PRIVACY + SECURITY FORUM | SPRING ACADEMY 2026

Privacy Under Pressure

Part 2 at the Intersection of Law, Technology, and Care Delivery

42 CFR Part 2 after the 2026 compliance deadline

May 7, 2026 | Washington, DC

Panelists

1

Brad Rostolsky

Shareholder
Greenberg Traurig

2

Trinity Car

Assistant General Counsel
Wolters Kluwer

3

Nicole Epstein

System Privacy Officer
University of Missouri Health Care

4

Roshal Marshall

Chief Privacy Officer
Verily

Why this conversation matters now

Timing

The deadline has passed

Compliance with the 2024 Final Rule was required by February 16, 2026. The question is no longer “what is coming?” but “how are we operating?”

Operations

Risk moved into workflows

Consent, redisclosure, data routing, analytics, and breach response now have to work inside EHRs, HIEs, apps, vendors, and care teams.

Pressure points

The hard cases are mixed cases

The toughest calls arise when privacy law meets mandated reporting, employers, licensing boards, courts, public health, and product design.

Roundtable premise

Part 2 is now less siloed from HIPAA, but it is still not “just HIPAA.”

The practical challenge is designing governance that protects patients while allowing appropriate care coordination and data use.

Roadmap for the discussion

1

Baseline

What Part 2 protects and who has to care

2

2024/2026 changes

Consent, redisclosure, notices, enforcement

3

Operational pressure points

Segmentation, secondary use, vendors, analytics

4

Scenarios

CPS/law enforcement, employers, boards, courts

5

Takeaways

Controls that reduce risk without blocking care

Part 2 in one slide

Core purpose

Encourage people to seek SUD treatment without fear that treatment information will be used against them.

That policy concern still drives the modern rule, even after HIPAA alignment.

Protected data

What it protects

Patient-identifying SUD diagnosis, treatment, or referral records that are subject to Part 2.

Obligated actors

Who it follows

Part 2 programs and, in many cases, lawful holders that receive Part 2 records.

Not just HIPAA

How it differs from HIPAA

Written consent and proceeding-use limits remain central. Alignment did not erase Part 2's heightened protections.

Governance

Why privacy/security teams care

The rule intersects with EHR configuration, HIEs, apps, analytics, breach response, subpoenas, and vendor governance.

Scope: follow the function and the data

PART 2 PROGRAM ANALYSIS

1. Is the organization federally assisted?
2. Does the program provide SUD diagnosis, treatment, or referral?
3. Is it a general medical facility with an identified SUD unit or personnel?
4. Is the information created, received, or maintained by that program?
5. Is the recipient now a lawful holder of Part 2 records?

COMMON SCOPE TRAPS

- Assuming every SUD reference is Part 2 data
- Assuming HIPAA permission automatically solves Part 2
- Missing data inherited from a Part 2 program
- Treating a vendor workflow as only a technical issue
- Ignoring state law, contract, or accreditation overlays

What counts as a Part 2 record?

Patient-identifying

The trigger

Information that identifies a patient as having or having had a substance use disorder, or as receiving SUD diagnosis, treatment, or referral for treatment.

Provenance

The source matters

The analysis depends on who created, received, or maintains the record - and whether the recipient is a lawful holder of Part 2 records.

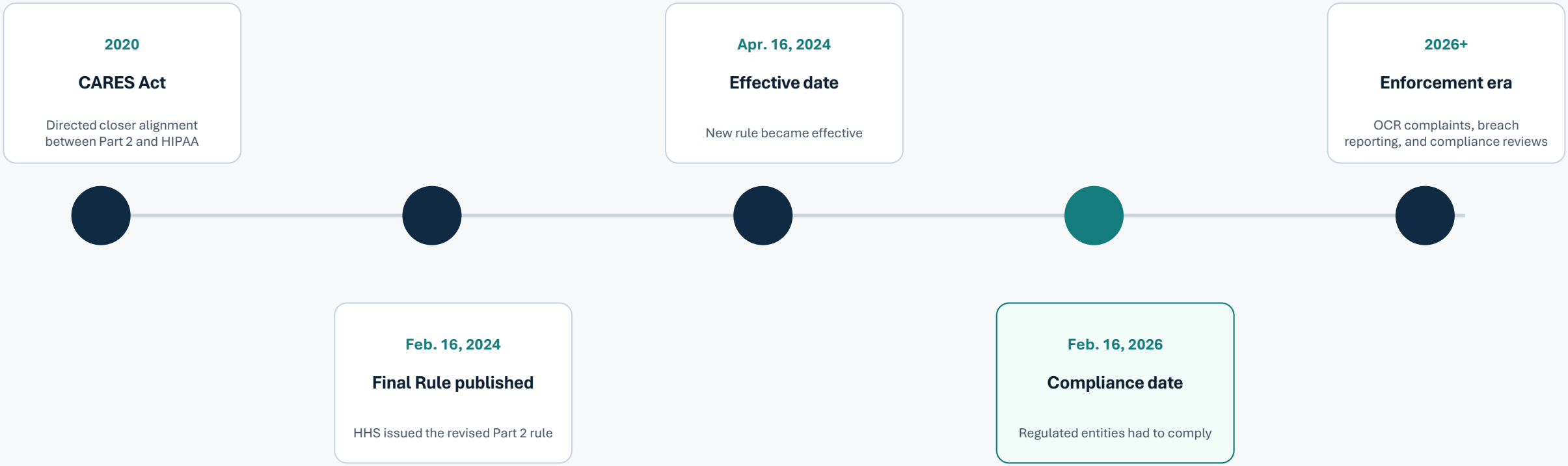
Practical documentation rule

Map the data path before applying the permission.

Origin -> consent basis -> recipient -> intended use -> redisclosure risk -> proceeding-use restrictions

Not every note about SUD in a general medical record becomes a Part 2 record - but imported Part 2 data can carry Part 2 obligations.

Timeline: from alignment to operational reality



Bottom line: the compliance project is now an operating model project.

The 2024 Final Rule: what changed most

Change 1

Single TPO consent

One written consent can cover future treatment, payment, and health care operations uses/disclosures.

Change 2

Redisclosure flexibility

HIPAA covered entities and business associates receiving records under TPO consent can redisclose under HIPAA.

Change 3

Proceeding-use limits

Part 2 records remain specially protected in proceedings against the patient absent consent or a Part 2 court order.

Change 4

Breach and enforcement

Breach notification requirements and HIPAA-style enforcement now apply.

Change 5

Patient rights/notices

Part 2 notice obligations are aligned more closely with HIPAA Notice of Privacy Practices concepts.

Change 6

Public health

Disclosure to public health authorities is permitted without consent only with HIPAA-standard de-identification.

Single TPO consent: relief and limits

WHAT IT PERMITS

- A single consent for all future uses and disclosures for treatment, payment, and health care operations
- A more workable basis for care coordination and related operational sharing
- A cleaner pathway for HIPAA covered entities and business associates to use records under HIPAA after receipt

Design question: who is in the recipient class, and does the language match the workflow?

WHAT IT DOES NOT DO

- It does not eliminate the need for written consent/QSOA for TPO sharing
- It does not cover SUD counseling notes
- It does not create a blanket waiver for proceedings against the patient
- It does not override stricter state law or narrow organizational policies

Practical takeaway: consent forms need to be legally valid and operationally readable.

Redisclosure: easier for TPO, still bounded

Use limits

Guardrail 1

Proceedings against the patient remain specially restricted. Do not treat TPO redisclosure as a green light for subpoenas, licensing actions, custody disputes, or law enforcement requests.

Source path

Guardrail 2

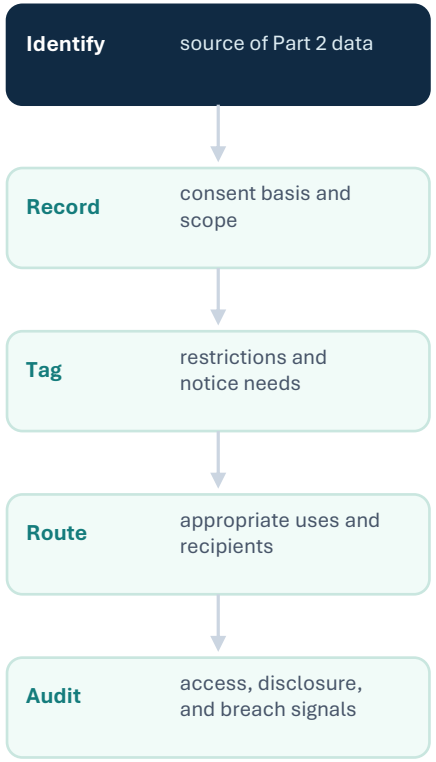
Know whether the record was received under a TPO consent, another consent, QSO arrangement, audit/evaluation pathway, court order, or another exception.

Operations

Guardrail 3

Notice language, data tags, access controls, and staff training need to travel with the operational flow.

Data segmentation and technology design



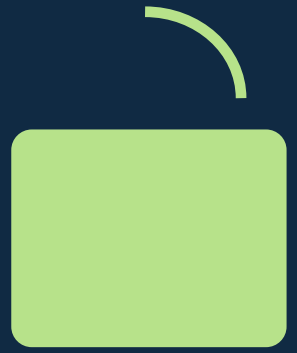
DESIGN PRINCIPLE

Segmentation is no longer the only answer, but traceability still matters.

- Classify data by origin, not only by diagnosis code
- Translate consent language into system-readable rules where possible
- Build exception workflows for subpoenas, boards, law enforcement, and courts
- Tie analytics and secondary uses to a documented legal basis
- Train privacy, HIM, product, and clinical teams on the same decision tree

Question for the room: Where does your organization lose Part 2 context today?

SUD counseling notes: separate treatment



Separate consent

A broad TPO consent does not cover SUD counseling notes.

Definition

What they are

Notes recorded by a Part 2 program provider who is an SUD or mental health professional documenting or analyzing counseling session content, kept separate from the rest of the record.

Risk

Why they matter

They are treated much like psychotherapy notes: high sensitivity, separate consent, limited exceptions, and a need for clear separation from ordinary treatment records.

Action

Storage/classification

Decide whether such notes exist, where they live, who can access them, and how the consent workflow differs from standard Part 2 TPO consent.

Enforcement, breaches, and notices

1

OCR enforcement

OCR administers and enforces Part 2; complaints may be filed for noncompliance.

2

Breach reporting

Part 2 programs must report breaches of unsecured Part 2 records.

3

Penalty alignment

The Final Rule aligns Part 2 penalties with HIPAA-style civil/criminal enforcement.

4

Notice updates

Part 2 programs and certain HIPAA entities must update patient notice practices.

Post-deadline question: Can you prove the rule is operating in practice?

Public health, analytics, and secondary use

PUBLIC HEALTH

Disclosure without patient consent to public health authorities is permitted only if the records are de-identified under HIPAA standards.

- De-identification is not a label - it is a standard
- Re-identification risk belongs in governance
- Consider state and program-specific reporting laws

SECONDARY USE

The big governance question is whether the use is supported by consent, HIPAA, Part 2, de-identification, QSO/vendor terms, research rules, or another path.

- Model training and analytics
- Quality improvement and care management
- Product development and vendor access
- Public health and population health reporting

Decision lens for Part 2 applicability

1. **Is it Part 2 data?** — Identify origin, holder, and what the information reveals.
2. **Who is asking?** — Care team, employer, board, court, law enforcement, public health, vendor?
3. **What is the legal path?** — Consent, TPO, QSO, audit/evaluation, emergency, mandated report, court order, de-identification?
4. **Will it be used against the patient?** — Proceeding-use restrictions are the recurring red flag.
5. **What is the minimum disclosure?** — Narrow the recipient, purpose, information, duration, and documentation.

Scenario 1: CPS and law enforcement

A Part 2 program participant/parent discloses keeping illegal drugs in a home where minor children reside.

Does the provider have an obligation to report to child protective services or law enforcement?

Scenario 2: Employer Return-To-Work Form

An employer asks the provider to complete a return-to-work document so the participant can resume driving as part of the job.

What written permissions are needed before the provider completes and sends the form?

Scenario 3: Professional Licensing Board

A physician, pharmacist, nurse, PT, or other licensee participates in a Part 2 program. A licensing board requests information.

What can be reported voluntarily, and what happens if the board later issues a subpoena?

Scenario 4: Court/custody Request

A court representative asks whether an individual continues to participate successfully in a Part 2 program for a child-custody evaluation.

Does court-ordered treatment change the permissions needed?

Scenario 5: Impact on Treatment of not getting a Part 2 Consent

A patient receives treatment from a hospital's Part 2 Program, but the patient will not sign a Part 2 consent. The patient also receives treatment from other physicians employed by the hospital and independent community physicians.

- A non-Part 2 provider employed by the hospital views the Part 2 records. Is this ok? What about an independent provider?

- The patient is on vacation, and a treating doctor accesses the Part record through an HIE. Is this ok?

Key takeaways for privacy and security teams

Takeaway

1. Treat Part 2 as a data-governance problem

Forms matter, but the hard work is tracing Part 2 data across EHRs, HIEs, vendors, analytics, legal requests, and breach workflows.

Takeaway

2. Update consents and notices for real workflows

TPO consent, redisclosure notices, SUD counseling notes, patient notices, and specific non-TPO disclosures need to fit how the organization actually operates.

Takeaway

3. Build a legal-request playbook

Boards, courts, CPS, law enforcement, and employers should not be handled from scratch every time.

Prepare for the eventual OCR inquiry, and not just in connection with a Breach.

30-day practical checklist

1. Refresh consent templates 2. Map Part 2 data flows 3. Confirm SUD counseling notes workflow 4. Update notices 5. Train legal-request intake 6. Test breach response