AN A.S. PRATT PUBLICATION
MAY 2024
VOL. 10 NO. 4

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

Pratt's Privacy & Cybersecurity Law Report

VOLUME 10 **NUMBER 4** **May 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.

Substance Use Disorder Confidentiality Regulations Modified to Align with HIPAA

By Beth Neal Pitman and Eddie Williams III*

In this article, the authors summarize the significant changes to the Part 2 Regulations that were recently published, as finalized by the Department of Health and Human Services, Office for Civil Rights in coordination with the Substance Abuse and Mental Health Services Administration.

After more than a year since the U.S. Department of Health and Human Services' (HHS) Office for Civil Rights (OCR) and Substance Abuse and Mental Health Services Administration (SAMHSA) issued the proposed changes to the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations (known as Part 2 of the Part 2 Regulations) through a Notice of Proposed Rulemaking,[1] these agencies have now finalized such rules to better harmonize the Part 2 Regulations with certain requirements under the Heath Insurance Portability and Accountability Act of 1996 (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act.

In the midst of the COVID-19 pandemic, Congress passed Section 3221 of the Coronavirus Aid, Relief, and Economic Security (CARES) Act, which, in addition to providing relief during the public health emergency (PHE), amended the federal statute that establishes the protections for the confidentiality of SUD patient records. In addition, the HHS Secretary was charged with amending the Part 2 Regulations to align certain of its provisions with HIPAA and HITECH for purposes of reducing burden on providers and providing additional protections to Part 2 patients.

This article is a summary of the significant changes to the Part 2 Regulations published on February 16, 2024, as finalized by the Department of Health and Human Services, Office for Civil Rights (OCR) in coordination with SAMHSA.

USES AND DISCLOSURES FOR TREATMENT, PAYMENT AND HEALTHCARE OPERATIONS

A Part 2 program may use and disclose SUD records based on a single prior consent signed by the patient for all future uses and disclosures for treatment, payment and healthcare operations (TPO). Such consent must advise the patient regarding the potential for the records to be redisclosed and no longer be subject to protection under

* The authors, attorneys with Holland & Knight LLP, may be contacted at Beth.Pitman@hklaw.com and Eddie.Williams@hklaw.com, respectively.

[1] https://www.govinfo.gov/content/pkg/FR-2022-12-02/pdf/2022-25784.pdf.

the Part 2 rules. In addition, the consent must advise the patient of the consequences for refusal to sign.

When a patient provides a single consent for all future uses and disclosures for TPO, a recipient who is a HIPAA-covered entity or business associate may use and disclose such SUD records as permitted by HIPAA until such time as the patient revokes the consent in writing. When SUD records are disclosed pursuant to a single consent for all future TPO activities to a Part 2 program that is not a covered entity or business associate, the Part 2 program may use and disclose such records in accordance with the consent. The Part 2 program, covered entity or business associate is still prohibited from using and disclosing the SUD records for civil, criminal, administrative and legislative proceedings against the patient.

When SUD records are disclosed for payment and healthcare operations activities to a lawful holder that is not a covered entity or business associate, the recipient may redisclose such records as may be necessary for its contractors, subcontractors or legal representatives to carry out the payment or healthcare operations specified in the consent. However, such lawful holders who wish to redisclose patient identifying information must have in place a written contract or comparable legal instrument with the contractor or voluntary legal representative, which provides that the contractor, subcontractor or voluntary legal representative is fully bound by the provisions of Part 2.

In addition, a lawful holder must provide the recipient the required notice regarding the prohibition on redisclosures, require recipients to implement appropriate safeguards to prevent unauthorized uses and disclosure and require recipients to report any unauthorized uses, disclosures or breaches of patient identifying information to the lawful holder.

BREACH NOTIFICATION

The final rule incorporates HIPAA's breach notification rule into the Part 2 Regulations.

Specifically, Part 2 programs, including those not directly regulated by HIPAA, are now required to comply with the HIPAA breach rule with respect to breaches of unsecured Part 2 records in the same manner as the breach rule applies to a covered entity with respect to breaches of unsecured protected health information. Unsecured Part 2 records mean any record that is not rendered unusable, unreadable or indecipherable to unauthorized persons through the use of a technology or methodology specified by the HHS Secretary in the guidance issued under Public Law 111-5, Section 13402(h)(2).

NOTICE OF PRIVACY PRACTICES

The final rule modifies the Part 2 patient confidentiality notice requirements to closely mirror the HIPAA notice of privacy practices (NPP) requirements. In addition to requiring a statement that a patient may provide a single consent for all future uses or disclosures for TPO, the notice must provide that records that are disclosed to a Part

2 program, covered entity or business associate with the patient's consent for TPO may be further disclosed by such entities without the patient's written consent to the extent the HIPAA regulations permit such disclosure. If a Part 2 program wishes to engage in fundraising activities, the notice must include a statement that the Part 2 program may use or disclose records to fundraise for the benefit for the program only if the patient is first provided a clear and conspicuous opportunity to elect not to receive fundraising communications.

ACCOUNTING OF DISCLOSURES

The final rule requires Part 2 programs to provide a patient, upon request, an accounting of all disclosures made with the patient's consent for the three years prior to the date of the request (or a shorter time period as chosen by the patient). The accounting of disclosures must meet certain requirements under the HIPAA Privacy Rule. An accounting for disclosures of records for TPO is required only where such disclosures are made through an electronic health record. The new accounting of disclosures requirement, however, will not go into effect until the HIPAA regulations are updated to address an accounting of disclosure through an electronic health record as required by the HITECH Act.

RIGHT TO REQUEST PRIVACY PROTECTION FOR RECORDS

Similar to HIPAA, the final rule requires a Part 2 program to permit a patient to request that the program restrict uses and disclosures of the patient's SUD records to carry out TPO, including when the patient has signed written consent for such disclosures.

However, a Part 2 program is not required to agree to a restriction unless the request is to restrict disclosure to a health plan where the disclosure is for the purpose of carrying out payment or healthcare operations and is not otherwise required by law and the record pertains solely to a healthcare item or service for which the patient, or a person other than the health plan on behalf of the patient, has paid the Part 2 program in full.

PENALTIES

The final rule makes HIPAA and HITECH Act civil and criminal penalties applicable to violations of the Part 2 Regulations. The final rule creates a safe harbor from civil and criminal liability for a person acting on behalf of an investigative agency having jurisdiction over the activities of a Part 2 program or other person holding SUD records for a use or disclosure of such records inconsistent with the Part 2 Regulations that occurs while acting within the scope of their employment in the course of the investigation or prosecuting a Part 2 program or person holding the record.

Certain conditions must be satisfied in order for the safe harbor to be available.

ADDITIONAL CONSIDERATIONS; EFFECTIVE AND COMPLIANCE DATES

In addition to the revisions to the Part 2 Regulations discussed above, the final rule also enhances the security and protection for SUD records, including the expansion of the prohibitions on the use and disclosure of such records in civil, criminal, administrative or legislative proceedings conducted by a federal, state or local authority against a patient, absent a court order or the consent of the patient.

The final rule became effective 60 days after being published in the Federal Register, April 16, 2024, and, unless delayed, the proposed compliance date is 24 months after publication of the final rule, except for the accounting of disclosures for TPO through an electronic health record, which is delayed until similar revisions to the HIPAA regulations are finalized. In the interim, Part 2 programs, covered entities and business associates should review their consent and authorization forms, policies and procedures, including privacy notices, and implement or amend them as necessary to comply with the final rule. In addition, these entities should update their training materials and tools and have the staff trained on the new requirements. Part 2 programs will also need to become accustomed to the HIPAA breach notification requirements and establish breach response policies and procedures.

IN SUMMARY

- The OCR and SAMHSA have finalized rules to better align SUD Patient Records Part 2 Regulations with certain requirements of HIPAA and the HITECH Act.
- A Part 2 program may use and disclose SUD records based on a single prior consent signed by the patient for all future uses and disclosures for treatment, payment and healthcare operations.
- The final rules make HIPAA and HITECH Act civil and criminal penalties applicable to violations of the Part 2 Regulations and create a safe harbor from civil and criminal liability for a person acting on behalf of an investigative agency having jurisdiction over the activities of a Part 2 program while providing other protections when other certain conditions are met.
- The Part 2 regulations aligning with HIPAA apply to all Part 2 programs and lawful holders, including those not regulated by HIPAA.