AN A.S. PRATT PUBLICATION
NOVEMBER/DECEMBER 2021
VOL. 7 NO. 9

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis

Pratt's Privacy & Cybersecurity Law Report

VOLUME 7 **NUMBER 9** **November/December 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 [293] (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.

Important FTC Rules for Health Apps Outside of HIPAA

By Marissa C. Serafino, Ashley Thomas, and Shannon Britton Hartsfield*

The Federal Trade Commission has adopted a policy statement emphasizing that developers of digital health apps, connected devices, and other health products have obligations under the Health Breach Notification Rule. The rule requires certain businesses not covered by HIPAA to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information. The authors of this article discuss the policy statement, which signals a need for a renewed focus on the personal health record breach rules and may lead to future enforcement.

The Federal Trade Commission ("FTC") adopted a policy statement[1] on September 15, 2021, emphasizing that developers of digital health apps, connected devices and other health products have obligations under the Health Breach Notification Rule. The Health Breach Notification Rule requires certain businesses not covered by the Health Insurance Portability and Accountability Act ("HIPAA") to notify their customers and others if there is a breach of unsecured, individually identifiable electronic health information.

The Health Breach Notification Rule was adopted in 2009 to ensure that entities not covered under HIPAA would still be held accountable in the event of a breach of customers' sensitive health information. Since the Health Breach Notification Rule's inception, the FTC has never enforced it. The FTC's policy statement signals the FTC's commitment to utilize its enforcement tools where sensitive health information may be compromised.

BREACH NOTIFICATION PROVISIONS

The FTC's rules implement breach notification provisions found in the Health Information Technology for Economic and Clinical Health Act ("HITECH Act"). As part of the American Recovery and Reinvestment Act ("ARRA"), Congress passed the HITECH Act, which focused on the implementation and use of health information

* Marissa C. Serafino (marissa.serafino@hklaw.com) is an associate at Holland & Knight LLP and member of the firm's Public Policy & Regulation Group focusing on the intersection of law and public policy on privacy and cybersecurity matters, political law and compliance, national security, and the environment. Ashley Thomas (ashley.thomas@hklaw.com) is a data strategy, security, and privacy senior counsel at the firm. Shannon Britton Hartsfield (shannon.hartsfield@hklaw.com) is a partner at the firm and the executive partner in the firm's Tallahassee office focusing her practice on corporate compliance, particularly in the regulatory and data privacy areas.

[1] https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

technology, with a particular emphasis on privacy and security. The FTC regulations affect situations where there is a breach of a "personal health record" ("PHR").

The regulations require vendors of PHRs and PHR-related entities to notify U.S. consumers, the FTC and, in some cases, the media if a breach of unsecured identifiable health information occurs. The rules define "personal health record" as "an electronic record of PHR identifiable information of an individual that can be drawn from multiple sources and that is managed, shared, and controlled primarily by or primarily for the individual."[2] Until the FTC's September 2021 statement, there was no clear guidance regarding a definition of "multiple sources." In the FTC's policy statement, it clarified that multiple sources can be drawn through a combination of consumer inputs and application programming interfaces ("APIs") even if the health information comes from only one source.

"PHR identifiable health information" means individually identifiable health information ("IIHI") as defined in 42 U.S.C. §1320d(6) "and, with respect to an individual, information: 1) That is provided by or on behalf of the individual; and 2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."[3] IIHI is defined as any identifying information, including demographic information, that is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse and relates to an individual's health.[4]

An important and often complex question for PHR vendors is whether they are "business associates" under the HIPAA privacy and security rules. If so, the FTC rules would not apply if the PHR vendor experiences a data breach. The HIPAA privacy and security rules only apply to "covered entities," their "business associates" and "subcontractors" of business associates. Covered entities include health plans, healthcare clearinghouses and most healthcare providers. Business associates and subcontractors are third parties that need access to protected health information to perform certain functions or services on behalf of covered entities or other business associates. For example, a person who offers a PHR to individuals on behalf of a covered entity is a business associate.

The U.S. Department of Health and Human Services' ("HHS") Office for Civil Rights ("OCR"), which enforces HIPAA, has observed that PHR vendors may offer PHRs directly to individuals and also on behalf of covered entities. The PHR vendor only becomes a HIPAA business associate to the extent that the vendor offers PHRs to individuals on behalf of covered entities.[5] Whether a vendor is offering a PHR "on behalf of" a covered entity is not always clear and "is a fact specific determination."[6]

---

[2] *See* 16 C.F.R. §318.2.

[3] *Id.*

[4] 42 U.S.C. §1320d(6).

[5] 78 FR 5572 (Jan. 25, 2013).

[6] *Id.* at 5572.

A vendor is not a business associate merely because it has an agreement with a covered entity governing how data will be exchanged. Instead, the PHR vendor would have to be providing and managing a service that the covered entity is offering to patients or enrollees, or some other function or service provided to or for the covered entity.[7] If the PHR vendor is a business associate and experiences a data breach, the HIPAA breach notification rules would apply, rather than the FTC rules.

If the PHR vendor is not subject to HIPAA and has a data breach, it will need to fulfill its reporting obligations under the Health Breach Notification Rule. Under the Health Breach Notification Rule, PHR vendors and PHR-related entities must notify individuals, the FTC, and possibly the media within 60 days after discovering a breach of unsecured personally identifiable health information, or within 10 days if 500 or more individuals are affected by the breach.

Third-party service providers of PHR vendors or PHR-related entities also have their own obligations under the Health Breach Notification Rule. PHR vendors and PHR-related entities are required to inform their third-party service providers if they are covered under the rule. In addition, a service provider must inform the PHR vendor or PHR-related entity within 60 days of a breach and obtain acknowledgment that notice was received. The Health Breach Notification Rule preempts contradictory state breach notification laws, but not those that impose additional non-contradictory breach notification requirements. Over the past decade, the FTC has only received four notifications of data breaches involving 500 or more individuals.

Earlier this year, the FTC reached a settlement with Flo Health and, in a joint statement, Commissioners Rebecca Kelly Slaughter and Rohit Chopra argued that a violation of the Health Breach Notification Rule should have been included in the settlement, but the FTC majority declined to make this charge. In March 2021, three U.S. Congressional members sent a letter to the FTC requesting that it enforce the Health Breach Notification Rule regarding health apps that share personal health information ("PHI") with third parties without consumer consent. This recent FTC policy statement signals a need for renewed focus on the FTC PHR breach rules and may lead to future enforcement.

COMPARISON CHART

The chart accompanying this article analyzes questions raised by the statement which, to some extent, appears to go beyond the existing rules.

---

[7] *Id.*

FTC Statement of the Commission on Breaches by Health Apps and Other Connected Devices (2021)[8]	**FTC Health Breach Notification Rule (16 C.F.R. § 318) (2009)**[9]	**Analysis**
"Under the Rule's requirements, vendors of personal health records (PHR) and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations. The Rule also covers service providers to these entities. In practical terms, this means that entities covered by the Rule who have experienced breaches cannot conceal this fact from those who have entrusted them with sensitive health information." "The Rule covers vendors of personal health records that contain individually identifiable health information created or received by health care providers. The Rule is triggered when such entities experience a 'breach of security.'"	Entities governed by the rule (emphases added): "It applies to foreign and domestic *vendors of personal health records, PHR related entities, and third party service providers,* irrespective of any jurisdictional tests in the Federal Trade Commission (FTC) Act, that maintain information of U.S. citizens or residents." (318.1(a)). *"Vendor of personal health records* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, *that offers or maintains a personal health record."* "*PHR related entity* means an entity, other than a HIPAA-covered entity or an entity to the extent that it engages in activities as a business associate of a HIPAA-covered entity, that: (1) Offers products or services through the Web site of a vendor of personal health records;	The policy statement only targets vendors of personal health records.

[8] https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

[9] https://www.ecfr.gov/current/title-16/part-318.

	(2) Offers products or services through the Web sites of HIPAA-covered entities that offer individuals personal health records; or (3) Accesses information in a *personal health record* or sends information to *a personal health record*." "*Third party service provider* means an entity that: (1) Provides services to a vendor of personal health records in connection with the offering or maintenance of a *personal health record* or to a PHR related entity in connection with a product or service offered by that entity; and (2) Accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured PHR identifiable health information as a result of such services." "*PHR identifiable health information* means 'individually identifiable health information,' as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)),[10] and, with respect to an individual, information: (1) That is provided by or on behalf of the individual; and	

[10] https://www.govinfo.gov/link/uscode/42/1320d.

	(2) That identifies the individual or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual."	
Under the definitions cross-referenced by the rule, the developer of a health app or connected device is a "health care provider" because it "furnish[es] health care services or supplies."	No definition in the rule. Section 13400 of ARRA[11] defines "Health Care Provider" as "a provider of services (as defined in section 1861 of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." (45 CFR Section 160.103).[12]	The basis for the FTC's statement regarding the definition of a healthcare provider as an entity that "furnish[es] health care services or supplies" to determine that health apps/ connected devices is not clear. The phrase is not in any of the citations listed. This conclusion is likely part of the overreach referred to by FTC Commissioners Noah Joshua Phillips[13] and Christine S. Wilson,[14] particularly given the narrow definition of "health care provider" in the governing statute.

[10] https://www.govinfo.gov/link/uscode/42/1320d.

[11] https://www.govinfo.gov/content/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf.

[12] https://www.law.cornell.edu/cfr/text/45/160.103.

[13] Dissenting Statement of Commissioner Phillips Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021) (stating that the Democratic Commissioners' "reading of the relevant texts is convoluted, and apparently beyond what Congress, the Commission, and sister agencies had in mind in drafting them.") *See*, https://www.ftc.gov/system/files/documents/public_statements/1596328/hbnr_dissent_final_formatted.pdf.

[14] Dissenting Statement of Commissioner Wilson Regarding the Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021) (stating that the Policy Statement ". . . seeks to improperly expand our statutory authority. . . ."). *See*, https://www.ftc.gov/system/files/documents/public_statements/1596356/wilson_health_apps_policy_statement_dissent_combined_final.pdf.

"When a health app, for example, discloses sensitive health information without users' authorization, this is a 'breach of security' under the Rule."	*Unsecured* means PHR identifiable information that is not protected through the use of a technology or methodology specified by the Secretary of Health and Human Services in the guidance issued under section 13402(h)(2) of the American Reinvestment and Recovery Act of 2009. (318.2(i)).	The policy statement leaves out an important element of a "breach of security," which is that the PHR identifiable health information must be "unsecured."
"The statute directing the FTC to promulgate the Rule requires that a 'personal health record' be an electronic record that can be drawn from multiple sources. The Commission considers apps covered by the Rule if they are capable of drawing information from multiple sources, such as through a combination of consumer inputs and application programming interfaces ("APIs"). For example, an app is covered if it collects information directly from consumers and has the technical capacity to draw information through an API that enables syncing with a consumer's fitness tracker. Similarly, an app that draws information from multiple sources is covered, even if the health information comes from only one source.	*Personal health record* means an electronic record of PHR identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual. (318.2(d)). (Section 13400 of ARRA uses[15] same definition).	The FTC's interpretation of "drawn from multiple sources" is broad and would likely cover most health apps. ARRA defines "personal health record" as "an electronic record of PHR identifiable health information (as defined in section 13407(f)(2)) on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

[15] https://www.govinfo.gov/content/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf.

For example, if a blood sugar monitoring app draws health information only from one source (e.g., a consumer's inputted blood sugar levels), but also takes non-health information from another source (e.g., dates from your phone's calendar), it is covered under the Rule."		
"In addition, the Commission reminds entities offering services covered by the Rule that a 'breach' is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule."	Unauthorized acquisition will be presumed to include unauthorized access to unsecured PHR identifiable health information *unless* the vendor of personal health records, PHR-related entity or third-party service provider that experienced the breach has reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information.	The rule includes an important exception regarding "breach of security" that excludes situations where an entity has "reliable evidence showing that there has not been, or could not reasonably have been, unauthorized acquisition of such information." Thus, unauthorized *access may* not trigger notification requirements. Section 13400 of ARRA also included exceptions to breach, including: (i) any unintentional acquisition, access, or use of protected health information by an employee or individual acting under the authority of a covered entity or business associate if 1) such acquisition,

		access or use was made in good faith and within the course and scope of the employment or other professional relationship of such employee or individual, respectively, with the covered entity or business associate, and 2) such information is not further acquired, accessed, used or disclosed by any person; or (ii) any inadvertent disclosure from an individual who is otherwise authorized to access protected health information at a facility operated by a covered entity or business associate to another similarly situated individual at same facility; and (iii) any such information received as a result of such disclosure is not further acquired, accessed, used or disclosed without authorization by any person.

"Violations of the Rule face civil penalties of $43,792 per violation per day."	A violation of this part shall be treated as an unfair or deceptive act or practice in violation of a regulation under § 18(a)(1)(B) of the Federal Trade Commission (FTC) Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.	In January 2021, the FTC[16] adjusted its maximum civil penalty based on inflation to $43,792 for violations of Sections 5(l), 5(m)(1)(A), and 5(m)(1)(B) of the FTC Act. The policy statement states that it will levy fines at the maximum amount, not *up to* the maximum amount.

[16] https://www.ftc.gov/news-events/press-releases/2021/01/ftc-publishes-inflation-adjusted-civil-penalty-amounts-2021.