LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC's Hasty Health Data Rule Change Could Cause Confusion

By **Jodi Daniel** (October 1, 2021, 5:42 PM EDT)

Jodi Daniel

On Sept. 15, the Federal Trade Commission issued a policy statement[1] that seems to sweep in a large number of technology companies and activities into compliance with its Health Breach Notification Rule, Title 16 of the Code of Federal Regulations, Part 318.

Specifically, the HBN rule has applied to vendors of personal health records, and PHR-related entities when there is a breach of security generally, but according to the FTC's policy statement, the HBN rule applies to health apps broadly and notification is triggered when there is any sharing of information that is not authorized by the individual.

While the FTC claims that they are offering guidance and clarifying the scope of the HBN rule promulgated in 2009, the policy statement appears to substantially increase the scope of the HBN rule without going through the requisite notice and comment rulemaking process, and by providing interpretations that exceed other federal and state breach notification rules.

Background

The HBN rule implements the requirements of Subtitle D of the Health Information Technology for Economic and Clinical Health Act[2] to require notification where there is a breach of unsecured PHR identifiable information.

Subtitle D also provided the U.S. Department of Health and Human Services with authority to promulgate breach notification requirements for covered entities and business associates under the Health Insurance Portability and Accountability Act.

The HBN rule applies to vendors of personal health records and PHR-related entities, which excludes HIPAA-covered entities and business associates that offer PHRs. It requires these entities to notify individuals and the FTC following the discovery of a breach of security, which is defined as "acquisition of [PHR identifiable health information] without the authorization of the individual."[3]

The FTC has not brought any enforcement actions under the HBN rule to date, but states that it intends to enforce this rule consistent with its policy statement. Entities can face civil penalties of $43,792 per violation per day.

In May 2020, the FTC published a request for comment[4] on the HBN rule, claiming that this simply is a periodic review. However, the FTC policy statement, which addresses issues raised in the request for comment, seems to be an attempt to set privacy and security standards in response to the growing amount of health data that is collected by technology companies and other entities that are not covered by federal privacy and security requirements.

There have been concerns about the privacy and security of data held by these noncovered entities over the past decade.[5]

However, data-sharing from HIPAA-covered entities and business associates to noncovered entities is accelerating due to Office of the National Coordinator for Health Information Technology and Centers for Medicare & Medicaid Services interoperability rules,[6] which increase requirements for certain entities to provide data to third-party applications at the direction of the individual.

Analysis

Through the policy statement, the FTC attempts to expand the scope of the HBN rule and broaden the interpretation of the term "breach," but fails to go through the appropriate administrative process for making such significant policy modifications.

Significant Expansion of the Scope of the Rule

In short, the FTC is broadly interpreting its scope of authority to cover health apps. The HBN rule is limited in scope by the HITECH Act to vendors of personal health records, and PHR-related entities.

PHRs have traditionally been thought of as a narrow type of product, defined based on the use by the individual,[7] and only a subset of health apps. The HBN rule defines "personal health record" as "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."

The policy statement states that an app that has the technical capacity to draw information through an application programming interface, or API, from multiple sources is covered even if it does not collect information from multiple sources.

In clarifying what health apps may be covered, the FTC provides the example of a blood sugar monitoring app where the individual inputs their own information and the technology is integrated with a calendar app on a phone.

This is in direct conflict with the FTC's prior interpretation that a technology that enables an individual to input their own information and does not interact with a PHR is not a PHR-related entity.[8]

The FTC also fails to address the second requirement that the health information must be "managed, shared, and controlled by or primarily for the individual," which may limit the scope of the entities covered by the HBN rule.

Furthermore, the request for comment raises questions specifically about entities covered by the HBN rule, including what modifications should be considered to the rule to account for changes in relevant technology, economic conditions or laws, including with regard to access to health data through standardized APIs, and the cost of compliance.[9]

This policy statement does not address these questions raised in the request for comment.

Significant Expansion of the Interpretation "Breach"

The FTC also seems to redefine a "breach of security," which triggers action under the HBN rule. The policy statement states that:
"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.

This interpretation is inconsistent with the HBN rule's examples of unauthorized acquisition that focus on cybersecurity intrusions or nefarious behavior, specifically "the theft of a laptop containing unsecured PHRs; the unauthorized downloading or transfer of such records by an employee; and the electronic break-in and remote copying of such records by a hacker."[10]

The policy statement also seems to change the default by equating unauthorized access with sharing of information, and confuses security issues with privacy issues.

The FTC suggests that there is a breach if an entity covered by the HBN rule shares data without an individual's authorization with a partner even where it is consistent with their privacy policies and contracts.

Even entities subject to HIPAA requirement can share individually identifiable health information for a variety of reasons without individual authorization, including treatment, payment, health care operations, public health and research.

Here, where there is no federal floor for privacy protections for entities subject to the HBN rule and no privacy requirement that vendors of PHRs or PHR-related entities obtain individual authorization prior to sharing any information, the FTC seems to be attempting to create an unprecedented privacy policy in a breach notification rule.

Expansion of the Regulatory Scope Requires Rulemaking

While it is possible for the FTC to change its interpretation and applicability of the HBN rule, it can only do so through notice and comment rulemaking in accordance with its statutory authority and with the Administrative Procedures Act.

Through the policy statement, the FTC significantly increases the scope of entities covered and the events that trigger notification without considering public input.

Over 10 years ago, the HBN rule considered the burden of the rule, estimating that there would be approximated 900 entities subject to the Rule and 11 total breaches per year, for a total of $795,235 per year.

Today it is estimated that there are over 350,000 digital health apps available to consumers. Because there are more PHRs today than 10 years ago, if the HBN rule is to cover all of these health apps and the definition of a breach of security includes any sharing of information that is not authorized by the individual, the cost and burden would be exponentially higher than the growth of PHRs.

The FTC should consider the burden of these significant policy changes. To the extent the modifications do not exceed the FTC's statutory authority, the FTC should follow the process of going through notice and comment rulemaking and incorporating public input into the policy development. Otherwise, it will be difficult for the FTC to enforce policy changes adopted through guidance.

The Future of the FTC's Role in Breach Notification

This policy statement clearly indicates the FTC's intent to pay more attention to the HBN rule and to put some guardrails on health apps that currently have significant leeway to use and disclose health data, including identifiable health data. As more data flows outside the traditional health care space, filling this gap is incredibly important to protect consumers' health data and maintain trust that is necessary for innovation to succeed.

Nonetheless, if the FTC attempts to enforce compliance against health apps that are not PHRs, as the FTC has previously defined them, or if the FTC enforces breach notification requirements for sharing data with third parties without patient authorization but where such disclosures were consistent with the third parties' privacy policies, the FTC should expect challenges to this policy statement.

This hasty approach to expanding the FTC's efforts regarding the privacy and security of health apps could raise confusion and could delay effective and appropriate privacy and security policies that can advance interoperability and health innovation.

Jodi G. Daniel is a partner at Crowell & Moring LLP.

[1] Statement of the Commission, On Breaches by Health Apps and Other Connected Devices, September 15, 2021. [https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf].

[2] The Health Information Technology for Economic and Clinical Health (HITECH) Act is part of the American Recovery & Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115, codified at 42 U.S.C. § 17937, Subtitle D.

[3] 16. C.F.R. § 318.2(a).

[4] 85 Fed. Reg. 31085 (May 22, 2020).

[5] Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA, June 2016, [https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf].

[6] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program: Final Rule, 85 Fed. Reg. 25642 (May 1, 2020); Medicare and Medicaid Programs; Patient

Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers: Final Rule, 85 Fed. Reg. 25510 (May 1, 2020).

[7] FTC explained that a "personal health record" would include "an online service that allows consumers to store and organize medical information from many sources in one online location." ONC defines "PHR" as "an electronic application through which patients can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment." https://www.healthit.gov/faq/what-personal-health-record [Note: FAQ last reviewed by ONC on 5/2/2016, after the publication of the FTC PHR Breach Rule.].

[8] Complying with the FTC's Health Breach Notification Rule, FTC, April 2010 (edited January 2021) [https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule].

[9] 85 Fed. Reg. 31086.

[10] 74 Fed. Reg. 42966.