42 C.F.R. Part 2: Final Rule

Implementation Guide for SAPC Provider Agencies

Updates You Need to Know About

The U.S. Department of Health and Human Services ("HHS") has updated certain requirements under 42 C.F.R. Part 2 ("Part 2"), which impacts how providers and other organizations subject to Part 2 must handle client information concerning substance use disorders ("SUD"). Compliance with the Part 2 Final Rule updates is required by **February 16, 2026**.

To support compliance with the Part 2 updates, SAPC is providing complimentary training sessions to its network providers and their support staff that will include an overview of the recent changes to Part 2 regarding the handling, use, and disclosure of SUD information, and other relevant federal and California state privacy laws that interplay with Part 2. The training sessions will focus on: (1) identifying SUD information covered by Part 2; (2) understanding the stringent requirements for client consent; (3) exploring the exceptions to the consent requirement; (4) reviewing compliance obligations for uses and disclosures; and (5) discussions surrounding practical applications and use cases. Special attention will be given to recent updates that align certain Part 2 processes with HIPAA and the implications for day-to-day operations.

This Implementation Guide: (1) outlines key actions you need to take to ensure compliance with the Part 2 updates; (2) summarizes the requirements imposed by the Part 2 updates; and (3) provides a decision tree to support your assessment of whether Part 2 permits disclosure of SUD information.

Actions You Need to Take

1. **Attend a SAPC Part 2 Training Session**

   All individuals that interface with clients or handle client records should attend a training session.

2. **Update Your Consent for Release of SUD Information Form**

   SAPC will make an updated SAPC Release of Information available to SAPC Providers, which will be required for all future disclosures of SUD information related to SAPC.

3. **Update Your Notice of Privacy Practices**

   SAPC Providers are responsible for updating their Notice of Privacy Practices to comply with changes under the Final Rule.

4. **Update Your Notice of Confidentiality Which Accompanies Released Information**

   SAPC will make an updated Notice of Confidentiality available to SAPC Providers.

5. **Update Your Policies and Procedures**

   Providers are responsible for ensuring use of compliant policies and procedures that satisfy Part 2 requirements.

SUMMARY OF PART 2 UPDATES

This Summary outlines practical direction on complying with the requirements imposed by the Part 2 updates, highlighting key requirements and procedures regarding consent, court orders, important exceptions, and breach notification.

Treatment, Payment, and Healthcare Operations ("TPO")

Guiding Principle: SAPC Providers participating in Part 2 programs must obtain written consent to share SUD information for TPO purposes. Disclosures should be limited to the minimum necessary information described in the consent form. A client may submit a single consent form that covers all future uses and disclosures for TPO purposes, but this must be indicated in the consent form. For SAPC Providers, the updated SAPC Release of Information Form covers disclosures for TPO purposes.

When obtaining consent to disclosure from SAPC clients, SAPC Providers must use the SAPC Release of Information Form provided by SAPC. This is the only consent form required for TPO disclosures.

- **Treatment:** means the provision, coordination, or management of health care and related services by one or more providers.

Examples: coordination or management of health care with a third party; consultation between providers relating to a client; referral of a client for health care from one provider to another; submitting specimens to a lab for assessment or tests.

- **Payment:** means the activities undertaken by: (1) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the plan; or (2) a provider or health plan to obtain or provide reimbursement for care.

Examples: billing; claims submission; collections activities; determinations of eligibility or coverage; utilization management; prior authorization.

- **Healthcare Operations:** means support activities that help providers and health plans operate.

Examples: case management and care coordination; quality assessment; technology support; vendors for electronic health records and cloud information storage; legal and auditing services; customer service; business planning.

TPO Redisclosures: SAPC Providers should be able to explain to clients that a consent to disclosure for TPO purposes can "follow" the information downstream to additional recipients of the SUD information. When a SAPC Provider discloses SUD information for TPO purposes to another party subject to HIPAA (such as a primary care physician) pursuant to a TPO consent form, the recipient may redisclose that information to other parties subject to HIPAA for TPO purposes without obtaining additional consent.

Examples: A primary care physician that is subject to HIPAA may redisclose SUD information (pursuant to a TPO consent) to a cardiologist for the client's treatment. The same primary care physician could disclose SUD information to a health plan to seek reimbursement for services rendered to the client.

Consent Requirement

Guiding Principle: SAPC Providers participating in Part 2 programs generally may not disclose SUD information, unless the client has signed a consent form or a valid court order and subpoena permits the disclosure. **When in doubt, default to obtaining consent before disclosing SUD information!**

Court Orders

Guiding Principle: A court order authorizes, but does not compel, disclosure of SUD information or testimony relaying the information contained in SUD information. An order along with a subpoena/similar legal mandate are required to compel disclosure of SUD information.

Example: A SAPC Provider receives a subpoena for SUD information, but not a court order. The SAPC Provider may not disclose the SUD information unless it also receives a court order meeting Part 2's requirements.

Civil (Noncriminal) Matters: If a SAPC Provider receives a court order relating to a civil matter, the SAPC Provider must ensure that the client receives: (1) adequate notice; and (2) an opportunity to file a written response to the application (or to appear in person).

Criminal Matters: If the SAPC Provider receives a court order relating to a criminal matter, the SAPC Provider must ensure that the client receives: (1) an opportunity to appear and be heard to provide evidence on the criteria for issuance of the order; and an (2) opportunity to be represented by independent counsel if law enforcement applies for the court order. Additional obligations under Part 2 are also applicable for criminal matters.

Note: Prior to disclosing any SUD information pursuant to a court order, consult with Legal.

Exceptions to Consent Requirement

Bona Fide Medical Emergencies: Disclosure of SUD information to medical personnel is permitted when the client's written consent cannot be obtained due to a medical emergency, provided that the SAPC Provider documents the disclosure in the client's medical record.

Management/Financial Audits and Evaluations: Disclosure of SUD information is permitted for an audit/evaluation to a federal, state, or local governmental agency that provides financial assistance to a SAPC Provider or that is otherwise authorized by law to regulate the activities of the SAPC Provider.

Public Health: Disclosure of SUD information may be permitted for certain public health purposes, as long as: (1) the disclosure is to a public health authority; and (2) the content of the information being disclosed has been de-identified and there is no reasonable basis to identify the client. For example, this exception could permit disclosures to agencies such as the California Department of Public Health.

Research: SAPC Providers subject to HIPAA can disclose certain information for scientific research, if the researcher is either: (1) also a party subject to HIPAA that has obtained HIPAA-compliant client authorization; or (2) provides documentation to the SAPC Provider showing compliance with HHS regulations (45 CFR Part 46) or FDA regulations (21 CFR Parts 50 and 56) around the protection of human research subjects. Scientific research is limited to activities that benefit generalizable knowledge and does not include private quality assessment or improvement activities.

Note: Prior to disclosing any SUD information on the basis of an exception, consult with Legal.

Qualified Service Organizations

Guiding Principle: Part 2 permits SAPC Providers to disclose SUD information to qualified service organizations (QSO), which are entities that provide support services to the SAPC Provider, provided that the SAPC Provider and QSO have entered into a written agreement acknowledging that: (1) the QSO is fully bound by Part 2 in handling SUD information on behalf of the SAPC Provider; and (2) if necessary, that the QSO will resist judicial proceedings to obtain access to SUD information. A QSO is similar to a business associate under HIPAA.

Example: A QSO may include a party that provides data processing, bill collecting, dosage preparation, laboratory analyses, legal services, accounting services, population health management services, medical staffing services, or other professional services.

Breach Notification and Risk Assessments

Guiding Principle: The Part 2 updates align HIPAA's Breach Notification Rule for identifying and responding to impermissible disclosures of SUD information.

Mitigation: SAPC Providers must take steps to mitigate any disclosures that violate Part 2 regulations (or HIPAA). **It is not enough to spot the issue, you must also take steps to fix the issue!** Mitigation depends on the circumstances but typically involves retrieving, deleting, or destroying improperly disclosed information, including by remote wiping mobile devices, terminating access credentials, and changing passwords. Mitigation can also involve asking the unintended recipient for confirmation that they not access or further disclose the information, re-training staff involved in the breach, and updating policies and procedures.

Risk Assessment: HIPAA requires SAPC Providers to assess whether any disclosure of information that violates Part 2/HIPAA constitutes a "breach" that must be reported. In conducting the assessment, SAPC Providers must consider the following factors: (1) amount and type of information received/accessed; (2) identity of unauthorized person receiving/accessing the information; (3) actual receipt/access of information; and (4) extent of mitigation by SAPC Provider.

Notification: When a breach has occurred, the SAPC Provider must provide certain notices. In addition to notifying SAPC immediately after discovery of a breach, HIPAA requires the following actions:

- **Affected Client:** HIPAA requires that SAPC Providers provide notice of a breach to the affected clients. The notice must be provided within 60 days of discovery of a breach.
- **HHS:** HIPAA requires that notice of a breach be given to HHS. If the breach affects more than 500 individuals, notice must be provided within 60 days of discovery of a breach. If the breach affects fewer than 500 individuals, notice must be provided within 60 days after the end of the calendar year in which the breach occurred.
- **Media:** When a breach involves more than 500 residents of a State, HIPAA requires that notice of the breach be given to the local media outlets serving the State within 60 days of discovery of a breach.

Note: If you see something, say something! Report suspected breaches or inappropriate disclosures of SUD information to SAPC.

Decision Tree: Release of SUD Information

For SAPC Provider Agencies

Does Disclosure Involve SUD Information?

"SUD Information" includes any information, whether recorded or not, created by, received, or acquired by a Part 2 Program relating to a patient (e.g., diagnosis, treatment, and referral information, billing information, communications), and including patient identifying information.

NO ↓

Disclose Information If Also Permitted by HIPAA & State Law

YES ↓

Did Client Sign Consent Authorizing Disclosure of SUD Information?

Disclosure is permitted where the client signs a valid consent authorizing the disclosure.

YES ← **Disclose Information For Purpose Stated in Consent or for Treatment, Payment, Healthcare Operations If Also Permitted By HIPAA & State Law**

NO ↓

Is Disclosure Justified By Medical Emergency?

Disclosure is permitted when the client's written consent cannot be obtained due to a medical emergency.

YES ← **Disclose Information Necessary to Address Medical Emergency and Document Disclosure in Client Medical Record If Also Permitted By HIPAA & State Law**

NO ↓

Does Disclosure Facilitate Qualifying Audit/Evaluation?

Disclosure of certain information is permitted for an audit/evaluation on behalf of qualifying federal, state, or local governmental agencies

YES ← **Disclose Information As Necessary To Facilitate Qualifying Audit/Evaluation If Also Permitted By HIPAA & State Law**

NO ↓

Does Disclosure Facilitate Qualifying Research?

Disclosure of certain information is permitted for conducting qualifying scientific research.

YES ← **Disclose Information As Necessary To Facilitate Qualifying Research If Also Permitted By HIPAA & State Law**

NO ↓

Is Disclosure For Public Health Activity?

Disclosure is permitted for public health activities, where: (1) disclosure is to a public health authority; and (2) content has been de-identified.

YES ← **Disclose De-Identified Information To Public Health Authority As Necessary For Public Health Activity If Also Permitted By HIPAA & State Law**

NO ↓

Is Disclosure Directed to Qualified Services Organization?

Disclosure is permitted provided that written agreement is in place acknowledging qualified service organizations obligations under Part 2

YES ← **Disclose Information To Qualified Services Organization As Necessary For Organization To Complete Function If Also Permitted By HIPAA & State Law**

NO ↓

Is Disclosure Covered By Court Order and Subpoena?

A court order along with a subpoena/similar legal mandate are required to compel disclosure of SUD information.

YES ← **Consider Disclosing Information Covered by Court Order and Subpoena If Also Permitted By HIPAA & State Law**

NO ↓

Must Obtain Client Consent

SAPC Providers participating in Part 2 programs are generally prohibited from disclosing any SUD information, unless the client has submitted a consent form, an exception applies, or a court order permits the disclosure.