42 CFR Part 2 Compliance Checklist

NOTE! This checklist includes both HIPAA and 42 CFR Part 2 compliance requirements. If your organization is a Part 2 Program but *not* a HIPAA Covered Entity, some items below may not apply. Cross-references to "Tools," "Forms." "Policies" etc., correspond to the "Part 2 Program HIPAA Helper" resource which can be accessed here: Legal HIE Subscription (*subscription fee is applicable*).

Part 2 Applicability Assessment

❒ **Determine if your organization operates a Part 2 Program**. (*Check one*)
- ☐ Entire organization is the Part 2 Program (e.g., SUD treatment center).
- ☐ Dedicated unit is the Part 2 Program (e.g., inpatient SUD unit in a general hospital)
- ☐ Dedicated health care provider(s) are subject to Part 2 (e.g., one practitioner providing medication assisted treatment with Suboxone to patients)

TIP: Not sure if certain functions at your organization are covered by 42 CFR Part 2? Consult SAMHSA/ONC's resource "***Disclosure of Substance Use Disorder Records: Does Part 2 Apply to Me***?" *See* Tool 1B

❒ **Document Part 2 Program designations**. If the entire organization does *not* function as the Part 2 Program, identify which units/departments fall ***outside*** the Part 2 Program (e.g., emergency department, ICU, etc) and the legal basis for any disclosures made to non-Part 2 components (e.g., Part 2 Consent, Part 2 Exception). *See* Tool 1D

❒ **Part 2 Holder Status.** Assess whether your organization qualifies as a "Part 2 Holder," meaning any individual or entity that receives or maintains Part 2 Records from a Part 2 Program and is subject to Part 2's redisclosure restrictions. A Part 2 Holder is *not* a Part 2 Program but must comply with all applicable Part 2 protections for any Part 2 Records it receives, including scope of use pursuant to consent, redisclosure limitations (e.g., civil, criminal, administrative, or legislative proceeding against the patient), and certain patient rights (i.e. consent revocation).

HIPAA Applicability Assessment

❒ **HIPAA "Covered Entity" Activities & Functions.** Complete an assessment of all organizational functions, services, and departments for HIPAA Covered Entity status. *See* Tool 1C

❒ **Hybrid Entity Designation.** Determine whether your organization is a "single" HIPAA Covered Entity or a "Hybrid Entity". If applicable, complete the hybrid designation. *See* Tool 1D

Data Mapping

(*strongly recommended*)

❒ Complete comprehensive Data Mapping of how Part 2 Records are *created*, *stored*, *used*, and *disclosed*. This Data Mapping helps inform all downstream policies, consent design, EHR build, HIE participation, and breach-analysis requirements. *Data Mapping should include*:

❒ ***Source* Identification**
- ☐ Identify all systems where Part 2 information (diagnosis, treatment notes, medication list including MAT, lab results, care plans, therapy notes, encounter data) is created or stored. Examples: EHR modules, behavioral health (BH) platforms, e-prescribing systems, telehealth platforms, billing systems, CRM/engagement tools.
- ☐ Identify if Part 2 records are intermixed with general medical information or maintained in dedicated Part 2 segments.

42 CFR Part 2 Compliance Checklist

❒ **Identification of Part 2 "*Records*."** For each system, map:

- ☐ Whether the record meets the definition of a "Part 2 Record" (originated from a Part 2 Program and identifies a patient as having SUD or receiving SUD services).
- ☐ Whether downstream systems automatically replicate or transform the data (e.g., interoperability feeds, summary care records, HIE CCDs).

❒ ***Uses & Disclosures.*** For each workflow, document:

- ☐ Purpose (treatment, payment, operations, care coordination, billing, peer review, quality).
- ☐ Whether consent is required under Part 2.
- ☐ Whether an exception applies (e.g., bona fide medical emergency, research, court order, audit/evaluation, public health (must be de-identified now)).
- ☐ Whether all elements of the relevant exception can be satisfied, including documentation.

❒ ***TPO Consent Use Case***

- ☐ Identify whether the EHR will rely on a TPO Consent to allow Part 2 Records to be used and disclosed to non-Part 2 components within an integrated health system.
- ☐ Confirm whether the TPO Consent:
  - Meets all Part 2 Consent elements (post-2024 Final Rule).
  - Allows routing of Part 2 data to non-Part 2 treating providers.
  - Includes redisclosure permissions consistent with 2.33.
- ☐ Determine whether EHR system configuration supports:
  - Segmentation of Part 2 data when consent is not present.
  - Audit trails of disclosures for Accounting requirements under §2.24(b).
  - Role-based access restrictions.

❒ ***Health Information Exchange* Participation (HIE/HIN/TEFCA).** For each interoperability connection:

- ☐ Identify whether Part 2 information will be exchanged pursuant to a Part 2 Consent or treated under a TPO Consent.
- ☐ Determine:
  - How the consent will be made available to the HIE/HIN ("copy of the consent" requirement).
  - How the organization will provide a "clear explanation of the scope of the consent" when a full copy cannot be transmitted (per §2.32(b)).
  - Whether the HIE's participation agreement, QSOA, or BAA meets Part 2's redisclosure limitations.
  - Whether downstream participants may redisclose consistent with the patient's consent.

❒ ***External Disclosures* (Providers, Payers, Vendors, Care Partners).** For each external party:

- ☐ Identify data elements disclosed (e.g., CCD, encounter data, meds, billing codes).
- ☐ Determine the legal basis:
  - Part 2 Consent *or* Part 2 Exception?
  - QSOA/BAA?
  - Court order?
- ☐ Document redisclosure restrictions applicable to each party.

❒ ***Patient-Facing Systems.*** Map any flows involving:

- ☐ Patient portals
- ☐ Third-party apps (API access / SMART-on-FHIR). Ensure that disclosures via APIs comply with Part 2 Consent requirements and redisclosure limitations.

42 CFR Part 2 Compliance Checklist

Privacy

❒ **Privacy Officer.** HIPAA requires designation of a Privacy Officer; while 42 CFR Part 2 does not, organizations should assign Part 2 privacy compliance responsibilities to the HIPAA Privacy Officer and ensure job description alignment. *See* Form 2D ; Policy 3A:#G02

❒ **Privacy Policies.** Update Privacy P&Ps for all Part 2 Final Rule changes by **February 16, 2026**.

- ☐ **Complaints and Reporting Part 2 Non-Compliance** Policy 3A:#G05
- ☐ **Right to Access** Policy 4A:#PP-01
- ☐ **Right to Accounting of Disclosures** Policy 4A:#PP-03
- ☐ **Right to Request Restrictions and Confidential Communications** Policy 4A:#PP-04
- ☐ **Personal Representatives** Policy 4A:#PP-05
- ☐ **Business Associates and Qualified Service Organizations** Policy 4B:#PP-07
- ☐ **Treatment, Payment, Health Care Operations** Policy 4B:#PP-08 -09 -10
- ☐ **Public Health** Policy 4B:#PP-14
- ☐ **De-identified Information** Policy 4B:#PP-16
- ☐ **Law Enforcement Requests** Policy 4B:#PP-22
- ☐ **Disposing Records When Part 2 Program is Discontinued or Acquired** Policy 4B:#PP-28

❒ **Update Written/Electronic Consents.** Update all Part 2 Consents and HIPAA Authorization forms for Part 2 Final Rule compliance:

- ☐ **Part 2 Consent for TPO** Form 2A(i)
- ☐ **Part 2 Consent for Intermediary** Form 2A(ii)
- ☐ **Part 2 for all non-TPO Uses** Form 2A(iii)

Technology Tip: *Ensure any electronic Part 2 consent applications that your organization is evaluating can satisfy **all** Part 2 consent elements and required notice statements.* *See* Form 2A(iv)

❒ **Consent Copy or Explanation.** Develop a process to provide the disclosure recipient **either** (1) a copy of the patient's consent **or** (2) a clear explanation of the scope of that consent, as required by § 2.32(b).

- ☐ *Paper Option:* Attach a copy of the signed consent (or a brief written explanation of its scope) to each disclosure. This can be done manually by HIM/ROI staff as part of the standard release workflow.
- ☐ *Technical Option:* Coordinate with your EHR/HIE/IT vendor to enable electronic transmission of either (a) the Part 2 consent itself or (b) a standardized electronic "consent scope summary" that can accompany automated disclosures of Part 2 information.

❒ **Notice of Privacy Practices.** Update the Notice of Privacy Practices for Part 2 Final Rule changes by February 16, 2026. Obtain patients' signed Acknowledgment of receipt of organization's updated HIPAA NPP. *See* Form 2C To review a list of changes that need to be made to a current NPP in order to comply with the new Part 2 changes, *See* Checklist 1F: Part 2+HIPAA NPP – Required Elements
Compliance Tip*: This is required by 42 CFR Part 2 **and** HIPAA to be completed by February 16, 2026!*

❒ **Qualified Service Organization Addendum**. Update HIPAA Business Associate Agreements (BAA) with any third party that has access to PHI and incorporate Qualified Service Organization Agreements (QSOAs) language with any third party that has access to PHI which includes Part 2 Records to perform Health Care Operations and other services for your organization. *See* Form 2B

42 CFR Part 2 Compliance Checklist

- ☐ *Tracking:* Develop process for tracking BAAs and QSOAs, including limiting scope of who is authorized to execute BAAs/QSOAs, renewal ticker, expiration ticker, process to return PHI etc. *See* Tool 1I: *Documentation:* HIPAA BAA/QSOA Tracking

- ☐ *3rd Party Form Review:* If a third party requires their form of HIPAA BAA to be used, Organization should review the 3rd party BAA/QSO form for compliance. *See* Tool 1T: *Checklist:* Reviewing 3rd Party BAA/QSOA

❒ **Accounting of Disclosures.** Determine how your organization is going to meet the Accounting of Disclosures for Treatment, Payment and Health Care Operations made through an electronic health record, as required by Section 2.24(b) of 42 CFR Part 2. *See* Tool IK: AOD Documentation; *See* Policy 4A:#PP-03

❒ **State Law Standards.** Identify and incorporate any state laws that are more stringent than Part 2 into policies, forms, notices and agreements, as applicable. This is required under § 2.20 of Part 2.

***Compliance Tip*:** Not sure if your state has laws governing Substance Use Disorder (SUD) information that is more stringent or affords more patient rights than Part 2? Visit this 50-State SUD public resource:

- Disclosure of Substance Use Records Without Patient Consent
- Disclosure of Substance Use Records With Patient Consent
- Disclosure of Substance Use Records Pursuant to a Court Order

Security

❒ **Security Officer.** HIPAA requires designation of a Security Officer; while 42 CFR Part 2 does not, organizations should assign Part 2 security compliance responsibilities to the HIPAA Security Officer and ensure job description alignment. *See* Form 2E ; Policy 3A:#G03

❒ Complete a **Security Risk Analysis**. *See* Tool 1E: *Documentation:* Security Risk Analysis (OCR/ONC CRA Tool Identify and remediate gaps within 30 days where possible for potential affirmative defense.

❒ **Security Policies.** Update organization's Security Policies & Procedures for Part 2 Final Rule changes by February 16, 2026.

- ☐ **Breach Response & Notification** *See* Policy 5A:#SAP-09
- ☐ **Disposal of Information & Records** *See* Policy 5C:#SPP-05

❒ Ensure that any applicable State Law security standards that may apply to SUD providers or records are incorporated into all Security P&Ps.

Security Incidents & Data Breach Management

❒ **Update Breach Policy.** Update Breach Policy & Procedures for Final Rule Part 2 changes by no later than February 16, 2026. *See* Policy 5A:#SAP-09

Note: Unauthorized uses and disclosures of Part 2 information that did not otherwise violate HIPAA did not have to be reported. ***This will change on February 16, 2026****. For example, if Part 2 information is disclosed to a third party for treatment purposes but the patient's consent to such disclosure purpose was not obtained, as of February 16, 2026 this is potentially a reportable breach under Part 2, even though it would not be considered a "breach" under HIPAA.*

42 CFR Part 2 Compliance Checklist

- ❒ **Update Security Incident Policy.** Update Security Incident Policy & Procedures for Final Rule Part 2 changes by no later than February 16, 2026. *See* Policy 5A:#SAP-08

- ❒ **Breach Assessment**. Evaluate all discovered security incidents and disclosures of Part 2 information that are potentially unauthorized under Part 2. Tool 1M: *Documentation:* Part 2+HIPAA Breach Assessment (with "low probability" scoring)

Training

- ❒ **"Train-the-trainer."** Provide educational resources and support for Privacy Officer and Security Officer. Ensure training tools are up to date on most recent changes to 42 CFR Part 2. *See* Resource 1Q(i): 42 CFR Part 2 PowerPoint

- ❒ **Train new hires** and **existing workforce** on HIPAA and Part 2 P&Ps as necessary and appropriate to carry out functions. *See* Resource 1Q(ii): Workforce Training PowerPoint

- ❒ **Document** HIPAA and Part 2 Training, including attendees and materials used.

- ❒ **Provider periodic refresher** HIPAA and Part 2 training to workforce (at least annually, and periodically upon identification of deficiencies or areas in need of improvement).

- ❒ Develop and Implement "**Security Reminders**". *See* Policy 5A #SAP-11 *See* Tool 1P

Complaint Process

- ❒ Develop and implement a Part 2 Complaint process. *See* Policy 3A #G05
  - ☐ Determine intake process (i.e., email; phone; written complaint mailbox etc.)
  - ☐ Appoint individual with responsibility for investigation (i.e., Compliance Department)
  - ☐ Document all complaints, investigations and dispositions

Sanctions

- ❒ Develop Sanctions policy and process for violations of 42 CFR Part 2 policies. *See* Policy 3A: #G06
- ❒ Sanction Workforce members who fail to comply with Part 2.

On-Going Evaluation & Audits

- ❒ Assemble and activate a HIPAA/Part 2 Compliance Committee to oversee periodic reviews and updates. *See* Policy 3A: #G01

- ❒ Complete a Security Risk Analysis (SRA) upon any change in circumstances. *See* Tool 1E Identify and remediate within 30 days if possible (potential affirmative defense to penalties).

- ❒ **Identify Gaps.** Identify any gaps in your organization's compliance with 42 CFR Part 2. Remediate all Part 2 Gaps identified

Document Retention

- ❒ All required HIPAA documentation **must be retained** for at least **6 years**. *May* be maintained electronically.