AN A.S. PRATT PUBLICATION
SEPTEMBER 2021
VOL. 7 NO. 7

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 7** **September 2021**

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
Customer Service Web site ..... http://www.lexisnexis.com/custserv/
For information on other Matthew Bender publications, please call

Your account manager or ..... (800) 223-1940
Outside the United States and Canada, please call ..... (937) 247-0293

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 [217] (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

(2021–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.

Emerging Trends in OCR's Right of Access Initiative and Implications for Business Associates

By Melissa M. Crespo, Dan Kagan, and Eleanor C. Anthony*

Under the Right of Access Initiative, the U.S. Department of Health and Human Services Office for Civil Rights has aimed to support individuals' right to timely access of their protected health information and has targeted covered entities' non-compliance with fulfilling HIPAA's right of access requirements. This article analyzes right of access trends and implications and provides recommendations for how business associates may best address their right of access obligations and ensure compliance.

The U.S. Department of Health and Human Services Office for Civil Rights' ("OCR") 2021 enforcement actions started with a bang, with five Right of Access Initiative settlements in the first three months of the year. Under the Right of Access Initiative, OCR has aimed to support individuals' right to timely access of their protected health information ("PHI")[1] and has targeted covered entities' non-compliance with fulfilling HIPAA's right of access requirements.

While the emerging enforcement trends from this Initiative are particularly relevant for covered entities, they also have important implications for business associates, especially with respect to contractual obligations and liabilities under business associate agreements ("BAAs"). This article analyzes these trends and implications and provides recommendations for how business associates may best address their right of access obligations and ensure compliance.

KEY TAKEAWAYS

It is clear from OCR's activity under its Right of Access Initiative that:

- OCR pursues enforcement actions against covered entities, big and small, across a wide range of sub-industries;
- Partial compliance is not sufficient; entities must comply when patients direct access to their electronic PHI to third parties, or risk enforcement; and

* Melissa M. Crespo is of counsel at Morrison & Foerster LLP handling privacy compliance and data security matters. Dan Kagan is an associate at the firm advising clients on health care regulatory compliance and health privacy issues. Eleanor C. Anthony is an associate at the firm focusing on privacy and data security matters. The authors may be reached at mcrespo@mofo.com, dkagan@mofo.com, and eanthony@mofo.com, respectively.

[1] *See* 45 CFR 164.524.

- Entities should pay attention when OCR provides technical assistance regarding access requests.

Further, while the right of access is a covered entity's obligation under HIPAA, and one that a business associate is obligated to support contractually, we expect that the increase of enforcement actions will prompt covered entities to more closely monitor business associate compliance with right-of-access obligations under BAAs. Accordingly, business associates that maintain PHI in designated record sets should, in addition to the other activities described below, implement and/or review policies and procedures aimed at ensuring timely and compliant responses to such access requests.

EMERGING TRENDS IN THE RIGHT OF ACCESS INITIATIVE

Since starting its Right of Access Initiative in 2019, OCR has actively pursued right-of-access enforcement actions, recently settling its 19th investigation.[2] By way of background, the right of access under HIPAA generally requires HIPAA covered entities to provide individuals with access to their PHI that is maintained in designated record sets[3] either by or on behalf of the covered entity.

Specifically, individuals have the right to obtain a copy of their PHI and inspect it, as well as the right to direct a covered entity, if it uses or maintains the individual's PHI in an electronic health record ("EHR"),[4] to transmit an electronic copy of their PHI in the EHR to a designated third party of the individual's choice.[5]

---

[2] *See* https://www.hhs.gov/about/news/2021/06/02/ocr-settles-nineteenth-investigation-hipaa-right-access-initiative.html.

[3] A designated record set is a group of records maintained by or for a covered entity that comprises:

- Medical records and billing records about individuals maintained by or for a covered health care provider;
- Enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Other records that are used, in whole or in part, by or for the covered entity to make decisions about individuals, including records that are used to make decisions about *any* individuals, whether or not the records have been used to make a decision about the particular individual requesting access.

[4] An EHR is an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

[5] In 2013, the Omnibus Rule modified provisions of the Privacy Rule and the HITECH Act to broaden the right of access to include the right of an individual to direct copies of their PHI contained in designated record sets to third parties, regardless of format (e.g. paper and electronic health records). In 2016, OCR issued guidance (www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html), regarding the rates that an entity can charge for an individual's access to their PHI and stated that this rate limit also applied to when an individual directed such access to a third party (e.g. a law firm, an insurance company) to receive a copy of such records. In 2020, the U.S. Court of Appeals for the D.C. Circuit vacated this expansion of the right of access, regardless of format, and OCR's price limits when individuals directed access to their designated record sets to third parties, with its decision in *Ciox Health, LLC v. Azar*. *See* 435 F. Supp. 3d 30 (D.D.C. 2020).

So far, OCR's right-of-access investigations have involved covered entities of varying sizes and sub-industries, including:

- Hospitals;
- Primary care providers;
- Multi-specialty medical clinics;
- Private medical practices;
- Mental health care providers;
- Academic medical centers; and
- Non-profits.

In a majority of these cases, covered entities have settled potential violations of the HIPAA Privacy Rule involving their failure to provide individuals with a copy of their requested PHI within the required time frames. Monetary settlements have ranged from $3,500 to $200,000, and all settlement agreements have included corrective action plans, with compliance monitoring for one to two years.

Additional enforcement trends that have emerged from the Initiative include:

- *Partial compliance is insufficient.* Several of OCR's settlements have involved covered entities who failed to provide the full scope of requested PHI to individuals, underscoring that partial compliance with the right of access is insufficient to avoid enforcement. For example, Dignity Health, dba St. Joseph's Hospital & Medical Center ("SJHMC"), a large, acute care hospital with several hospital-based clinics, agreed to pay $160,000 and enter into a corrective action plan with two years of monitoring, to settle potential violations of the right of access involving its failure to provide a mother with a copy of all of her son's medical records that she requested, though SJHMC initially provided some of the requested records.

- *Right to direct copies of EHR to third party will be enforced.* Several of OCR's investigations have also involved covered entities failing to send a copy of an individual's PHI contained in an EHR to a designated third party, suggesting that OCR views the third-party directive right as an important part of the right to access. For example, OCR entered into a settlement agreement with Sharp HealthCare, dba Sharp Rees-Stealy Medical Centers ("SRMC"), a California health care group with several hospitals, affiliated medical groups, and a health plan, in which SRMC agreed to pay $70,000 and enter into a corrective action plan with two years of monitoring, to settle potential violations of the right of access involving its failure to respond to a patient's records access request directing that an electronic copy of PHI in an EHR be sent to a third party.

- *OCR is responsive to complaints and will not provide technical assistance in the case of repeated violations*. In all of its Right of Access Initiative settlements, OCR has initiated investigations based on its receipt of a complaint alleging that a covered entity had violated the right of access. Upon receiving such a compliant, OCR has often – but not always – chosen to provide technical assistance to covered entities to help them comply with the right of access requirements; however, it has not done so in the case of subsequent violations. For example, after receiving a complaint alleging that The Arbour, Inc., dba Arbour Hospital ("Arbour"), a provider of behavioral health services in Massachusetts, had failed to take timely action in response to a patient's records access request, OCR provided Arbour with technical assistance regarding the HIPAA right of access requirements. After receiving a second complaint that Arbour had still failed to respond to the same records access request, OCR initiated an investigation and ultimately entered into a settlement agreement in which Arbour agreed to pay $65,000 and enter into a corrective action plan with one year of monitoring.

IMPLICATIONS FOR BUSINESS ASSOCIATES

While to date OCR's Right of Access Initiative has only targeted covered entities, as covered entities are primarily responsible for responding to individuals' requests to access PHI under HIPAA, the Initiative could prompt covered entities to more closely monitor compliance with business associates' contractual obligations regarding access requests. To comply with HIPAA, BAAs require a business associate to make PHI available in accordance with HIPAA's individual access rights requirements. While this may simply require providing access to the covered entity, often, the parties may agree in the BAA that the business associate will provide access to individuals directly, particularly where the business is the only holder of the designated record set or part thereof.

Similarly, to the extent that the business associate maintains PHI in an EHR for a covered entity, it may be called on to send an electronic copy of such PHI to a third party, upon an individual's request.

Business associates, therefore, must understand and define what PHI, if any, they maintain in designated record sets, including EHRs, in order to comply with their BAA right-of-access obligations. Note that although EHRs and designated record sets may contain overlapping information, they are not identical.

Moreover, while certain kinds of information–such as medical records and insurance information–are clearly part of both EHRs and designated record sets, business associates may require assistance from covered entities in determining what other information is included, such as other information that is created or consulted by health care clinicians in the case of an EHR, or other records that the covered entity may use to make decisions about individuals in the case of a designated record set.

In addition, business associates must be conscious of required timeframes for responding to access requests, in order to comply with their BAA obligations. Currently, a covered entity must respond to an individual's access request within 30 days, or 60 days if it utilizes a one-time, 30-day extension; however, under the current Notice of Proposed Rulemaking, OCR has proposed cutting this timeframe in half to 15 days, with the possibility for one 15-day extension. Covered entities may therefore obligate business associates to provide PHI to them within even shorter timeframes under their BAAs.

Additionally, due to the regulatory scrutiny a covered entity may expect to receive from OCR under the Initiative, in the event that a business associate fails to respond to an access request within the designated timeframe in its BAA, the covered entity may also seek to enforce any breach and/or audit provisions of the BAA to address such a failure. The covered entity may also seek to shift liability for right-of-access noncompliance to the business associate, to the extent it has not already done so, through an indemnification provision in the BAA.

To avoid contractual liability and oversight, business associates should review their right-of-access obligations under any applicable BAAs, to determine:

- Whether the business associate maintains PHI in any EHRs or designated record sets, and if not, seek to include limiting language regarding the access provision(s) in its BAAs;
- How the business associate is required to make requested PHI available (i.e., to the covered entity, the individual, or any requested third parties);
- What the applicable reporting periods are (i.e., within how many days must PHI be made available); and
- Whether the business associate must comply with any format or reporting specifications (i.e., is there a specific address of the covered entity to which PHI must be sent and will the covered entity only accept PHI in a particular form).

Although not required by HIPAA, to ensure compliance with their BAAs, business associates should also implement policies and procedures to ensure compliance with their right-of-access obligations, addressing:

- Contents and locations of any EHRs and/or designated record sets it maintains for a covered entity;
- Monitoring channels that may be used to submit access requests directly to the business associate;
- Forwarding of requests to covered entities, in accordance with contractual obligations; and

- Acknowledging receipt of and responding to requests, in accordance with contractual obligations and HIPAA requirements.

Finally, business associates should also monitor their compliance with their internal policies and procedures, and review and modify these policies and procedures periodically to account for any changes in law, new BAA obligations, or process improvements.