability Hub:**
<https://www.cms.gov/interoperability>
- **Final Rules & Proposals:**
<https://www.cms.gov/Regulations-and-Guidance>