AN A.S. PRATT PUBLICATION
JULY-AUGUST 2023
VOL. 9 NO. 6

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

EDITOR'S NOTE: YOUR GREATEST DATA PRIVACY RISK
Victoria Prussen Spears

MITIGATING YOUR GREATEST DATA PRIVACY RISK: HOW TO ESTABLISH AN EFFECTIVE VENDOR MANAGEMENT PROCESS
Kathryn T. Allen and Kelsey L. Brandes

NAVIGATING THE HIPAA RISKS OF WEBSITE TRACKERS
Alexander Dworkowitz and Scott T. Lashway

MARITIME RANSOMWARE
Vanessa C. DiDomenico, Sharon R. Klein and Karen H. Shin

FEDERAL TRADE COMMISSION PROPOSES FURTHER RESTRICTIONS ON META'S PRIVACY PRACTICES AND A COMPLETE PROHIBITION ON META MONETIZING YOUTH DATA
Christopher N. Olsen and Nikhil Goyal

LIMIT YOUR HEALTH DATA SHARING AND CALL ME IN THE MORNING: FEDERAL TRADE COMMISSION PRESCRIBES ENFORCEMENT OF THE HEALTH BREACH NOTIFICATION RULE
Kathleen Benway, David C. Keating, Sara Pullen Guercio and Hyun Jai Oh

WASHINGTON TRANSFORMS CONSUMER HEALTH DATA LANDSCAPE WITH PASSAGE OF MY HEALTH MY DATA ACT
Meghan O'Connor and Kiana Baharloo

ILLINOIS SUPREME COURT CLARIFIES SCOPE OF STATE'S BIOMETRIC INFORMATION PRIVACY ACT CLAIMS: FIVE YEAR STATUTE OF LIMITATIONS AND CONTINUOUS ACCRUAL OF CLAIMS
Kathleen L. Carlson, Lawrence P. Fogel, Geeta Malhotra, Stephen W. McInerney, Vera M. Iwankiw, Andrew F. Rodheim and Carly R. Owens

ÖSTERREICHISCHE POST: EUROPEAN COURT OF JUSTICE SPECIFIES THE REQUIREMENTS FOR COMPENSATION FOR BREACHES OF GENERAL DATA PROTECTION REGULATION
Huw Beverley-Smith and Jeanine E. Leahy

Pratt's Privacy & Cybersecurity Law Report

VOLUME 9 **NUMBER 6** **July - August 2023**

Editor's Note: Your Greatest Data Privacy Risk
Victoria Prussen Spears 183

Mitigating Your Greatest Data Privacy Risk: How to Establish an Effective Vendor Management Process
Kathryn T. Allen and Kelsey L. Brandes 186

Navigating the HIPAA Risks of Website Trackers
Alexander Dworkowitz and Scott T. Lashway 191

Maritime Ransomware
Vanessa C. DiDomenico, Sharon R. Klein and Karen H. Shin 194

Federal Trade Commission Proposes Further Restrictions on Meta's Privacy Practices and a Complete Prohibition on Meta Monetizing Youth Data
Christopher N. Olsen and Nikhil Goyal 198

Limit Your Health Data Sharing and Call Me in the Morning: Federal Trade Commission Prescribes Enforcement of the Health Breach Notification Rule
Kathleen Benway, David C. Keating, Sara Pullen Guercio and Hyun Jai Oh 202

Washington Transforms Consumer Health Data Landscape with Passage of My Health My Data Act
Meghan O'Connor and Kiana Baharloo 208

Illinois Supreme Court Clarifies Scope of State's Biometric Information Privacy Act Claims: Five Year Statute of Limitations and Continuous Accrual of Claims
Kathleen L. Carlson, Lawrence P. Fogel, Geeta Malhotra, Stephen W. McInerney, Vera M. Iwankiw, Andrew F. Rodheim and Carly R. Owens 213

Österreichische Post: European Court of Justice Specifies the Requirements for Compensation for Breaches of General Data Protection Regulation
Huw Beverley-Smith and Jeanine E. Leahy 218

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:
Alexandra Jefferies at ..... (937) 560-3067
Email: ..... alexandra.jefferies@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*, [1] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [82] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.
LexisNexis and the Knowledge Burst logo are registered trademarks of Reed Elsevier Properties Inc., used under license.A.S. Pratt is a trademark of Reed Elsevier Properties SA, used under license.

Copyright © 2023 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. All Rights Reserved.

No copyright is claimed by LexisNexis, Matthew Bender & Company, Inc., or Reed Elsevier Properties SA, in the text of statutes, regulations, and excerpts from court opinions quoted within this work. Permission to copy material may be licensed for a fee from the Copyright Clearance Center, 222 Rosewood Drive, Danvers, Mass. 01923, telephone (978) 750-8400.

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

(2023–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

EDITOR-IN-CHIEF
Steven A. Meyerowitz
President, Meyerowitz Communications Inc.

EDITOR
Victoria Prussen Spears
Senior Vice President, Meyerowitz Communications Inc.

BOARD OF EDITORS

Emilio W. Cividanes
Partner, Venable LLP

Christopher G. Cwalina
Partner, Holland & Knight LLP

Richard D. Harris
Partner, Day Pitney LLP

Jay D. Kenisberg
Senior Counsel, Rivkin Radler LLP

David C. Lashway
Partner, Baker & McKenzie LLP

Craig A. Newman
Partner, Patterson Belknap Webb & Tyler LLP

Alan Charles Raul
Partner, Sidley Austin LLP

Randi Singer
Partner, Weil, Gotshal & Manges LLP

John P. Tomaszewski
Senior Counsel, Seyfarth Shaw LLP

Todd G. Vare
Partner, Barnes & Thornburg LLP

Thomas F. Zych
Partner, Thompson Hine

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. Copyright 2023 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. 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.

Navigating the HIPAA Risks of Website Trackers

By Alexander Dworkowitz and Scott T. Lashway*

In this article, the authors explain that it is critical that HIPAA covered entities understand exactly what data is being collected via tracking technologies operating on their websites and with whom that data is shared.

Covered entities are used to ensuring that many different facets of their operations comply with Health Insurance Portability and Accountability Act (HIPAA) rules. Among other things, covered entities must ensure that they provide individuals with access to protected health information (PHI) in accordance with HIPAA, that they obtain authorization for the use and disclosure of PHI when necessary, that they maintain PHI securely, and that they timely and appropriately report breaches of PHI.

But recently, a new area of HIPAA compliance has come into prominence: ensuring that the use of tracking technologies on covered entity websites does not result in the improper disclosure of PHI to technology vendors. As summarized below, it is critical for HIPAA covered entities to evaluate their website's tracking features, determine what data is collected and with whom it is shared (if anyone), consult with legal counsel to determine if HIPAA obligations are triggered, and develop countermeasures or containment strategies where necessary.

TRACKING TECHNOLOGIES 101

Tracking technologies are used to gather information about how a user of a website or a mobile app interacts with such website or app. Common third-party tracking technologies are offered by various internet, social media and ad tech companies. In the case of such technologies, code from a third party may be incorporated into a site, and such code may allow data about the website visitor's usage to be transmitted to the third party. In some cases, depending on what technology is deployed and how, the data collected can be detailed, including information such as mouse movements (often referred to as session replay technology). Certain data that may be available can be used to generate important insights as to who is using the site and what the site is being used for.

A website operator has to agree to permit the use of tracking technologies on a particular site. But website operators may nevertheless be unaware of all the trackers being used on their sites, as in some cases, "piggybacking" trackers can be incorporated into the code deployed by a particular vendor.

* The authors, attorneys with Manatt, Phelps & Phillips, LLP, may be contacted at adworkowitz@manatt.com and slashway@manatt.com, respectively.

HIPAA AND TRACKING TECHNOLOGIES

HIPAA does not prohibit outright covered entities from using tracking technologies, and such technologies are frequently used by hospitals and other covered entities to operate their websites, to guide visitors around their websites and to gain insights on the use of their websites to make improvements. However, HIPAA may limit how data may be disclosed from the covered entity website to social media companies or ad tech companies providing services to covered entities.

Critically, information disclosed by tracking technologies can be PHI in some cases. In December guidance,[1] the Department of Health and Human Services Office of Civil Rights (OCR) offered its interpretation as to when such data constitutes PHI. Generally speaking, PHI subject to HIPAA is (1) individually identifiable data (2) collected by or on behalf of a HIPAA covered entity (3) that relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual. In the guidance, OCR asserts that data disclosed by tracking technologies from a covered entity website can meet all three of these tests. Even in cases where the disclosure to the third-party technology vendor does not include direct identifiers like names or email addresses, OCR notes that data can be identifiable even if it includes information such as an IP address or the geographic location of the user. And some data on covered entity websites – particularly patient portal pages or authenticated pages – may contain information related to an individual's health condition and past health care.

Notably, OCR asserts that PHI is not limited to information maintained on user-authenticated pages of a covered entity's website, such as a patient portal. Instead, the agency maintains that unauthenticated pages that do not require a login nevertheless may sometimes generate PHI. For instance, OCR says a covered entity discloses PHI to a technology vendor if "tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider." The guidance also indicates that a search for information related to particular conditions, such as pregnancy, can constitute PHI in certain circumstances.

RISKS FOR COVERED ENTITIES

Providers around the country have been hit with lawsuits under which patients have sought damages for the disclosure of their data via tracking technologies. These lawsuits often rest on the novel legal theory that disclosures via tracking technologies violate wiretapping laws, and plaintiffs often rely on HIPAA violations as a basis for their claims.

---

[1] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

Beyond patient lawsuits, there are risks to HIPAA covered entities through their use of tracking technologies. In March, Cerebral, a virtual behavioral health platform, disclosed that it had provided a breach notice to OCR involving the disclosure of data from 3.1 million users via tracking technologies. Such breach reporting can result in administrative penalties imposed by OCR. Further, given OCR's recent restructuring to create a dedicated enforcement division and the widespread attention to this issue, the agency could begin to take more proactive enforcement steps in this area.

OCR is not the only agency taking notice. The Federal Trade Commission (FTC) fined GoodRx $1.5 million for sharing its users' health data with social media companies. States also can take action. Disclosures via tracking technologies can implicate state breach reporting laws and, in certain states, comprehensive privacy laws like the California Consumer Privacy Act.

STEPS TO PROMOTE COMPLIANCE

Given this environment, it is critical that covered entities understand exactly what data is being collected via tracking technologies operating on their websites and with whom that data is shared. Legal counsel should determine whether any such data could constitute PHI and, if PHI has been disclosed, determine appropriate steps to respond to such disclosure and mitigate any future risks, including entering into business associate agreements with vendors when feasible and appropriate.

Policies and procedures should also be in place to ensure that any disclosures of data via tracking technologies occur in compliance with not only HIPAA, but all applicable privacy and security laws.