FTC Health Breach Notification Rule: Proposed Rule and Request for Comment

Diane Sacks, Esq.
Counsel to Confidentiality Coalition
June 22, 2023

Diane Sacks LLC

Time Line

- Proposed rule issued May 18, 2023
- Comments due August 8, 2023 (60 days from June 9, 2023 Federal Register publication)
- Compliance would be required within 180 days after final rule effective date (which will be 60 days after publication in federal register)

Background: Current Rule

- Rule issued August 2009, implementing Section 13407 of the HITECH Act
- Applies to:
  - Vendors of personal health records (PHRs)
  - PHR related entities
  - Their 3rd party service providers
- Does not apply to HIPAA covered entities or their business associates (HIPAA entities)
- Requires notification of breaches of "unsecured PHR identifiable health information (PHR IHI)"

Background: Developments Since 2009

- Since 2009, consumer health apps, such as fitness trackers have proliferated
- Comments in response to FTC's May 2020 ten-year review of Rule encouraged FTC to clarify that the Rule applies to consumer health apps and to increase enforcement
- FTC issued a Policy Statement in September 2021 explaining that:
  - Rule covers most health app makers because they qualify as as "health care providers" and therefore, the data they create or receive qualifies as "individually identifiable health information"
  - A breach of security under the Rule includes disclosures without authorization, and is not limited to "cybersecurity intrusions or nefarious behavior"
- First enforcement action in February 2023 against GoodRx for disclosing IIHI to third party advertising platforms like Google and Facebook without authorization contrary to explicit promises made to users of its website and mobile apps

Key Proposed Changes

- Expands scope of entities covered
- Expands definition of breach of security
- Revises the definition of PHR related entity
- Clarify what it means to draw PHR IHI from multiple sources
- Expanded use of electronic notice
- Expands required content of the notice
- Adds reference to civil monetary penalties for violations

Expand Scope of Entities Covered

- Creates new definition "**health care provider**" that includes any entity "furnishing health care services or supplies"
- Creates new definition "**health care services or supplies**" to include any online service 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
- New definitions make clear that:
  - Developers of health apps hold "PHR IHI" because they are health care providers that furnish health services or supplies
  - Mobile health apps are PHRs and therefore, their developers are "vendors of PHR"
  - Websites, apps and internet-connected devices that provide medical or wellness services are covered

Expands definition of “breach of security”

- Currently defined as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the authorization of the individual. Also includes a rebuttable presumption that unauthorized acquisition includes unauthorized access
- Proposed definition adds that the term includes “unauthorized acquisitions that occur as a result of a data breach or an unauthorized disclosure”
- Makes clear that the Rule covers voluntary disclosures that were not authorized by the consumer, such as to third party companies for advertising

Revised definition of “PHR related entity”

- Currently defined as an entity, other than a HIPAA entity, that (1) offers products or services through a website of a PHR vendor or of a HIPAA-covered entity that offers individuals PHRs, or that (2) accesses information in a PHR or sends information to a PHR
- Revised definition clarifies that PHR related entities (1) include entities offering products and services not only through the websites of PHR vendors, but also through any online service, including mobile applications, and (2) do not include entities that simply access data in or send data to a PHR unless that data is unsecured PHR IHI
- To avoid third party service providers (TPSPs) also being PHR related entities, FTC proposes to revise definition of TPSP to clarify that a TPSP is not also a PHR related entity when it accesses unsecured PHR IHI to provide services to a PHR vendor

Revised definition of “PHR related entity”

- Includes mobile health apps like heart or blood pressure monitors when individuals sync them with a PHR, but would not include a grocery delivery service that sends data about food purchases to a diet and fitness app
- It would not include an analytics firm that provides services for a PHR vendor, which will be a TPSP. FTC notes that treating an analytics firm as TPSP will create incentives for responsible stewardship of data and encourage sharing of only de-identified data to such entities

Draw Information from Multiple Sources

- Current rule defines PHR as an electronic record of PHR IHI that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual
- Revised definition would change the definition to require that the electronic record have the technical capacity to draw information from multiple sources
  - A product is a PHR if it can draw information from multiple sources, even if the consumer elects to limit information from a single source only, in a particular instance.
  - A product is a PHR if it can draw any information from multiple sources, even if it only draws health information from one source

Examples of Drawing Info from Multiple Sources

FTC provides these examples:

- Diet and Fitness App X has the technical capacity to draw IIHI (name, weight, age) from the user and from a fitness tracker (name, miles run), but user does not connect the fitness tracker. App X is a PHR even though it draws info from only one source, since it has the capacity to draw info from two sources.
- Diet and Fitness App Y has the technical capacity to draw IHII (name, weight, height) and non-health information (calendar entry info) from the user's calendar. App Y is a PHR even though it can draw IHII from only once source, since it can draw info from two sources

Expanded Use of Electronic Notice

- Current rule allows notice by email if the individual is given a clear, conspicuous, and reasonable opportunity to receive notification by first-class mail, and the individual does not exercise that choice
- Proposed rule requires written notice at the last known address of the individual
  - Notice may be sent by email if the individual has specified email as the primary method of communication. If email is not available, notice must be sent by first class mail
  - Would allow entities to send an email or inapp alert notifying users that they will receive breach notices by electronic mail unless they opt out and instead receive notice by first class mail
  - Email notice must be “clear and conspicuous” i.e., it must be reasonably understandable and designed to call attention to the nature and significance of the information in the notice

Model Notice

- FTC proposes a model notice attached as an exhibit to the proposed rule, that may be used to provide notice
- Topics for comment:
  - Whether use of model notice should be mandatory
  - Whether and how the model notice could be compatible with electronic notice, such as text, banner and within-app messaging, including whether and how entities could suitably link to model notice language from a text message, electronic banner, or in-application message
  - Recommended changes to the substance and format of the model notice

Expanded Content of Notice

Additional content:

- Brief description of potential harm
- Full name, website, and contact information (such as a public email address or phone number) of any third parties that acquired unsecured PHR IHI as a result of a breach of security, if this information is known
- Expands list of examples of types of PHR IHI that must be described to include health diagnosis or condition, lab results, medications, other treatment information, the fact of an individual's use of a particular health-related mobile app, and device identifier
- In addition to current requirement describing what entity is doing to investigate, mitigate and protect against future harm, notice would have to describe what it is doing to protect affected individuals, such as offering credit monitoring or other services
- Entity must provide two or more (instead of one) means of contacting the entity for more information

Adds Reference to Penalties for Non-compliance

- Proposed rule states that a violation will be treated as a violation of a rule promulgated under section 18 of the FTC Act, regarding unfair or deceptive acts or practices, and thus subject to civil penalties (as adjusted for inflation), and the Commission will enforce this Rule in the same manner, by the same means, and with the same jurisdiction, powers, and duties as are available to it pursuant to the FTC Act
- Violations with actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that the act is unfair or deceptive and prohibited is liable for civil penalties
- Current penalties are up to $50,120 per violation per day

Topics for Comment

- Do changes make clear which entities are covered and under what circumstances?
- Do definitions overlap (e.g., PHR related entity and TPSP) and how to avoid this?
- Comments on proposed definition of “health care provider”
- Comments on the scenario where an analytics firm that is a TPSP sells PHR IHI (e.g., device identifier and geolocation data from which health information about an individual can be inferred) without the consumer’s authorization. The FTC consider this to be a reportable breach, even if the consumer consented to the original collection of their data and asks whether, as a policy matter, it is advisable under the Rule to require a PHR vendor to notify its customers about such “onward disclosures”
- Comments on whether use of model notice should be mandatory and new content requirements