ABHW
Advancing Health Care Policy for
Mental Health & Substance Use Disorders

2024 FINAL RULE TO AMEND 42 CFR PART 2

Summary and Analysis of Key Provisions

On February 16, 2024, the U.S. Department of Health and Human Services ("HHS") released a Final Rule ("the 2024 Final Rule" or "Final Rule") to amend confidentiality requirements for substance use disorder ("SUD") patient records under 42 C.F.R. Part 2, pursuant to changes to the underlying statute at 42 U.S.C. § 290dd–2 that were made by section 3221 of the Coronavirus Aid, Relief, and Economic Security ("CARES") Act. This Final Rule follows and generally aligns with the provisions of a notice of proposed rulemaking ("NPRM") that was published on December 2, 2022.

The Final Rule includes a number of significant revisions to the Part 2 regulations with regard to compliance requirements and enforcement. Most of the changes finalized in this rule align with the text that was proposed by the NPRM, and most of the differences in the Final Rule relative to the NPRM are very minor or non-substantive. However, the Final Rule did diverge from the NPRM in several important ways. The following summary outlines the changes from the pre-existing regulations and also specifically notes key differences in the Final Rule relative to the NPRM:

(1) **Definitions:** The Final Rule revises the definitions for a variety of key terms under Part 2. Many of these changes are designed to better align with definitions from the HIPAA Rules.
- In response to public comments, the Final Rule adds new definitions for several terms that were not defined under the NPRM (including "Lawful Holder" and "Personal Representative") and clarifies definitions for several key terms that were introduced by the NPRM.
- The Final Rule also excludes Business Associates and Covered Entities from the definition for "Intermediary," significantly reducing the scope of application of the specific consent requirements that apply to Intermediaries.

(2) **Patient consent and redisclosure:** The Final Rule creates or modifies several requirements for patient consent and redisclosure of Part 2 records. The Final Rule permits the redisclosure of SUD records received from a Part 2 Program with patient consent for treatment, payment, and health care operations (TPO) purposes. This aligns Part 2 more closely with HIPAA patient consent requirements, facilitating better integration of care.
- The Final Rule adds a new specific consent requirement for SUD counseling notes not included in the NPRM.
- The Final Rule newly stipulates that a blanket consent to disclose Part 2 records for TPO must be a separate document from a consent to use Part 2 records in civil or criminal proceedings.
- The Final Rule adds a new requirement for a copy of the patient's written consent to accompany each disclosure.

(3) **Accounting of disclosures:** The Final Rule creates a new right for patients to obtain an accounting of all disclosures made with consent for up to three years and a right to request restrictions on disclosures.
    - The Final Rule newly announces that the compliance date for §2.25 will be tolled until the HIPAA Accounting of Disclosures provision at 45 C.F.R. §164.528 is revised to address accounting for TPO disclosures made through an EHR.

(4) **Updates to notice obligations:** The Final Rule updates requirements for the Notice of Privacy Practices ("NPP") to address uses and disclosures of Part 2 records and individual rights with respect to those records.
    - The Final Rule adopts changes to the Part 2 Patient Notice only; it does not finalize the proposed changes to the HIPAA NPP in 45 CFR 164.520, which will instead be promulgated as part of a future HIPAA rulemaking.

(5) **Security of records and breach notification obligations:** The Final Rule imposes new breach notification obligations that align with corresponding requirements under HIPAA.
    - The Final Rule updates the de-identification provision to fully align with the HIPAA Privacy Rule at 45 CFR 164.514 by removing language that would have created a slightly different standard for de-identification for Part 2 information.
    - The Final Rule adds breach notification requirements by requiring compliance with the HIPAA Breach Notification Rule for breaches of records by Part 2 Programs.

(6) **New civil money penalties ("CMPs") and enforcement:** The Final Rule aligns the criminal and civil penalty structure for Part 2 with HIPAA in an attempt to ensure a consistent enforcement process. Patients are also given the right to file a complaint directly with HHS for alleged violations of Part 2.
    - To closer align with the HIPAA Enforcement Rule, the Final Rule clarifies that enforcement and penalties are not limited to formal findings of violations, but apply for "noncompliance" more generally, including through the form of informal resolutions.

(7) **Restrictions on use and disclosure for legal proceedings:** To better protect patients from the unauthorized use of Part 2 records against them in civil, criminal, administrative, and legislative proceedings, the Final Rule significantly expands the restrictions on the use and disclosure of Part 2 records in such proceedings without patient consent. The Final Rule also creates a new limitation on liability for government agencies that investigate and prosecute Part 2 Programs and unknowingly receive records subject to Part 2.

Compliance Timeline

While the regulation itself is "effective" on April 19, 2024 (sixty days after publication in the Federal Register), persons/entities subject to the regulation will not be required to comply with the revised requirements until February 19, 2026, two years after the date of Federal Register publication. This allows an extended time period for entities to make

operational and systems changes before the compliance date. However, there may be actions affected parties must take prior to the compliance date, specifically where HHS's preamble reflects positions on currently effective Part 2 requirements. Thus, for example, it is important to note that HHS may undertake investigations that lead to enforcement actions with regard to existing requirements while abstaining from making compliance determinations with regard to Part 2 obligations that are new under this Final Rule.

I. Revisions to definitions of key terms under Part 2 (§ 2.11)

The Final Rule adds sixteen defined regulatory terms and materially modifies the definitions of seven existing terms. **Most of the new terms and definitions are added or modified by referencing existing terms from the HIPAA Rules** in 45 CFR parts 160 and 164, either as required by the CARES Act or as a logical outgrowth of CARES Act amendments. **These changes to defined terms clarify the specific components of the relevant HIPAA statutory and regulatory provisions that have been incorporated into the Part 2 rule**.

The key terms that have been aligned with HIPAA requirements and enforcement include Covered Entity, Treatment, Payment, Health Care Operations, Third-Party Payer, Unsecured Protected Health Information, and Breach. Terms that are specific to Part 2 include Records and Unsecured Records. Thus, for example, the alignment of definitions for Unsecured Record for Part 2 and Unsecured Protected Health Information (PHI) under HIPAA help to implement the newly required breach notification standards for Part 2 records that align with the breach notification standards under HIPAA.

Similarly, **HHS also finalized edits to the definition of Qualified Service Organization ("QSO") to include entities that meet the definition of a Business Associate under the HIPAA Rules.** This modification clarifies that HIPAA Business Associates are QSOs in circumstances when Part 2 records also meet the definition of PHI (i.e. when a Part 2 Program is also a Covered Entity). The HIPAA Rules generally permit disclosures from a Covered Entity to a person who meets the definition of a Business Associate (i.e., a person or entity that works on behalf of or provides services to the Covered Entity) without individual authorization, when based on a Business Associate agreement that incorporates certain protections. Similarly, the Final Rule specifies that the use and disclosure restrictions of this part do not apply to the communications between a Part 2 Program and QSO when the information is needed by the QSO to provide services to, or work "on behalf of", the Part 2 Program.

The Final Rule also significantly narrows the definition of "Intermediary." This defined term "Intermediary" is necessary with regard to considerations about how downstream entities will continue to need to be able to identify and protect Part 2 records in ways that are different from their protections for PHI under HIPAA. The Final Rule defines an Intermediary as a person who has received records, under a general designation in a written patient consent, for the purpose of disclosing the records to one or more of its member participants who have a treating provider relationship with the patient. HHS considered removing the specific Intermediary requirements entirely in order to diminish

the regulatory burden of compliance for Intermediary entities and eliminate inconsistencies in the requirements for Intermediary and non-Intermediary entities that serve TPO functions but ultimately declined to do so. However, one notable change that HHS did make in the Final Rule relative to the NPRM is to exclude Covered Entities and Business Associates from the definition of "Intermediary." Thus, for example, a Health Information Exchange ("HIE") would generally be excluded from the definition of "Intermediary," and could therefore receive Part 2 records pursuant to a general consent to share for TPO purposes, without being required to be specifically named in the Part 2 consent.

II. New or modified requirements for patient consent and redisclosure of Part 2 records and the patient consent (§§ 2.31, 2.32, 2.33, 2.53)

The Final Rule modifies the required elements of the written consent forms for Part 2 records to more closely track the core elements of a written authorization form under HIPAA, at 45 CFR 164.508(c). The Final Rule also implements the requirements of the CARES Act to permit a single consent for all future uses and disclosures for treatment, payment, and health care operations ("TPO").

Several of the changes do not appear to be intended to substantively change the current requirements but do modify the wording to align with the specific phrasing of similar requirements under HIPAA (e.g., changes related to the identity of the discloser, description of the information to be disclosed, the right to revoke consent, and the expiration of consent). For example, HHS notes in the preamble that once a Part 2 Program discloses a record for TPO purposes to a Part 2 Program, Covered Entity, or Business Associate with prior written consent, a revocation of consent is only effective to prevent additional disclosures to those entities.[1]

Part 2 Programs are not required to notify recipients of Part 2 records of a revocation of consent or "pull back" records that it has disclosed under a valid consent. However, once a recipient is informed of the revocation, the recipient must stop making further uses and disclosures of Part 2 records, except to the extent they have already acted in reliance on the consent. For example, a health plan that is already processing a claim pursuant to a TPO consent that has been revoked may complete the transaction but may not process new part 2 claims for that plan member. Similarly, a HIE would not be required to purge the Part 2 records but would be required to stop making further disclosures of the patient's record to other member participants.

Despite the increased alignment, HHS does note in the preamble that it remains necessary to distinguish between "consent" for disclosure under Part 2 vs. "authorization" under HIPAA due to differences in the requirements and scope of application of these two different sets of requirements, in particular for Part 2 Programs that are not Covered

[1] The NPRM considered the possibility of allowing an oral revocation of consent. However, the preamble of the Final Rule notes that the statute requires revocation of a TPO consent to be in writing. Nonetheless, HHS notes that an entity may be obligated to assist a patient to document any oral attempt to revoke consent.

Entities under HIPAA (e.g., an SUD provider that does not submit electronic claims). For example, a HIPAA authorization is not required for uses and disclosures of PHI for TPO, but the Part 2 regulations stipulate that consent is required for uses and disclosures of Part 2 records for TPO. The Final Rule does reiterate that a Part 2 Program may condition the provision of treatment on the patient's consent to disclose information as needed.

The Final Rule also eliminates language in section 2.12 ("Applicability") that some commenters had interpreted to create an obligation to segregate or segment Part 2 records from PHI or other records. **Instead, the Final Rule now explicitly stipulates that there is no requirement for a Part 2 Program, Covered Entity, or Business Associate that receives records based on a single consent for all TPO purposes to segregate or segment such records. However, given the ongoing need to comply with various Part 2 requirements, including the need to ensure that the consent form remains attached to the Part 2 Record, as well as restrictions related to redisclosure for legal proceedings, it appears that it will be necessary to continue to be able to flag the information as a Part 2 Record.**

It is also important to note that if consent is not given for TPO, the prohibition on redisclosure in 42 C.F.R. § 2.12(d) is still required. Therefore, this distinction between records that can be used or disclosed for TPO (i.e., single use consent for TPO) and those that cannot (i.e., no consent or records sought for legal proceedings) must be effectively operationalized. Even HHS recognized that "it is unclear how that can be accomplished (the applicability of the notice of prohibition on redisclosure) unless the recipient is aware that the records are subject to the prohibition."[2] Therefore, as a practical matter, this may require a Part 2 program to continue to segment these SUD records that are not subject to a TPO consent to properly apply, transmit, and display the required notice.

The Final Rule adds a variety of new requirements for the written consent form. Specific requirements include:

- Where applicable, language indicating a single patient consent is meant to apply to all future uses and disclosures for TPO;
- Where the disclosure is for TPO – a statement that the patient's record may be redisclosed in accordance with HIPAA, except for uses and disclosure for civil, criminal, administrative, and legislative proceedings against the patient;
- A description of purpose statements sufficient for relaying (i) when a patient initiates the consent and elects not to provide a statement of purpose, (ii) when a patient provides consent once for all TPO uses and disclosures; and (iii) a statement about the patient's right to elect not to receive any fundraising communications;
- For disclosure to an Intermediary, the name of the Intermediary and either the name of the Intermediary's participants or a general designation for such members;
- Statements around (i) the potential for the records to be redisclosed and no longer protected by Part 2 and (ii) the consequences of refusal to sign the consent.

[2] See www.federalregister.gov/documents/2024/02/16/2024-02544/confidentiality-of-substance-use-disorder-sud-patient-records, at p. 12555 and p. 12559 (Feb. 16, 2024) segment.

The Final Rule diverges from the proposed requirements for consent forms in newly stipulating that separate, dedicated consent forms are necessary for two purposes.

First, a separate consent form is required to share SUD counseling notes. Where it is necessary to share these notes, it is insufficient to rely on a general consent to share Part 2 Records for all TPO purposes (except in limited circumstances, such as staff training). This is analogous to protections in HIPAA for psychotherapy notes, and a single form can be used for authorization to disclose psychotherapy notes and consent to disclose SUD counseling notes.

In addition, a separate patient consent form is also required for use and disclosure of Part 2 Records in a civil, criminal, administrative, or legislative investigation or proceeding. This consent form for disclosure for legal proceedings cannot be combined with consent for any other purpose. Part 2 providers will, therefore, need to maintain a separate consent form for any need to disclose Part 2 records for legal proceedings.

The Final Rule also identifies how a recipient may further disclose Part 2 records that have been shared for TPO purposes. The existing Section 2.33 allows disclosure with the written consent of the patient, and if the patient consents to disclosure of their records for payment or health care operations, it allows a Lawful Holder to further disclose those records as necessary for its contractors, subcontractors, or legal representatives to carry out the payment or operations specified in the consent.

The Final Rule creates three categories of redisclosure permissions, depending primarily on whether or not the recipient is a Business Associate or Covered Entity:

- **(1) The recipient is a Business Associate or Covered Entity.** A Business Associate or Covered Entity that receives Part 2 records pursuant to consent to share for TPO purposes can redisclose the Part 2 Records for uses and disclosures as permitted by the HIPAA Rules (subject to the limitations of Part 2, subpart E, pertaining to legal proceedings).

- **(2) The recipient is NOT a Business Associate or Covered Entity.** If the recipient is NOT a Business Associate or Covered Entity and receives Part 2 records pursuant to consent to share for TPO purposes, the recipient may redisclose the Part 2 records as permitted by the consent (subject to the limitations of Part 2, subpart E for legal proceedings). The receiving entity must contractually require its contractors and subcontractors that receive Part 2 Records to comply with Part 2 requirements.[3]

- **(3) Any other Lawful Holder that is not a Business Associate, Covered Entity, or Part 2 Program** and that receives Part 2 records pursuant to consent to share

[3] The Final Rule excludes Covered Entities and Business Associates from the requirements for a written agreement between a Lawful Holder and redisclosure recipient because these entities are already subject to the HIPAA requirements for Business Associate agreements.

for payment or health care operations, ***but where the consent does NOT include redisclosure for treatment purposes***, can further use or disclose those records as permitted by the consent (subject to the limitations of Part 2, subpart E pertaining to legal proceedings). However, in this category, because the patient did not consent for information to be shared for treatment purposes, the Lawful Holder must obtain an additional written consent from the patient to redisclose these records for treatment purposes.

Thus, in brief, redisclosure by Business Associates and Covered Entities will typically be governed by the HIPAA Rules, whereas redisclosure by entities that are NOT Business Associates and Covered Entities will typically be governed by the terms of the consent.

The Final Rule departs from the NPRM by adding a new requirement for a copy of the patient's written consent to accompany each disclosure. Regulators state that because the attached consent may be combined with the required Notice to Accompany Disclosure, this will significantly reduce any administrative burdens associated with the new requirement. However, the Notice to Accompany Disclosure is a standard disclaimer only, and includes no patient information, whereas the signed consent form itself likely constitutes a Part 2 Record and Protected Health Information (PHI) because it identifies the patient and indicates that the patient is being treated for an SUD. Thus, where the standardized statement that was previously required could be shared in a non-protected manner—e.g., in the body of an email or other communication that may be accessible to unauthorized parties—the signed patient consent form is subject to all protections of HIPAA and Part 2. The new requirement, therefore, restricts the ability to flag for any unauthorized party that the information contained in a file is a Part 2 Record. It also remains unclear how the patient consent form will be transmitted as a standard transaction for entities that exchange electronic health information for claims submission purposes.

In summary, these provisions of the Final Rule will generally streamline operations, reduce barriers to treatment, and improve patient care and outcomes with a free information exchange amongst the provider team. It will be important to monitor whether the freer flow of SUD information, even for legitimate TPO purposes (with consent), will undermine patients' confidence in the confidentiality and security of these SUD records. It will also be useful to consider practical challenges and opportunities for implementing and operationalizing these requirements, and HHS expresses an openness to further guidance in response to ongoing feedback.

III. New rights to obtain an accounting of disclosures made with consent and to request restrictions on disclosures (§§ 2.25, 2.26)

Accounting of Disclosures

The Final Rule adopts new requirements for a Part 2 Program to provide to a patient, upon request, an accounting of all disclosures made with consent under § 2.31 in the three years prior to the date of the request. In the Final Rule, HHS clarified that the

period for which an accounting can "look back" is limited to those disclosures occurring after the first day of the compliance date.

The Final Rule also requires that a Part 2 Program provide a patient with an accounting of disclosures of records for TPO under § 2.33 only where such disclosures are made through an electronic health record, and that a patient only has a right to receive an accounting of these disclosures during the three years prior to the date on which the accounting is requested. This right to an accounting of disclosures of records mirrors the proposed standard in the HIPAA Rules.

Under the existing Part 2 regulations, only intermediaries are required to provide an accounting of disclosures of Part 2 records. Revisions to the Part 2 statute made by the CARES Act now require an accounting of all disclosures made with consent and of disclosures for TPO made through an electronic health record. As an acknowledgment of the potential compliance burden that this requirement creates, in the Final Rule, **HHS has tolled the effective and compliance dates for the accounting of disclosures requirement until the HITECH requirement is finalized within the HIPAA Rules at 45 C.F.R. §164.528**.

HHS declined to establish a maximum cost that a patient can incur when requesting an accounting of disclosures. HHS mentioned (but did not explicitly state the applicability to Part 2) that, under the HIPAA Privacy Rule, a Covered Entity must provide the first accounting to an individual in any 12-month period without charge, but the Covered Entity may charge a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the 12-month period, as long as the individual is informed of the fee in advance and is given an opportunity to withdraw or modify the request.

Further, HHS clarified that the right to an accounting of redisclosures depends on the status of the recipient. For example, a Covered Entity or Business Associate is subject to 45 C.F.R. §164.528 for redisclosures. A Part 2 Program that rediscloses records received from another Part 2 Program is subject to §2.25 for such redisclosures that fall within the scope of §2.25 in the same manner as for disclosures. The accounting of disclosures requirements under §2.25 do not distinguish between disclosures and redisclosures but focus on whether a disclosure is made with consent and the purpose of the disclosure or redisclosure. The accounting of disclosures under §2.25 would not need to include a separate and distinct list of redisclosures accompanied by a notice under §2.32.

Note that HHS has maintained existing requirements for intermediaries to provide patients who have consented to disclosure of their Part 2 records using a general designation, upon request, a list of persons to which the patient's record has been disclosed within the past 3 years. Revisions to the regulation text adopted in the Final Rule at §2.24 (redesignated from §2.13(d)) have, in some respects, broadened the list of disclosures requirement for intermediaries (i.e., by requiring a list of all "persons," rather than "entities," and by requiring a look-back of 3 years rather than 2 years). Further, HHS has not tolled the list of disclosures requirement for intermediaries, as it has for the new disclosure requirements in §2.25, because these obligations on intermediaries already exist and are currently in

effect. However, HHS has sought to reduce the burden associated with this requirement by limiting the entities that meet the definition of "Intermediary." Specifically, as finalized, HHS has revised the definition of "Intermediary" in §2.11 to exclude Part 2 Programs, Covered Entities, and Business Associates. This will permit HIEs that are Business Associates to receive Part 2 records under a broad TPO consent (rather than requiring special consent for an Intermediary) and redisclose them consistent with the HIPAA Rules. This approach is expected to encourage HIEs to accept Part 2 records and include Part 2 Programs as participants, to facilitate the integration of behavioral health information with other medical records, and to reduce burdens on Business Associates that serve as HIEs. Further, a QSO is only considered an Intermediary when it is providing services to a program that is not a Covered Entity. Part 2 Programs that are Covered Entities will be able to use a HIE that is a QSO and Business Associate to exchange Part 2 data as well as PHI. This is expected to benefit patients by enhancing their ability to receive comprehensive care.

Finally, note that because the NPP requirements have been updated to specifically address the patient's right to obtain an accounting of disclosures, Part 2 Programs may experience an increase in the volume of such requests.

Right to Request Restrictions on Disclosures

Further, the Final Rule adopts a new section that incorporates two distinct patient rights into Part 2:

- A patient right to request restrictions on disclosures of records otherwise permitted for TPO purposes; and
- A patient right to obtain restrictions on disclosures to health plans for services paid in full by the patient, including a requirement for Part 2 Programs to permit a patient to restrict uses or disclosures of the patient's records to carry out TPO.

Prior to the amendments to the Part 2 statute included in the CARES Act, patients did not have an explicit right to request restrictions on disclosures of Part 2 records for TPO, although patients could tailor the scope of their consent, which would govern the disclosure of their Part 2 records. As finalized by HHS, these new patient rights are intended to align with the individual right in the HITECH Act, as implemented at 45 C.F.R. §164.522.

A Part 2 Program is <u>not</u> generally required to agree to a requested restriction. A requested restriction would not be effective to prevent uses or disclosures required by law or permitted for purposes other than TPO. However, a Part 2 Program is required to agree to restrict the disclosure of a patient record to a health plan, even for payment or health care operations, if the record pertains solely to an item or service for which the patient has paid in full.

Once a request for a restriction is made, a Part 2 Program must not use or disclose the records unless the patient is in need of emergency treatment and the restricted record is

needed to provide the treatment. If a record is disclosed to provide emergency care, the program would be required to request that the emergency health care provider not further disclose the information. A Part 2 Program would only be able to terminate a restriction under certain listed circumstances.

Although HHS acknowledges data segmentation concerns associated with such requested restrictions in the Final Rule, HHS also points out that Covered Entities already have to address individual requests for restrictions of TPO uses and disclosures. Accordingly, both Covered Entities and Part 2 Programs that are not Covered Entities are encouraged to make reasonable efforts, to the extent feasible, to comply with a patient's request. Providers retain the responsibility for patient care and determining what is reasonable under the circumstances.

HHS also states that Part 2 Programs and Covered Entities are expected to do more than merely establish policies and procedures on the right to request restrictions—they need to make a concerted effort to evaluate how they can reasonably accommodate patients' requests. If an entity lacks EHR system capability to accommodate some patients' requests for restrictions, then the entity should consider whether it is appropriate to adopt a policy of conditioning treatment on signing a single consent for all TPO. If an entity agrees to a requested restriction, it should explain to the patient any limits on its ability to ensure that the request is implemented fully. HHS has provided examples related to the analogous HIPAA provision that could be used to demonstrate "reasonable effort" to operationalize compliance with a patient's request, including in circumstances when an individual is unable to pay for their health care in full.

IV. Updates to the Notice of Privacy Practices requirements in the HIPAA Privacy Rule to address uses and disclosures of Part 2 records and individual rights with respect to those records (42 CFR § 2.22)

The Final Rule significantly changes § 2.22 to require all Part 2 Programs, at the time of admission, to inform the patient that federal law protects the confidentiality of substance use disorder records. The Final Rule, noting HIPAA's "more robust notice requirements," adopts much of the content and structure of the HIPAA Notice of Privacy Practices set forth in 45 C.F.R. § 164.520, while excluding elements that are inapplicable to Part 2 Programs.

The Final Rule now requires Part 2 Programs to include a list of patient rights in their Patient Notice. The patient rights include the following:

- Request restrictions of disclosures made with prior consent for purposes of TPO;
- Request and obtain restrictions of disclosures of Part 2 records to the patient's health plan for those services for which the patient has paid in full (mirrors the HIPAA restriction on disclosure contained in 45 C.F.R. § 164.522);

- Obtain an electronic or paper copy of the notice from the Part 2 Program on request;
- Discuss the notice with a designated contact person identified by the Part 2 Program (must include the name or title, telephone number, and email address of the contact);
- A list of disclosures by an Intermediary for the past 3 years.
- Elect not to receive any fundraising communications (again more closely aligning with HIPAA).

Key changes to the requirements for the content of the Notice include:

- Header is now almost identical to the HIPAA NPP header.
- Description of uses and disclosures permitted for TPO, allowed without written consent, or only allowed with written consent.
- Fundraising notice and right to opt-out (where applicable).
- Summary of patient rights with respect to Part 2 records or
- List of Part 2 Program Duties that parallel statements of duties required in HIPAA NPP (including new duty of breach notification under Part 2).

HHS notes that the Final Rule allows providers the flexibility to give separate notice or a combined notice with regard to both HIPAA and Part 2 protections, so long as all required elements are included. The Final Rule also requires that Part 2 Programs, consistent with HIPAA's requirements, use plain language that is easily understandable when updating their Patient Notice.

The Final Rule also updates the Program's requirements for delivery of the Notice. Part 2 Programs are required to provide the Notice, as follows:

- To anyone who requests it;
- To a patient not later than the date of the first service delivery, including where first service is delivered electronically or as soon as reasonably practicable after emergency treatment;
- To be posted in a clear and prominent location at any physical delivery site where a patient would be able to read the notice in a manner that does not identify the patient as receiving SUD treatment; and
- To be included on a program's website, where available.

As a practical matter, the Final Rule did not finalize proposed amendments to the HIPAA NPP requirements. Thus, providers need to be aware that further changes to their notice obligations under this Rule may be coming since the Part 2 notice provisions will again be realigned with any changes to the HIPAA NPP requirements.

Finally, the Final Rule clarifies the timeline for compliance with these requirements, noting that updated patient notices must be provided by the first day of health care provided to the patient or as soon as reasonably practicable after emergency treatment AFTER the

compliance date for the program (i.e., after February 16, 2026, unless the compliance date is further extended to align with HIPAA NPP changes).

V. New requirements impose breach notification obligations (§ 2.16)

The Final Rule applies the HIPAA Breach Notification Rule, contained in 45 CFR §§ 164.400-414, to Part 2 Programs with respect to breaches of unsecured SUD records in the same manner as those provisions apply to a Covered Entity with respect to breaches of unsecured PHI.

HIPAA provides that a breach is, generally, impermissible access, use, or disclosure under the Privacy Rule that compromises the security or privacy of the PHI. Impermissible access, use, or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Following a breach of unsecured SUD information, Part 2 Programs, pursuant to the HIPAA Breach Notification Rule, must provide notification of the breach as follows.

Individual Notice

Part 2 Programs must now notify affected individuals following the discovery of a breach of SUD information. Part 2 Programs must provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the Part 2 Program has insufficient or out-of-date contact information for 10 or more individuals, the Part 2 Program must provide substitute individual notice by either posting the notice on the home page of its website for at least 90 days or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the Part 2 Program has insufficient or out-of-date contact information for fewer than 10 individuals, it may provide substitute notice by an alternative form of written notice, by telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Covered Entity is doing to

investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Covered Entity (or Business Associate, as applicable).

With respect to a breach at or by a Business Associate, while the Part 2 Program is ultimately responsible for ensuring individuals are notified, it may delegate the responsibility of providing individual notices to the Business Associate.

Media Notice

Part 2 Programs that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Part 2 Programs will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary

In addition to notifying affected individuals and the media (where appropriate), Part 2 Programs must notify the Secretary of HHS ("the Secretary") of breaches of unsecured SUD information. Part 2 Programs will notify the Secretary by visiting the HHS website and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, Part 2 Programs must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the Part 2 Program may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches are discovered.

VI. New civil money penalties (CMPs) for violations of Part 2 (§2.3)

The Final Rule aligns Part 2 enforcement and penalties with HIPAA by replacing existing criminal penalties for Part 2 violations with references to the HIPAA enforcement authorities at Social Security Act sections 1176 (related to civil enforcement, including the Civil Monetary Penalty tiers established by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009) and 1177 (related to criminal penalties), thereby establishing specific civil and criminal penalties for violations of the Part 2 rules, as required by the CARES Act. Further, the Final Rule applies the HIPAA Enforcement Rule to violations of Part 2 in the same manner as the Enforcement Rule applies to Covered Entities and Business Associates for violations of HIPAA.

The Final Rule further creates a safe harbor against civil or criminal liability for persons acting on behalf of investigative agencies when, in the course of investigating or prosecuting a Part 2 Program or other person holding Part 2 records (or their employees or agents), the person acting on behalf of the investigative agency may unknowingly

receive Part 2 records without first obtaining the requisite court order. This safe harbor is limited to only instances where records are obtained for the purposes of investigating a program or person holding the record, not a patient.

Investigative agencies must follow Part 2 requirements for obtaining, using, and disclosing Part 2 records as part of an investigation or prosecution; such requirements include seeking a court order, filing protective orders, maintaining security for records, and ensuring that records obtained in program investigations are not used in legal actions against patients who are the subjects of the records. The limitation on liability is available for uses or disclosures inconsistent with Part 2 when the person acted with reasonable diligence to determine in advance whether Part 2 applied to the records or program. "Reasonable diligence" requires acting within a reasonable period of time but no more than 60 days prior to the request for records or placement of an undercover agent or informant. "Reasonable diligence" also includes taking the following actions to determine whether a health care practice or provider (where it is reasonable to believe that the practice or provider provides SUD diagnostic, treatment, or referral for treatment services) provides such services by (1) checking a prescription drug monitoring program in the state where the provider is located, if available and accessible to the agency under state law; or (2) checking the website or physical location of the provider.

VII. Greater restrictions against the use and disclosure of records in civil, criminal, administrative, and legislative proceedings against patients (§2.13, 2.63, 2.64, 2.65) and new limitation on liability for government agencies that investigate and prosecute Part 2 Programs and unknowingly receive records subject to Part 2 (§§2.66, 2.67, 2.68)

Under the existing regulation at §2.13, confidentiality restrictions and safeguards apply to how Part 2 records may be used and disclosed, and specifically provides that Part 2 records may not be used and disclosed in any civil, criminal, administrative, or legislative proceedings. Unconditional compliance is required by Part 2 Programs and Lawful Holders and restricts the ability of programs to acknowledge the presence of patients at certain facilities. Accordingly, Part 2 Programs and other Lawful Holders were already required to have in place formal policies and procedures to reasonably protect against unauthorized uses and disclosures of patient identifying information and to protect against reasonably anticipated threats or hazards to the security of patient identifying information. The provisions applied to paper records and electronic records. While the Final Rule applies breach notification requirements to "unsecured records" in the same manner as they currently apply to "unsecured PHI" in the Breach Notification Rule, including specific requirements related to the manner in which breach notification is provided (see §2.16), HHS has not made any additional modifications to align the HIPAA Security Rule and Part 2 at this time.

Revisions to the existing regulation text at §§2.63, 2.64, and 2.65 clarify and expand protections for patients from the unauthorized use of Part 2 records against them in civil, criminal, administrative, and legislative proceedings. Specifically, the intent of §2.63 is to protect communications that are narrow in scope and limited to statements made by a

patient to a Part 2 Program in the course of diagnosis, treatment, or referral for treatment by requiring a court order to authorize disclosure. Although such disclosure is only permitted under circumstances of serious harm or when a patient "opens the door" in legal proceedings, HHS clarifies that an applicant is not restricted from seeking a court order and subpoena authorizing and compelling disclosure, respectively, of information that is broader than that governed by §2.63, such as information contained in records subject to disclosure under §2.64.

Under §2.64, the Final Rule expands the forums for which a court order must be obtained, absent written patient consent, to permit the use and disclosure of records in civil, administrative, or legislative proceedings. The Final Rule also applies the requirement for the court order to "testimony" relaying information within the records, in addition to the records themselves. Of note, HHS clarified that, although a Covered Entity or Business Associate may redisclose records obtained pursuant to a TPO consent "in accordance with the HIPAA Rules," any person seeking to redisclose such records or information in a proceeding against the patient is required to obtain the Part 2 court order or a separate consent of the patient. If the underlying proceedings are not against the subject of the records or "patient," the Covered Entity would be permitted to redisclose the records in accordance with the HIPAA Privacy Rule permission at 45 C.F.R. §164.512(e).

Further, under §2.65, the Final Rule expands the types of criminal proceedings subject to the existing court order requirement, as criminal investigations may be carried out by executive agencies and legislative bodies as well as in criminal prosecutions through the judicial process. The changes widen the scope of confidentiality protections for patients in all of the forums where an investigation or action may be brought against them. The Final Rule also expressly permits disclosures and uses of records and testimony in legal proceedings against the patient if a patient consents.

The Final Rule also amends § 2.66 to add a new paragraph (a)(3) that details procedures for investigative agencies to follow in the event they unknowingly obtain Part 2 records during an investigation or prosecution of a Part 2 Program or person holding Part 2 records. Specifically, the Final Rule requires an investigative agency that discovers in good faith that it has obtained Part 2 records to secure the records according to 2.16 and cease using or disclosing them until it obtains a court order authorizing the use and disclosure of the records and any records later obtained.

Section 2.68 requires investigative agencies to file an annual report with the Secretary of the applications filed for court orders after the use or disclosure of records in an investigation or prosecution of a program or holder of records under 2.66(a)(3)(ii) and after placement of an undercover agent or informant under 2.67(c)(4).