AN A.S. PRATT PUBLICATION
SEPTEMBER 2024
VOL. 10 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 7** **September 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Deneil C. Targowski at ..... (908) 673-3380
Email: ..... Deneil.C.Targowski@lexisnexis.com
For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at ..... (800) 833-9844
Outside the United States and Canada, please call ..... (518) 487-3385
Fax Number ..... (800) 828-8341
LexisNexis® Support Center ..... https://supportcenter.lexisnexis.com/app/home
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (518) 487-3385

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY &CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [7] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [179] (LexisNexis A.S. Pratt)

An A.S. Pratt Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report*, LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

HHS's CARES Act Final Rule Better Aligns Part 2 Substance Use Disorder Patient Records Confidentiality Regulations With HIPAA

By Jennifer Geetter, Daniel Gottlieb, Li Wang, Edward Zacharias and Kyle Hafkey*

In this article, the authors examine a final rule amending the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations under 42 C.F.R. Part 2, applicable to certain federally assisted SUD treatment programs, to implement Section 3221 of the Coronavirus Aid, Relief, and Economic Security Act.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and the Substance Abuse and Mental Health Services Administration (SAMHSA) have jointly issued a final rule[1] to amend the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations under 42 C.F.R. Part 2 (Part 2), applicable to certain federally assisted SUD treatment programs (Part 2 Programs), to implement Section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[2]

The final rule modifies longstanding restrictions under Part 2. It newly permits disclosures of SUD patient records (Part 2 Records) for treatment, payment and health care operations purposes under a general consent and makes other changes to align Part 2's record requirements with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) privacy, breach notification and enforcement regulations applicable to protected health information (PHI).

OCR Director Melanie Fontes Rainer said, "The Final Rule strengthens confidentiality protections while improving care coordination for patients and providers. Patients can seek needed treatment and care for substance use disorder knowing that greater protections are in place to keep their records private, and providers can now better share information to improve patient care."

The final rule compliance date is February 16, 2026, giving entities two years to make the necessary updates to their privacy, security and information-sharing practices.

KEY CHANGES TO PART 2

The final rule includes the following key changes:

- Applies HIPAA penalty provisions to violations of Part 2 in accordance with authority under the CARES Act.

---

* The authors, attorneys with McDermott Will & Emery, may be contacted at jgeetter@mwe.com, dgottlieb@mwe.com, lwang@mwe.com, ezacharias@mwe.com and khafkey@mwe.com, respectively.

[1] https://www.govinfo.gov/content/pkg/FR-2024-02-16/pdf/2024-02544.pdf.

[2] https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf.

- Allows Part 2 Programs to obtain a single consent from patients for all future uses and disclosures of Part 2 patient identifying information for treatment, payment and health care operations purposes.

- Applies the HIPAA Breach Notification Rule to Part 2 Programs with respect to breaches of unsecured Part 2 patient records in the same manner that the Breach Notification Rule applies to a HIPAA covered entity with respect to breaches of unsecured PHI.

- Expands the definition of qualified service organizations (QSOs) to include HIPAA business associates when the QSO is a business associate of a covered entity that is also a Part 2 Program and the PHI to be disclosed to the QSO is a Part 2 record.

- Appears to impose requirements for de-identification of Part 2 patient identifying information that go beyond HIPAA Privacy Rule requirements, requiring that the data not only be de-identified but also aggregated, despite purporting to harmonize de-identification standards under the Privacy Rule and Part 2.

CIVIL AND CRIMINAL PENALTIES FOR PART 2 VIOLATIONS

Prior to the adoption of the CARES Act, the Public Health Service Act did not permit HHS to issue civil money penalties for violations of Part 2. Instead, it authorized the US Attorney of the appropriate jurisdiction to initiate criminal charges against persons or entities that violated Part 2 and to seek fines under a US Criminal Code provision, which limits fines for infractions to $5,000 per violation for individuals and $10,000 per violation for organizations. We are not aware of any criminal prosecution under that authority.

Under the CARES Act, Congress gave HHS the authority to issue civil money penalties for violations of Part 2 in accordance with the penalty provisions established for HIPAA violations. The final rule amends Part 2 to apply the HIPAA enforcement authorities, including the civil money penalty and criminal provisions as implemented by the HIPAA Enforcement Rule. As a result, violations of Part 2 requirements by Part 2 Programs are subject to potential civil monetary penalties as established under HIPAA. This change means that HIPAA business associates and covered entities are subject to enforcement actions by HHS for Part 2 violations in addition to HIPAA violations. HIPAA also authorizes state attorneys general to bring civil enforcement actions, such as seeking an injunction against the offender or damages for those harmed.

Stakeholders should be aware of the impact of this expanded enforcement framework, which will make enforcement of Part 2 more likely, resulting in potential civil monetary penalties. The final rule does not make clear whether SAMHSA (the HHS agency that is currently responsible for Part 2) or OCR (the HHS agency that enforces HIPAA) will be responsible for imposing civil monetary penalties for violations of Part 2 against

Part 2 Programs that are not covered entities or business associates. Instead, the final rule preamble states that HHS will identify the enforcing agency before the final rule compliance date.

Additionally, the CARES Act and the final rule replace the criminal enforcement actions previously available for Part 2 violations (and discussed above) with actions under Section 1177 of the Social Security Act, including imprisonment of up to 10 years or fines of up to $250,000, depending on the severity and intent of the violation. The U.S. Department of Justice is responsible for criminal enforcement actions.

CONSENT REQUIREMENTS

Single Consent for Future TPO and Consent Requirements

Unlike HIPAA, Part 2 requires Part 2 Programs to obtain a patient's consent for uses and disclosures of Part 2 Records for treatment, payment and health care operations purposes (TPO). The final rule amends the Part 2 consent requirements to decrease the burden on Part 2 Programs and facilitate the exchange of Part 2 Records for TPO. These changes include:

- Allowing Part 2 Programs to obtain a single consent from patients for all future uses and disclosures of Part 2 patient identifying information for TPO, including redisclosures of Part 2 information by recipients of the information under the single consent until such time that the consent expires or is revoked (if any).
- Aligning the required elements of a Part 2 consent with those required for a valid HIPAA authorization.
- Permitting Part 2 Programs to include in the consent an *opt-out* to receiving fundraising communications from the program.

Redisclosure By Recipient/Lawful Holder Pursuant to General Consent for TPO

If a Part 2 patient consents to a use or disclosure of Part 2 Records for TPO pursuant to a valid Part 2 consent, the recipient (also called a lawful holder) may redisclose the records as follows:

- When records are disclosed for TPO activities to a HIPAA covered entity or business associate, the covered entity or business associate may further disclose the records in accordance with HIPAA, except for uses and disclosures for civil, criminal, administrative and legislative proceedings against the patient.
- When records are disclosed with consent given once for all future TPO activities to a Part 2 Program that is not a covered entity or business associate, the Part 2 Program may further disclose those records consistent with the consent.

- When records are disclosed for payment or health care operations activities to a lawful holder that is not a covered entity or business associate, the lawful holder may further disclose the records as may be necessary for its contractors, subcontractors or legal representatives to carry out the payment or health care operations specified in the consent on behalf of such lawful holders.

In the third scenario, the lawful holder that is not a covered entity or business associate – and that wants to redisclose Part 2 patient identifying information – must have in place a written contract or comparable legal instrument with the contractor or legal representative. That contract must provide that the contractor, subcontractor or legal representative is fully bound by Part 2 upon receipt of the patient identifying information. In making any such redisclosures, the lawful holder must furnish the recipients with a notice statement (discussed below) and require the recipients to implement appropriate safeguards to prevent unauthorized uses and disclosures. It must also require the recipients to report any unauthorized uses, disclosures or breaches of patient identifying information to the lawful holder.

The lawful holder may only redisclose information to the contractor, subcontractor or legal representative that is necessary for such recipient to perform its duties under the contract or legal instrument. Contracts may not permit a contractor, subcontractor or legal representative to redisclose information to a third party unless that third party is a contract agent of the contractor or subcontractor, helping them provide services described in the contract – and only as long as the agent only further discloses the information back to the contractor or lawful holder from which the information originated.

Elements Required for a Valid Consent Form

HHS amends the requirements for a valid consent form under Part 2 to better align them with the requirements for a valid authorization under HIPAA. Under the final rule, a valid consent form must include the following elements:

- Name of the Part 2 patient.
- Name or other specific identification of the persons, or class of persons, authorized to make the requested use or disclosure.
- Specific and meaningful description of the information to be used or disclosed. The final rule preamble indicates that "my substance use disorder treatment records" would meet the standard, but states that the description "my medical records" is insufficient.
- Name(s) of the person(s), or class of persons, to which a disclosure is to be made. For a single consent for all future uses and disclosures for TPO, the recipient may be described as "my treating providers, health

plans, third-party payers, and those helping operate this program" or a similar statement. If the recipient is a covered entity or business associate to whom information is disclosed for purposes of TPO, a consent must include the statement that the patient's information may be redisclosed in accordance with the permissions contained in the HIPAA regulations, except for uses and disclosures for civil, criminal, administrative or legislative proceedings against the patient. The final rule also includes additional requirements for designating recipients when the recipient is an intermediary.

- Description of each purpose for which information may be used or disclosed. The statement "for treatment, payment and health care operations" is a sufficient description when a patient provides consent once for all such future uses or disclosures for those purposes. The statement "at the request of the patient" is a sufficient description when a patient initiates the consent and does not provide a statement of the purpose. If a Part 2 Program intends to use or disclose records to fundraise on its own behalf, the consent must include a statement about the patient's right to elect not to receive any fundraising communications.

- Statement that the patient has the right to revoke the consent in writing (except to the extent that the Part 2 Program or other lawful holder of patient identifying information that is permitted to make the disclosure has already acted in reliance on it), and how the patient may revoke consent.

- Expiration date or event that relates to the Part 2 patient or the purpose of the use or disclosure. The final rule provides that "end of the treatment," "none" or similar language is sufficient if the consent is for a use or disclosure for TPO. Importantly, "none" or similar language allows TPO consents to remain in place until revoked.

- Signature of the patient or other person authorized to give consent. Electronic signatures are permitted to the extent that they are permitted by any applicable law.

- Notice statement advising the patient of the potential for the records used or disclosed pursuant to the consent to be subject to redisclosure by the recipient and no longer protected by Part 2.

- Notice statement advising the patient of the consequences to the patient of a refusal to sign the consent. HHS states in the final rule preamble that a Part 2 Program may condition the provision of treatment on the patient's consent to disclose information as needed (e.g., to make referrals to other providers, obtain payment from a health plan – unless the patient has paid in full – or conduct quality review of services provided). This is inconsistent with the HIPAA Privacy Rule's authorization requirements,

but HIPAA does not require a patient's authorization to use or disclose PHI for TPO.

Separate Consents: SUD Counseling Notes and Part 2 Records in Legal Proceedings

The final rule adopts requirements for the disclosure of SUD counseling notes that are similar to the HIPAA Privacy Rule's protections around the disclosure of psychotherapy notes, requiring a separate consent for the disclosure of SUD counseling notes and specifically prohibiting combining a consent for disclosure of SUD counseling notes with a consent for disclosure of any other type of health information (other than psychotherapy notes).

Similarly, the final rule requires a separate consent for the use and disclosure of Part 2 Records in civil, criminal, administrative or legislative proceedings.

Copy of Consent and Notice Statement to Accompanying Disclosure Under Consent

When disclosing Part 2 Records to a third party pursuant to a consent, disclosure must be accompanied by a copy of the consent or a clear explanation of the scope of the consent, which must travel with each disclosure of records for which a consent is required. In addition, each disclosure made pursuant to a patient's consent must be accompanied by one of the following statements:

> This record which has been disclosed to you is protected by Federal confidentiality rules (42 CFR part 2). These rules prohibit you from using or disclosing this record, or testimony that describes the information contained in this record, in any civil, criminal, administrative, or legislative proceedings by any Federal, State, or local authority, against the patient, unless authorized by the consent of the patient, except as provided at 42 CFR 2.12(c)(5) or as authorized by a court in accordance with 42 CFR 2.64 or 2.65. In addition, the Federal rules prohibit you from making any other use or disclosure of this record unless at least one of the following applies:
>
> (i) Further use or disclosure is expressly permitted by the written consent of the individual whose information is being disclosed in this record or as otherwise permitted by 42 CFR part 2.
>
> (ii) You are a covered entity or business associate and have received the record for treatment, payment, or health care operations, or
>
> (iii) You have received the record from a covered entity or business associate as permitted by 45 CFR part 164, subparts A and E.

A general authorization for the release of medical or other information is NOT sufficient to meet the required elements of written consent to further use or redisclose the record (see 42 CFR 2.31).

Or:

42 CFR part 2 prohibits unauthorized use or disclosure of these records.

No Segregation of Part 2 Records From Other PHI

Under the final rule, Part 2 Programs, covered entities and business associates that receive records based on a single consent for all future uses and disclosures for TPO are no longer required to segregate Part 2 Records from other PHI, but the information is still considered a Part 2 Record. HHS specifically declined to permit records received under a consent for TPO to be treated as non-Part 2 Records, stating that recipients must still comply with the continuing prohibition on use and disclosure of such records in investigations or proceedings against the patient, absent written consent or a court order. However, if the recipient of the Part 2 Records under a consent for TPO is a Part 2 Program, covered entity or business associate, it may redisclose the data for TPO as permitted by HIPAA, including to a subcontractor business associate. In addition, HHS requires entities to attach a copy of the patient consent to disclosures.

QUALIFIED SERVICE ORGANIZATIONS

Part 2's use and disclosure restrictions do not apply to the communications between Part 2 Programs and their QSOs under an agreement meeting the Part 2 requirements for a QSO agreement (QSOA).

HHS acknowledges that the relationship between a Part 2 Program and a QSO is analogous to the relationship between a covered entity and business associate under HIPAA. Accordingly, in the final rule, HHS expands the definition of QSOs to include business associates when (1) the PHI in question also constitutes a Part 2 record and (2) the QSO meets the definition of a business associate of a covered entity that is also a Part 2 Program.

In the final rule preamble commentary, HHS reconfirms its prior guidance that a QSO may redisclose Part 2 patient identifying information to the QSO's "contract agents" because they are treated as the QSO when providing services described in the underlying QSOA. In addition, a QSO may redisclose patient identifying information to any subcontractors that are not contract agents in accordance with the patient's consent for future TPO. It is not clear under the HHS guidance when a subcontractor qualifies as a "contract agent," since that term (unlike the terms "agent" and "independent contractor") does not have a well-understood meaning under federal or state law.

CONSENT FOR MINOR PATIENTS

The final rule defers to state law regarding whether a minor patient can consent to care governed by Part 2. If a minor patient can independently, without the knowledge or participation of a consenting adult (i.e., a parent, guardian or other legal representative), provide consent to obtain SUD treatment, then only the minor can provide written consent for use or disclosure of Part 2 Records in such cases where consent is required.

If state law requires the consent of a consenting adult for the minor to obtain SUD treatment, consent for disclosure of Part 2 Records must be given by both the consenting adult and the patient.

If state law requires the consent of a consenting adult for treatment, the fact that a minor has sought treatment may only be communicated to such consenting adult if the minor lacks the capacity to make a rational choice regarding such consent. The final rule clarifies that such assessment is made by the Part 2 Program director. Further, the final rule clarifies that this assessment is a clinical evaluation as to decision-making capacity, but it is not a determination as to the legal question of whether the minor may make independent decisions.

Relatedly, a Part 2 Program may disclose information relevant to reducing a substantial threat to the life or physical well-being of the minor seeking treatment to the consenting adult or any other person authorized by state law to act on behalf of the minor if:

- The Part 2 Program director determines that the minor "lacks capacity because of extreme youth, or mental or physician condition to make a rational decision on whether to consent to a disclosure," or
- The minor poses a substantial threat to their own life or physical well-being, or that of any other person, and such risk may be reduced by communicating relevant facts to the consenting adult or other authorized individual.

Given that these assessments are foreseeable, Part 2 Programs should consider developing evaluation protocols and documentation.

CONSENT FOR PATIENTS WHO LACK CAPACITY AND DECEASED PATIENTS

The final rule amends Part 2 to clarify substitute decision-making for adult and emancipated minor patients to require a personal representative to give consent for health care decisions for such a patient who a court has determined lacks decision-making capacity for health care decisions. The final rule defines a personal representative as a person with authority under applicable state or other law to make decisions related to health care for the patient. The personal representative would have authority only with respect to Part 2 Records relevant to such personal representation.

In the case of an adult or emancipated minor patient who has not been adjudicated to lack decision-making capacity, but who (for any length of time) suffers from a medical condition that prevents knowing or effective action on their own behalf, the Part 2 Program director may provide substitute consent to the use or disclosure of Part 2 Records for the patient, but only for the purpose of obtaining payment from insurance.

In the case when consent is sought on behalf of a decedent for the use of disclosure of Part 2 Records pertaining to such individual, the personal representative is authorized to provide such consent.

USE OF DE-IDENTIFIED INFORMATION FOR RESEARCH

The final rule purports to harmonize the de-identification standard for Part 2 with the HIPAA Privacy Rule's de-identification standards in the research context. It provides that a researcher using Part 2 patient identifying information for research may include data in research reports only if:

- The information has been de-identified in accordance with the HIPAA de-identification standards,
- There is no reasonable basis to believe that the information can be used to identify a patient, and
- The data is only in aggregate form.

While the final rule provision references the Privacy Rule's de-identification standard, it also requires that the information be included in publication only in "aggregate form," which is arguably a requirement that can (in some cases) go beyond the de-identification standards in HIPAA, which allows individual patient-level data (rather than aggregate data) in certain cases. In the final rule preamble commentary, HHS explained that the aggregation requirement applies to disclosure of data in reports, not the use of such data for research, and therefore HHS determined that the additional safeguard was appropriate. In most cases, research reports and publications traditionally present aggregate data (e.g., total counts or percentages) but there could be instances in which de-identified line-item data would be appropriate (e.g., in chart form). Part 2 Programs will need to consider whether such reports are sufficiently aggregated to meet this stricter standard.

In addition, the final rule provision requires that there be no reasonable basis to believe that data in a research report could be used to identify a patient. It is not clear whether that standard is consistent with the "very small" residual risk requirement of the Privacy Rule's expert determination de-identification method or the safe harbor method that requires removal of 18 HIPAA identifiers.

The final rule permits the use and disclosure of Part 2 patient identifying information for scientific research, provided that the Part 2 Program's director, managing director, or person otherwise vested with authority to act as chief executive officer determines that the recipient of the information is a covered entity or business associate that has obtained the research subject's authorization, or an institutional review board's or other privacy board's waiver of the authorization requirement in accordance with HIPAA. Further, if the Part 2 Program is a HIPAA covered entity or business associate, the use and disclosure of such data must be made in accordance with the Privacy Rule's provisions governing research. The final rule does not appear to permit, however, uses and disclosures of patient identifying information for research purposes with a research partner that is not a covered entity or business associate.

Recipients of such data may not redisclose the identifying information and may only include data that is aggregated and de-identified in any research reports. Researchers may

obtain patient identifying information that is linked to data sets from data repositories, provided that such linked data is only used for research as permitted by the final rule.

DISCLOSURES TO PUBLIC HEALTH AUTHORITIES

The final rule permits the disclosure of records without patient consent to public health authorities but, unlike the HIPAA Privacy Rule, only permits the disclosure of records that are de-identified in accordance with the Privacy Rule's de-identification standard, such that there is no reasonable basis to believe that the information can be used to identify a patient. HHS stated in preamble guidance that, once Part 2 Records are de-identified for disclosure to public health authorities, Part 2 requirements no longer apply to such de-identified records. The definition of "public health authority" is identical to the definition of the term under the Privacy Rule. Accordingly, Part 2 Programs should be careful when making public health authority disclosures, given that the HIPAA exception for disclosures to public health authorities does not require de-identification.

SECURITY OF PART 2 PATIENT IDENTIFYING INFORMATION

The final rule amends Part 2's information security provision to require Part 2 Programs and other lawful holders to have formal policies and procedures in place to reasonably protect Part 2 patient identifying information against unauthorized uses and disclosures, and from reasonably anticipated security threats or hazards. The policies must address certain standard security practices for sensitive information.

For paper Part 2 Records, the final rule requires that policies and procedures address transferring and removing records, destroying records such that patient identifying information is non-retrievable, and maintaining the records in a secure place when not in use.

For electronic records, the policies and procedures must address creating, receiving, maintaining, transmitting, using and accessing the records, as well as destroying the records to render the patient identifying information non-retrievable.

For both paper and electronic records, the policies must address de-identifying patient identifying information in accordance with the Privacy Rule's de-identification standard such that there is no reasonable basis to believe that the information could be used to identify a particular Part 2 patient. While the final rule intends to align Part 2's and the HIPAA Privacy Rule's de-identification standards, this provision includes the additional requirement that there be no reasonable basis to believe that the information could be used to identify a particular patient as having or as having had an SUD. It is not clear whether the additional requirement is consistent with the "very small" risk of re-identification standard used in the expert determination method of de-identification under the Privacy Rule.

Part 2 Programs that are covered entities must also secure Part 2 patient identifying information that is PHI in accordance with the Privacy Rule's reasonable safeguards requirements and electronic PHI in accordance with the Security Rule.

BREACH NOTIFICATION

The final rule requires Part 2 Programs to comply with the HIPAA Breach Notification Rule with respect to breaches of unsecured records in the same manner that a HIPAA covered entity must comply with the Breach Notification Rule with respect to breaches of unsecured PHI. While certain Part 2 Programs previously were not subject to the Breach Notification Rule (because they were not HIPAA covered entities or business associates), the final rule requires all Part 2 Programs to comply with the Breach Notification Rule.

While the final rule aligns the Breach Notification Rule obligations of Part 2 Programs and covered entities, the final rule does not require QSOs to report breaches of unsecured Part 2 Records to Part 2 Programs in the same manner that business associates must report breaches of unsecured PHI to covered entities. Instead, HHS expects – but does not require – a Part 2 Program to contractually obligate a QSO to report breaches to the Part 2 Program (e.g., within a QSOA). Further, if a QSO is also a business associate of a Part 2 Program that is a HIPAA covered entity, the Breach Notification Rule requires the QSO to report breaches to the Part 2 Program.

HHS has indicated that it is considering a new reporting process with regard to a Part 2 Program's notification obligations and noted this new process will (1) emphasize bringing entities into compliance with Part 2 and (2) avoid duplicative reporting by Part 2 Programs that may have triggered both Part 2 and HIPAA breach notification requirements.

PART 2 PATIENT NOTICE

Part 2 currently requires a Part 2 Program to provide patients with a notice (Patient Notice) of its Part 2 compliance obligations that includes content that is less comprehensive than the content that the HIPAA Privacy Rule requires for a Notice of Privacy Practices (NPP). The CARES Act requires HHS to harmonize the Patient Notice and NPP requirements and to modify the current NPP requirements to address Part 2 Records transmitted to or maintained by a covered entity.

To implement the CARES Act requirement, the final rule aligns Part 2 requirements for Patient Notices with the Privacy Rule's NPP requirements. The final rule requires that Part 2 Programs provide Patient Notices that meet certain content requirements, including:

- Header that includes text that is nearly identical to the header that the Privacy Rule requires for an NPP, as well as other notice statements.
- Descriptions of each purpose for which the Part 2 Program is permitted or required to use or disclose records without the patient's written consent, subject to any other laws that are more stringent than Part 2.
- Statement that a patient may provide a single consent for all future uses or disclosures for treatment, payment and health care operations purposes.

- Statements of patient rights with respect to Part 2 Records.
- Statements describing certain duties of a Part 2 Program.
- Notice that a patient may file a complaint with the Part 2 Program and the HHS Secretary regarding the Part 2 Program.
- Contact information for questions about the Patient Notice.

HHS intends to modify the Privacy Rule's NPP requirements as part of a future HIPAA rulemaking. The final rule only adopts requirements for Patient Notices.

REQUESTED RESTRICTIONS ON USE AND DISCLOSURE OF SUD INFORMATION

The final rule gives patients the right to request restrictions on disclosures of Part 2 Records for TPO purposes. In addition, a Part 2 Program must agree to patient requests for restrictions on the disclosure of Part 2 Records to a health plan if the disclosure is for the purpose of carrying out payment or health care operations and is not otherwise required by law, and if the record pertains solely to a health care item or service for which a patient self-paid in full. A Part 2 Program is not otherwise required to agree to all patient requests for restrictions.

The final rule states that, even if a Part 2 Program has agreed to a patient's request for restrictions on the use and disclosure of Part 2 Records, it may use or disclose information in the records to provide treatment to a patient who needs emergency treatment if the restricted record is needed to provide the emergency treatment. In such cases, the Part 2 Program must request that any health care provider who received Part 2 information not further use or disclose the information.

ACCOUNTING OF DISCLOSURES

The final rule creates a new patient right to an accounting of all disclosures that the Part 2 Program made with consent under Part 2 in the three years prior to the date of the patient's request (or a shorter time period chosen by the patient). The accounting must meet the Privacy Rule's requirements for content and provision of an accounting of accountable disclosures of PHI.

Additionally, the final rule requires a Part 2 Program to provide an accounting of its TPO disclosures made through an electronic health record (EHR) up to three years prior to the date of request (if HHS implements a similar requirement for disclosures of PHI for TPO under the Privacy Rule in the future). This right to request an accounting of TPO disclosures reflects Congress's directive under the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. However, HHS has not yet finalized the HITECH requirements due to stakeholder feedback to a proposed rule issued by OCR in 2011.

Accordingly, the effective date and compliance date of the accounting of disclosures requirements for Part 2 are tolled until the effective date and compliance date of those modifications to the Privacy Rule's accounting of disclosures standard.

There are no plans under the current regulatory agenda for HHS to implement the HITECH modifications.

Accordingly, it is unclear if or when the accounting of TPO disclosures requirement will become effective.

REQUIREMENTS FOR INTERMEDIARIES

Part 2 currently imposes certain privacy requirements on intermediaries that receive Part 2 Records, but it does not define the term "intermediaries." The final rule adds a definition and new requirements for these entities.

The final rule defines an intermediary as a person (other than a Part 2 Program, covered entity or business associate) who has received Part 2 Records under a general designation in a written patient consent to be disclosed to one or more of its member participant(s) who has a treating provider relationship with the patient. The definition is based on the function of the person or entity receiving Part 2 Records and not based on the title or category of the entity's business.

According to HHS, an intermediary could be a research institution providing treatment, an accountable care organization, or a care coordination or care management organization. HHS also clarified that a health app providing individual patients with access to their records would not be considered an intermediary unless it is also facilitating the exchange of Part 2 Records from a Part 2 Program to other treating providers using a general designation in a consent.

Under the final rule, upon request, an intermediary must give patients who have consented to the disclosure of their records using a general designation a list of persons to whom their records have been disclosed pursuant to the general designation. Patient requests must be made in writing and must be limited to disclosures made within the past three years. The intermediary must respond within 30 days of receipt of the written request and provide, for each disclosure, the names of the entities to which the disclosure was made, the date of the disclosure and a brief description of the patient identifying information disclosed.

HHS expects far fewer entities (such as health information exchanges (HIEs)) to be subject to the rule's intermediary consent requirements and the list of disclosures obligations, because the final rule excludes business associates from the intermediary definition.

HHS intends for the final rule's changes to encourage HIEs to accept Part 2 Records and include Part 2 Programs as HIE participants, facilitating the integration of behavioral health information with other medical records.

COMPLAINTS OF NONCOMPLIANCE

The final rule amends Part 2 to require a Part 2 Program to implement a process to receive complaints concerning the program's compliance with Part 2 and makes other changes consistent with requirements applicable to HIPAA Privacy Rule complaints. It also adds a new provision permitting patients to file complaints with the HHS Secretary in the same manner as under the Privacy Rule, prohibits Part 2 Programs from taking adverse actions against patients who file complaints, and prohibits requiring patients to waive their right to file a complaint as a condition of providing treatment, enrollment, payment or eligibility for services.

NEXT STEPS

Part 2 Programs, QSOs and health plans should consider the following next steps to implement compliance with the final rule.

Organizations with Part 2 programs should consider:

- Revising their Patient Notice to address new final rule requirements.
- Evaluating and revising consent forms for Part 2 Records to transition to a single consent for all future TPO activities.
- Determining how to differentiate, in EHR systems and other systems, among (1) PHI subject to HIPAA and not Part 2, (2) PHI subject to Part 2 but for which a patient has provided a single TPO consent and (3) PHI subject to Part 2 and a consent with a more limited scope than all future TPO activities.
- Evaluating whether to share Part 2 patient identifying information for treatment or other purposes through HIEs pursuant to a consent.
- Reviewing, and updating as necessary, information security policies and procedures to address the final rule's new information security requirements.
- Updating their policies and procedures regarding requested restrictions on the use of PHI for TPO to address final rule requirements.
- Updating their accounting of disclosure policies and procedures to address new requirements.
- Updating their incident response plan to address breach notification obligations.
- Updating their complaint policy to address the final rule requirements for a complaint process.

- Updating policies on substitute decision-making to address final rule provisions regarding consent for minors, patients who lack capacity to make health care decisions and decedents.

QSOs should consider:

- Requiring Part 2 Programs to request a general consent for future TPO purposes to facilitate redisclosures to the QSO's subcontractors that are not contract agents.
- Analyzing and monitoring their notification obligations and liability under QSOAs governing their relationships with Part 2 Programs.

Health plans that receive Part 2 patient identifying information should consider:

- Requiring participating providers with Part 2 Programs to ask patients to sign a general consent for future TPO purposes as part of their intake processes.
- Adopting policies and procedures to address Part 2 requirements applicable to lawful holders.