Published on *The National Law Review* https://natlawreview.com

FTC Proposes Changes to Health Breach Notification Rule Clarifying Application to Health and Wellness Apps

Article By:

Michael D. Sutton

Jason Levy

In May, the Federal Trade Commission ("FTC") proposed changes (the "Proposed Rule") to the Health Breach Notification Rule (the "Rule"),[1] which, among other items, emphasize that the Rule applies to mobile health applications and related technologies that use or otherwise compile consumers' health information.[2] While the FTC's position on this point is not entirely new,[3] industry interpretations of the Rule have been inconsistent.

The Rule's purpose is to ensure that vendors of personal health records and certain related entities ("Vendors") that possess sensitive patient information but are not subject to the breach notification requirements of the Health Insurance Portability and Accountability Act ("HIPAA") are subject to some requirements.[4] The Rule accomplishes this goal by requiring Vendors to notify consumers and the FTC if a security breach of unsecured health information has occurred. If a Vendor fails to abide by the Rule, it may be subject to hefty civil penalties.

Proposed Changes to the Scope of the Rule

The FTC expressed concern that Vendors of certain health-oriented applications may not understand that they are subject to the Rule and its attendant obligations.[5] This concern was likely prompted by the wide popularity of Vendor applications in the commercial space. Specifically, the FTC has indicated that the Rule applies to developers of mobile health applications and technologies, including those marketed as "wellness" products rather than "health" products.[6] The Proposed Rule aims to eliminate confusion by clarifying the Rule's applicability to Vendors and updating relevant definitions.

First, the Proposed Rule updates the definition for "PHR identifiable information"[7] to include information that:

1. Is provided by or on behalf of an individual;

2. Identifies an individual or there is a reasonable basis to believe that the information could identify an individual;

3. Relates to the past, present, or future health condition of an individual;

4. Relates to the past, present, or future provision of health care to an individual; or

5. Is created or otherwise received by a health care provider, a health plan, employer, or health care clearinghouse.[8]

Second, the Proposed Rule adds a new definition for "health care provider," which includes: (i) a provider of medical or other health services; (ii) an entity furnishing health care services or supplies; or (iii) a hospital, critical access hospital, rural emergency hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, or hospice program.[9]

Third, the Proposed Rule adds a new definition for "health care services or supplies" which now includes online services such as "a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools."[10] The Proposed Rule's new definition would capture several popular applications and devices, facilitating its primary objective of clarifying the Rule's scope.

Fourth, the Proposed Rule updates the definition of "personal health record" to capture an "electronic record of PHR identifiable health information on an individual that has the technical capacity to draw information from multiple sources, and that is managed, shared, and controlled by or primarily for the individual."[11] This update is intended to clarify what it means for a personal health record to draw PHR identifiable health information from multiple sources.

Fifth, the Proposed Rule updates the definition of "breach of security" to clarify that it includes unauthorized acquisitions due to a data breach or an unauthorized disclosure.[12] This update seeks to clarify that a breach is not limited to instances of cybersecurity intrusions or other misbehavior but may also occur where there is an unauthorized sharing of protected information.

Sixth, the Proposed Rule updates the definition of "PHR related entity" to clarify that it includes entities offering products and services through Vendors' websites and any available online service, such as mobile applications.[13] In addition, the Proposed Rule clarifies that the definition includes only entities that access or send unsecured PHR identifiable health information to a personal health record rather than entities that merely access or send secure data to a personal health record.

Proposed Changes to Notice Requirement

The FTC also expressed concern about the functionality of the Rule's notice-related mailing requirement, as mailed notice is inconsistent with how consumers traditionally receive notifications about online technologies. In turn, the FTC proposed expanding the use of email and other electronic communications mediums to notify consumers of a breach.[14]

The Proposed Rule also seeks to include additional components in a breach notice required under the Rule. Specifically, the Proposed Rule recommends that Vendor breach notices:

1. Include a brief description of the potential harm from a particular breach.[15]

2. Incorporate the full name, website, and contact information of any third parties that acquired unsecured PHR identifiable health information due to a breach, provided that such information is known to the Vendor.[16]

3. Describe the types of unsecured PHR identifiable health information involved in a specific breach.[17]

4. Describe what the party that experienced the breach is doing to protect the affected individuals.[18]

5. Include two or more of the following means of contacting the party providing notice: (a) a toll-free telephone number; (b) email address; (c) website; (d) within-application medium; or (e) postal address.[19]

Comments on the Proposed Rule are due by August 8, 2023. We will continue to monitor the Proposed Rule, including any new developments.

FOOTNOTES

[1] 16 C.F.R. § 318.1, et seq.

[2] Proposed Rule, at p. 12.

[3] *See* Statement of the Commission, issued on September 15, 2021.

[4] Proposed Rule at pp. 2-3.

[5] *Id.*at p. 12.

[6] *Id.* at pp. 5, 15.

[7] “PHR” means “personal health records.” 16 C.F.R. § 318.2(h).

[8] 16 C.F.R. § 318.2(i).

[9] 16 C.F.R. § 318.2(f).

[10] 16 C.F.R. § 318.2(e).

[11] 16 C.F.R. § 318.2(h).

[12] 16 C.F.R. § 318.2(a).

[13] 16 C.F.R. § 318.2(j).

[14] 16 C.F.R. § 318.5.

[15] 16 C.F.R. § 318.6(a).

[16] 16 C.F.R. § 318.6(a).

[17] 16 C.F.R. § 318.6(b).

[18] 16 C.F.R. § 318.6(d).

[19] 16 C.F.R. § 318.6(e).

National Law Review, Volume XIII, Number 181