Dissenting Statement of Commissioner Christine S. Wilson

Policy Statement on Breaches by Health Apps and Other Connected Devices
Matter No. P205405

September 15, 2021

Today the Commission issues a Policy Statement on Breaches by Health Apps and Other Connected Devices. The Statement asserts that it "serves to clarify the scope of the [Health Breach Notification] Rule, and place entities on notice of their ongoing obligation to come clean about breaches." [1] Rather than "clarifying" the scope of the Rule, this Policy Statement in fact expands it – while contradicting existing FTC business guidance.[2] Moreover, the majority advances this policy U-turn while the agency has an open rulemaking that covers not just this Rule, but precisely the topics addressed by the Policy Statement. The actions taken by the majority today inappropriately curtail the rulemaking proceeding and deprive the public of the opportunity to comment on these significant modifications.

I am sympathetic to the majority's goals of providing higher levels of protection to sensitive consumer health data. During my tenure as a Commissioner, I have been an ardent advocate for federal privacy legislation.[3] One compelling rationale for comprehensive privacy legislation that I have cited pertains to "emerging gaps in sector-specific approaches created by evolving technologies."[4] Specifically, I have observed that Health Insurance Portability and

[1] FTC Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021) (italics added), https://www.ftc.gov/news-events/events-calendar/open-commission-meeting-september-15-2021.

[2] FTC Business Guidance, *Complying with the FTC's Health Breach Notification Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule, attached as Exhibit A.

[3] Oral Statement of Commissioner Christine S. Wilson, FTC, Before the U.S. House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce (July 28, 2021), https://www.ftc.gov/system/files/documents/public_statements/1592954/2021-07-28_commr_wilson_house_ec_opening_statement_final.pdf; Christine Wilson, Op-Ed, *Coronavirus Demands a Privacy Law*, WALL ST. J., May 13 2020, *available at* https://www.wsj.com/articles/congress-needs-to-pass-a-coronavirus-privacy-law-11589410686; Oral Statement of Commissioner Christine S. Wilson, FTC, Before the U.S. Senate Committee on Commerce, Science, and Transportation (April 20, 2021), https://www.ftc.gov/system/files/documents/public_statements/1589180/opening_statement_final_for_postingrevd.pdf; Christine Wilson, Privacy in the Time of Covid-19, TRUTH ON THE MARKET (Apr. 15, 2020), https://truthonthemarket.com/author/christinewilsonicle/; Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation, Remarks at the Future of Privacy Forum, Feb. 6, 2020, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf; Oral Statement of Commissioner Christine S. Wilson Before the U.S. House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce (May 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1519254/commissioner_wilson_may_2019_ec_opening.pdf; Oral Statement of Commissioner Christine S. Wilson, FTC, Before the U.S. Senate Committee on Commerce, Science, and Transportation Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security (Nov. 27, 2018), https://www.ftc.gov/system/files/documents/public_statements/1423979/commissioner_wilson_nov_2018_testimony.pdf.

[4] Oral Statement of Commissioner Christine S. Wilson Before the U.S. House Committee on Energy and Commerce Subcommittee on Consumer Protection and Commerce (May 8, 2019), https://www.ftc.gov/system/files/documents/public_statements/1519254/commissioner_wilson_may_2019_ec_opening.pdf.

Accountability Act (HIPAA) "applies to patient information maintained by doctors' offices, hospitals, and insurance companies, but not to wearables, apps, or websites like WebMD."[5] The COVID-19 pandemic has further underscored concerns about the privacy of sensitive health data.[6]

To the extent the Commission possesses authority to address consumer health data provided to mobile health apps through its Health Breach Notification Rule ("HBNR"), I support employing that authority. Here, though, I am concerned that the Policy Statement issued by the majority today not only short-circuits our ongoing rulemaking, but seeks to improperly expand our statutory authority[7] – and to do so unilaterally, rather than in concert with other federal agencies with related jurisdiction.

The Health Breach Notification Rule is Narrowly Crafted to Apply in Limited, Highly Specific Circumstances

The HBNR requires vendors of personal health records ("PHRs") and related entities to notify the Commission and consumers of a "breach of security."[8] This Rule was intended to serve as a gap-filler: it covers health care providers not already covered by HIPAA that collect consumer health data.[9] When promulgating this Rule, the FTC worked closely with the Department of Health and Human Services ("HHS") to make sure that entities not covered by HIPAA were subject to security breach reporting requirements similar to those imposed on their HIPAA-covered counterparts, given that both sets of entities maintain similar types of health records. Close coordination with HHS is imperative, because "the Rule does not apply to health information secured through technologies specified by [HHS] and it does not apply to businesses or organizations covered by HIPAA. HIPAA-covered entities and their 'business associates' must instead comply with HHS's breach notification rule."[10]

---

[5] *Id.*

[6] Christine Wilson, Privacy in the Time of Covid-19, TRUTH ON THE MARKET (Apr. 15, 2020), https://truthonthemarket.com/author/christinewilsonicle/; Christine S. Wilson, A Defining Moment for Privacy: The Time is Ripe for Federal Privacy Legislation, Remarks at the Future of Privacy Forum, Feb. 6, 2020, https://www.ftc.gov/system/files/documents/public_statements/1566337/commissioner_wilson_privacy_forum_speech_02-06-2020.pdf.

[7] Dissenting Statement of Commissioner Christine S. Wilson, Final Rule related to Made in U.S.A. Claims (July 1, 2021), https://www.ftc.gov/system/files/documents/public_statements/1591494/2021-07-01_commissioner_wilson_statement_musa_final_rule.pdf; Statement of Commissioner Christine S. Wilson Concurring in Part, Dissenting in Part, Notice of Proposed Rulemaking related to Made in U.S.A claims (June 22, 2020), https://www.ftc.gov/system/files/documents/public_statements/1577099/p074204musawilsonstatementrev.pdf

[8] 16 C.F.R. § 318.3.

[9] Notably, this Rule draws critical definitions from Section 13407 of the Health Information Technology for Economic and Clinic Health (HITECH) Act within the American Recovery and Reinvention Act. The hearing surrounding the privacy provisions of this Act focused almost exclusively on medical records and the clinical side of the health information technology space. Health Information Technology: Protecting Americans' Privacy in the Digital Age, Hearing before the Comm't on the Judiciary, U.S. Senate, 111 Cong. (Jan. 27, 2009), https://www.judiciary.senate.gov/meetings/health-it-protecting-americans-privacy-in-the-digital-age.

[10] Health Breach Notification, Request for Public Comment, 85 Fed. Reg. 31085 (May 22, 2020).

Understanding the Rule's application requires delving into the terminology contained both in this Rule and in the Social Security Act, which is cross-referenced in the Rule. These key terms are explained below.

1. Personal Health Record

A PHR is defined in the Rule 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." 16 C.F.R. §318.2(d) (italics added).

2. PHR identifiable health information

The Rule defines "PHR identifiable health information" as: "individually identifiable health information," as defined in section 1171(6) of the Social Security Act (42 U.S.C. 1320d(6)):

> (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. *Id.* § 318.2(e).

3. Individually identifiable health information

Section 1171(6) of the Social Security Act defines "'individually identifiable health information" as "any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and (B) 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, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual." 42 U.S.C. 1320d(6).

4. Health Care Provider

The Social Security Act defines health care provider to include "any other person furnishing health care services or supplies." 42 U.S.C. 1320d(3). Although this language is quite broad, guidance on the HHS website defines "health care provider" to include doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies.[11]

5. Drawn from Multiple Sources

As noted above, the Rule defines a PHR 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." This definition aligns with Section 13400(11) of ARRA. 42 U.S.C. § 17921(11) (italics added). The Commission has interpreted

---

[11] Guidance on HIPAA-covered entities on HHS's website states that the category of "Health Care Provider" includes doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies. "Covered Entities and Business Associates," Dep't of Health & Human Servs., https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html (last visited Sep. 14, 2020).

"can be drawn" to mean capable of being drawn from more than one source, as any other interpretation would render the phrase superfluous.[12]

Application of the Rule to Mobile Health Apps is a Novel, Expansive Interpretation

The U-turn advanced in the majority's Policy Statement under the guise of a "clarification" has sweeping implications that, under normal circumstances, would be subject to discussion with all relevant stakeholders and the public. For example, applying the moniker of "health care provider" to mobile health apps presents novel issues that deserve careful consideration. How broadly does the Commission intend to read this language? Presumably some limiting principles apply, or the language could sweep in, for example, the Amazon app because Amazon "furnishes" "health care…supplies" like Band-Aids. This issue is not a trivial one. Given statutory cross-referencing, the interpretation adopted by the FTC could have implications for our sister agencies, the Social Security Administration ("SSA") and HHS.

In addition, the interpretation of the phrase "can be drawn from multiple sources" is important here. The majority's Policy Statement observes:

> 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 synching 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*. 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.[13]

Remarkably, our existing business guidance discusses a strikingly similar scenario and concludes that the Rule does *not* apply:

> If consumers can simply input their own information on your site in a way that doesn't interact with personal health records offered by a vendor – for example, if your site just allows consumers to input their weight each week to track their fitness goals – you're not a PHR-related entity.[14]

In other words, the FTC previously viewed the phrase "multiple sources" as referring to actual entities, not other data sources on the consumer's mobile or connected device, such as calendar

---

[12] *See* FTC Business Guidance, *Complying with the FTC's Health Breach Notification Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule, attached as Exhibit A.

[13] FTC Policy Statement on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021) (italics added), https://www.ftc.gov/news-events/events-calendar/open-commission-meeting-september-15-2021.

[14] FTC Business Guidance, *Complying with the FTC's Health Breach Notification Rule*, https://www.ftc.gov/tips-advice/business-center/guidance/complying-ftcs-health-breach-notification-rule, attached as Exhibit A.

dates. And the Rule defines a covered record as one that includes PHR *identifiable health information* drawn from multiple sources, not any information drawn from another source.[15]

Issuance of this Policy Statement Curtails Ongoing Rulemaking

Perhaps even more noteworthy than a policy U-turn is a policy U-turn undertaken during the pendency of a rulemaking that covers precisely the topic at issue. Unfortunately, new leadership at the FTC appears poised to make this a regular practice. On September 21, 2020 the FTC and the Antitrust Division of the Department of Justice jointly issued a Notice of Proposed Rulemaking and an Advanced Notice of Proposed Rulemaking seeking public comment regarding the Hart-Scott-Rodino Act ("HSR") and its implementing rules.[16] The ANPRM posed two questions with a combined 11 sub-parts to the relationship between the treatment of debt and calculation of the acquisition price. Despite the pendency of a rulemaking proceeding seeking public comment on precisely this issue, the FTC last month unilaterally withdrew business guidance regarding the treatment of debt, enacting a policy U-turn before assimilating public input.[17]

Similarly, the Commission's ongoing rulemaking proceeding for the HBNR is directly relevant to the substance of the Policy Statement announced today. For example, the Federal Register Notice observed that "as consumers turn towards direct-to-consumer technologies for health information and services (such as mobile health applications, virtual assistants, and platforms' health tools), more companies *may be covered* by the FTC's Rule."[18] And we sought public input on several topics that directly pertain to the "clarification" covered by the majority's Policy Statement. Specifically, we asked:

- What modifications, if any, should be made to the Rule to account for changes in relevant technology, economic conditions, or laws? For example, as the healthcare industry adopts standardized application programming interfaces ("APIs") to help individuals to access their electronic health information with smartphones and other mobile devices (as required by rules implementing the 21st Century Cures Act), will the number of entities subject to the Commission's HBN Rule increase?

- Should the definitions of "PHR related entity" in § 318.2(f), "Third party service provider" in § 318.2(h), or "Vendor of personal health records" in Section 318.2(j) be modified in light of changing technological and economic conditions, such as the

[15] 16 C.F.R. §318.2(d). Commissioner Phillips notes in his statement that the Policy Statement appears also to go beyond the text of the statute in its description of "breaches" covered by the Rule's notification provisions extending covered to any unauthorized *access*, when the law limits the HBNR to breaches of security.

[16] Press Release, FTC and DOJ Seek Comments on Proposed Amendments to HSR Rules and Advanced Notice of Proposed HSR Rulemaking (Sept. 21, 2010), https://www.ftc.gov/news-events/press-releases/2020/09/ftc-doj-seek-comments-proposed-amendments-hsr-rules-advanced.

[17] FTC Blog Post, Reforming the Pre-Filing Process for Companies Considering Consolidation and a Change in the Treatment of Debt (Aug. 26, 2021), https://www.ftc.gov/news-events/blogs/competition-matters/2021/08/reforming-pre-filing-process-companies-considering; FTC Statement, The Treatment of Debt as Consideration (Aug. 26, 2021), https://www.ftc.gov/enforcement/premerger-notification-program/hsr-resources/treatment-debt-consideration.

[18] Health Breach Notification, Request for Public Comment, 85 Fed. Reg. 31085 (May 22, 2020) (emphasis added).

proliferation of mobile health applications ("apps"), virtual assistants offering health services, and platforms' health tools? If so, how, consistent with the Act's requirements?

- What are the implications (if any) for enforcement of the Rule raised by direct-to-consumer technologies and services such as mobile health apps, virtual assistants, and platforms' health tools?

I have not been provided with an analysis of, and the majority does not discuss, whether and to what extent commenters have addressed the directly relevant questions noted above. It is likely that we have received input on these issues, but it is not clear whether the majority's actions reflect that input.

Aside from the HSR incident mentioned above, I am aware of only one other instance in which the Commission issued a policy statement during a related rulemaking. Specifically, while the rule reviews for Textile, Wool and Fur Rules were ongoing, the Commission issued a policy statement describing the circumstances under which it would refrain from initiating enforcement actions.[19] In other words, while awaiting and assimilating public comment, the agency announced that it would use its prosecutorial discretion to forego legal action in certain circumstances. Today's situation is markedly different.

Here, the policy statement significantly expands both the covered universe of entities and the circumstances under which the Commission will initiate enforcement. Given the novel and expansive interpretation of this Rule that the Commission announces today, and consistent with past practice, it would be prudent for the Commission to publish a Federal Register Notice announcing the modifications to the Rule. The Federal Register Notice should be drafted by our knowledgeable staff from the Bureau of Consumer Protection and the Office of the General Counsel, and should include a full description of the public comments we received; a thorough analysis of the Rule changes; an explanation of how those changes comport with our legal authority and the statutory intent; and the nature of our consultation (if any) with HHS and the SSA, as this Rule cross references the SSA and intersects with HHS rules.

Instead, the majority is making a unilateral announcement that could have a substantial impact on our sister agencies that possess both significant expertise in the health care arena and authority for enforcing related regulatory frameworks. Moreover, our unilateral actions may impact entities otherwise subject to our sister agencies' jurisdiction. A good government approach would entail a robust dialogue with all relevant stakeholders, a thorough and objective assessment of the public comments we have received, and – if appropriate – modifications to the scope of the Rule within the guardrails of the ongoing rulemaking proceeding.

The majority has chosen quite a different approach. Accordingly, I dissent.

---

[19] *See* Enforcement Policy Statement Regarding Certain Imported Textile, Wool, and Fur Products (Jan. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/ftc-announces-enforcement-policy-statement-retailers-directly; *see also* 76 Fed. Reg. 68690 (Nov. 7, 2001); Press Release, FTC Seeks Public Input in Review of Textile Labeling Rules (Nov. 1, 2011); https://www.ftc.gov/news-events/press-releases/2011/11/ftc-seeks-public-input-review-textile-labeling-rules.

EXHIBIT A

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

COMPLYING WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE

TAGS: Privacy and Security | Consumer Privacy | Data Security | Health Privacy
RELATED RULE: Health Breach Notification Rule

Guidance for business on complying with the FTC's Health Breach Notification Rule. Who's covered by the Rule and what companies must do if they experience a breach of personal health records.

More and more, personal medical information is online. For most hospitals, doctors' offices, and insurance companies, the Health Insurance Portability and Accountability Act (HIPAA) governs the privacy and security of health records stored online. But many web-based businesses that collect people's health information aren't covered by HIPAA. These include online services people use to keep track of their health information and online applications that interact with those services.

The Federal Trade Commission (FTC), the nation's consumer protection agency, has issued the Health Breach Notification Rule to require certain businesses not covered by HIPAA to notify their customers and others if there's a breach of unsecured, individually identifiable electronic health information. FTC enforcement began on February 22, 2010.

Is your business covered by the Health Breach Notification Rule? Do you know your legal obligations if you experience a security breach?

WHO'S COVERED BY THE HEALTH BREACH NOTIFICATION RULE

The Rule applies if you are:

- a **vendor of personal health records (PHRs)**;
- a **PHR-related entity**; or
- a **third-party service provider** for a **vendor of PHRs** or a **PHR-related entity**.

Vendor of personal health records. For the purposes of the Rule, your business is a vendor of personal health records if it "offers or maintains a personal health record." A **personal health record** is defined as an electronic record of "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." For example, if you have an online service that allows consumers to store and organize medical information from many sources in one online location, you're a vendor of personal health records. You're not a vendor of personal health records if you're covered by HIPAA.

PHR-related entity. Your business is a PHR-related entity if it interacts with a vendor of personal health records either by offering products or services through the vendor's website – even if the site is covered by HIPAA – or by accessing information in a personal health record or sending information to a personal health record. Many businesses that offer web-based apps for health information fall into this category. For example, if you have an app that helps consumers manage their medications or lets them upload readings from a device like a blood pressure cuff or pedometer into a personal health record, your business is a PHR-related entity. However, if consumers can simply input their own information on your site in a way that doesn't interact with personal health records offered by a vendor – for example, if your site just allows consumers to input their weight each week to track their fitness goals – you're not a PHR-related entity. You're not a PHR-related entity if you're already covered by HIPAA.

Third-party service provider. Your business is a third-party service provider if it offers services involving the use, maintenance, disclosure, or disposal of health information to vendors of personal health records or PHR-related entities. For example, if a vendor of personal health records hires your business to provide billing, debt collection, or data storage services related to health information, you're a third-party service provider, and covered by the Rule.

WHAT TRIGGERS THE NOTIFICATION REQUIREMENT

The Rule requires that you provide notice when there has been an **unauthorized acquisition** of **PHR-identifiable health information** that is **unsecured** and in a **personal health record**. How those terms are defined is important:

- **Unauthorized acquisition**. If health information that you maintain or use is acquired by someone else without the affected person's approval, it's an unauthorized acquisition under the Rule. For example, say a thief steals an employee's laptop containing unsecured personal health records or someone on your staff downloads personal health records without approval. Those are probably unauthorized acquisitions that trigger the Rule's notification requirement.
- **PHR-identifiable health information**. The notification requirements apply only when you've experienced a breach of PHR-identifiable health information. This is health information that identifies someone or could reasonably be used to identify someone. For example, say someone hacks into a company database that contains zip codes, dates of birth, and medication information. Even though the database didn't contain names, it would be reasonable to believe the information could be used to identify people in the database. But what if a hacker gains access to a database that contains only city and medication data and finds out that ten anonymous individuals in New York City have been prescribed a widely-used drug? That probably wouldn't be considered PHR-identifiable health information because it couldn't reasonably be used to identify specific people.
- **Unsecured information**. The Rule applies only to unsecured health information, defined by the U.S. Department of Health and Human Services (HHS) to include any information that is not encrypted or destroyed. If your employee loses a laptop containing only encrypted personal health records, for example, you wouldn't be required to provide notification.
- **Personal health record**. A personal health record is an electronic health record that can be "drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." If your business experiences a breach involving only paper health records – not electronic records – the FTC's Rule doesn't require any notification. However, because many states have notification laws that might apply, it's wise to consult your attorney.

WHAT TO DO IF A BREACH OCCURS

If your business is a **vendor of personal health records** or a **PHR-related entity** and there's a security breach, the Rule spells out your next steps. You must notify:

1. each affected person who is a citizen or resident of the United States;
2. the Federal Trade Commission; and
3. in some cases, the media.

Here are the details of the Rule's main requirements about **who** you must notify and **when** you must notify them, **how** you must notify them, and **what** information to include.

WHO you must notify and WHEN you must notify them

People: If you experience a breach of unsecured personal health information, you must notify each affected person "without unreasonable delay" – and within 60 calendar days after the breach is discovered. The countdown begins the day the breach becomes known to someone in your company – or the day someone should reasonably have known about it. Although the Rule requires you to notify people within 60 calendar days, it also requires you to act without unreasonable delay. That means if a company discovers a breach and gathers the necessary information within, say, 30 days, it is unreasonable to wait until the 60th day to notify the people whose information was breached.

The FTC: The Rule requires you to notify the FTC, but the timing depends on the number of people affected.

If the breach involves the information of 500 people or more, you must notify the FTC as soon as possible and within 10 business days after discovering the breach. To report the breach to the agency, you must use the form at www.ftc.gov/healthbreach.

If the breach involves the information of fewer than 500 people, you have more time. Indeed, you must send the same standard form to the FTC – along with forms documenting any other breaches during the same calendar year involving fewer than 500 people – within 60 calendar days following the end of the calendar year. So, if your company experiences one breach in April affecting the records of 100 people and a second breach in September affecting the records of 50 people, the 60-day countdown begins January 1st of the next year.

The media: When at least 500 residents of a particular state, the District of Columbia, or a U.S. territory or possession are affected by a breach, notification takes on an extra dimension. Without unreasonable delay – and within 60 calendar days after the breach is discovered – you must notify prominent media outlets serving the relevant locale, including Internet media where appropriate. This media notice is a supplement to your notice to people whose information was breached, not a substitute for individual notices.

If your company is a **third-party service provider** to a vendor of personal health records or a PHR-related entity, you have notice requirements under the Rule, too. As a preliminary matter, the Rule requires those clients to tell you up front that they're covered by the Rule. If you experience a breach, you must notify an official designated in your contract with your client – or if there is no designee, a senior official of the company – without unreasonable delay and within 60 calendar days of discovering the breach. You must identify for your client each person whose information may be involved in the breach. But it isn't sufficient to simply send the notice and assume the ball is in your client's court. You must get an acknowledgment that they received your notice. They, in turn, must notify the people affected by the breach, the FTC, and, in certain cases, the media.

HOW to notify people

The best practice in notifying people is to find out from your customers in advance – perhaps when they sign up for your service – if they'd prefer to hear about a security breach by email or by first-class mail. If you collect only email addresses from your customers, you can send them a message – or let new customers know when they sign up – that you intend to contact them by email about any security breaches. However, remember that if you plan to use email as your default

method, you must give your customers the opportunity to choose first-class mail notification instead and that option must be clear and conspicuous. If email is a customer's preference, explain how to set up any spam filters so they will get your messages.

What if you've made reasonable efforts to reach people affected by the breach, but you haven't been able to contact each of them? If you fail to contact 10 or more people because of insufficient or out-of-date contact information, you must provide substitute notice through:

1. a clear and conspicuous posting for 90 days on your home page; or
2. a notice in major print or broadcast media where those people likely live.

Both of these forms of substitute notice must include a toll-free phone number that has to be active for at least 90 days so people can call to find out if their information was affected by the breach.

WHAT information to include

Regardless of the form of notification, your notice to individuals must be easy to understand and must include the following information:

- a brief description of what happened, including the date of the breach (if you know) and the date you discovered the breach;
- the kind of PHR-identifiable health information involved in the breach – insurance information, Social Security numbers, financial account data, dates of birth, medication information, etc.
- if the breach puts people at risk for identity theft or other possible harm, suggested steps they can take to protect themselves. Your advice must be relevant to the kind of information that was compromised. In some cases, for example, you may want to refer people to the FTC's identity theft website, www.ftc.gov/idtheft. In addition:
  - if the breach involves health insurance information, you might suggest that people contact their healthcare providers if bills don't arrive on time in case an identity thief has changed the billing address, pay attention to the Explanation of Benefit forms from their insurance company to check for irregularities, and contact their insurance company to notify them of possible medical identity theft or to ask for a new account number.
  - if the breach includes Social Security numbers, you might suggest that people get a free copy of their credit report from www.annualcreditreport.com, monitor it for signs of identity theft, and place a fraud alert on their credit report. If they spot suspicious activity, they should contact their local police and, if appropriate, get a credit freeze.
  - if the breach includes financial information – for example, a credit card or bank account number – you might suggest that people monitor their accounts for suspicious activity and contact their financial institution about closing any accounts that may have been compromised.
- a brief description of the steps your business is taking to investigate the breach, protect against future breaches, and mitigate the harm from the breach; and
- how people can contact you for more information. Your notice must include a toll-free telephone number, email address, website, or mailing address.

ANSWERS TO QUESTIONS ABOUT THE HEALTH BREACH NOTIFICATION RULE

Here are answers to some questions businesses have asked about the FTC's Health Breach Notification Rule:

Why did the FTC implement the Health Breach Notification Rule?

As part of the American Recovery and Reinvestment Act of 2009 – which advances the use of health information technology – Congress directed the FTC and HHS to study potential privacy, security and breach notification requirements and make recommendations. In the meantime, Congress directed the FTC to implement a temporary rule – the Health Breach Notification Rule – that non-HIPAA businesses must follow if there's a security breach. FTC enforcement began on February 22, 2010.

It looks like someone accessed our database without our consent. We don't know if they downloaded anything. Is that the kind of "unauthorized acquisition" that would trigger the Rule's notification requirements?

It should trigger an examination on your part to determine your obligations under the Rule. There may be unauthorized access to data, but it's not always clear at first blush whether the data also has been "acquired" – that is, downloaded or copied. In these cases the Rule has a rebuttable presumption: Where there has been unauthorized access, unauthorized acquisition is presumed unless you can show that it hasn't – or couldn't reasonably have – taken place. For example, if one of your employees accesses a customer's personal health record without authorization, the Rule presumes that because the data was accessed, it has been "acquired," and you must follow the breach notification provisions of the Rule. But you can overcome that presumption by establishing and enforcing a company policy – one that says if an employee inadvertently accesses a health record, he or she must not read or share the information, must log out immediately, and then must report the access to a supervisor right away. If the employee says he or she didn't read or share the information and you conduct a reasonable investigation that corroborates the employee's version of events, you may be able to overcome the presumption.

Consider another situation involving a lost laptop that contains personal health records. You could rebut the presumption of unauthorized acquisition if the laptop is recovered and forensic analysis shows that files were not opened, altered, transferred, or otherwise compromised.

Our business is in the "HIPAA business associate" category. Does the FTC's Rule apply to us?

If your business acts solely as a "HIPAA business associate" – that is, if you handle only the protected health information of HIPAA-covered entities – the FTC's Rule does not apply. Nor does it apply to HIPAA-covered entities, like a hospital, doctor's office, or health insurance company. If you are a HIPAA-covered entity or act only as a HIPAA business associate, your responsibilities are in the HHS breach notification rule.

The HHS rule requires HIPAA-covered entities to notify people whose unsecured health information is breached. If you are a business associate of a HIPAA-covered entity and you experience a security breach, you must notify the HIPAA-covered entity you're working with. Then they must notify the people affected by the breach.

We're a HIPAA business associate, but we also offer personal health record services to the public. Which Rule applies to us?

If your company is a HIPAA business associate that also offers personal health record services to the public, you may be subject to both the HHS and FTC breach notification rules. For example, say you have your own website that offers individual customers an online service to collect their health information and you sign a HIPAA business associate agreement with an insurance company to maintain the electronic health records of its customers. In the case of a breach affecting all your users, both the FTC Rule and HHS Rule would apply. Under the FTC's Rule, you must notify the people who use the service on your website. In addition, you must notify the insurance company so that it can notify its customers.

If you have a direct relationship with all the people affected by the breach – your customers and the customers of the insurance company – you should contract with the insurance company to notify both your clients and theirs. People are more likely to pay attention to a notice from a company they recognize.

What's the relationship between the FTC's Health Breach Notification Rule and state breach notification laws?

The FTC's Rule preempts contradictory state breach notification laws, but not those that impose additional – but non-contradictory – breach notification requirements. For example, some state laws require breach notices to include advice on monitoring credit reports or contact information for consumer reporting agencies. While these content requirements are different from the FTC Rule's requirements, they're not contradictory. In this example, you could comply with both federal and state requirements by including all the information in a single breach notice. The FTC Rule doesn't require you to send multiple breach notices to comply with state and federal law.

What's the penalty for violating the FTC's Health Breach Notification Rule?

The FTC will treat each violation of the Rule as an unfair or deceptive act or practice in violation of a Federal Trade Commission regulation. Businesses that violate the Rule may be subject to a civil penalty of up to $43,792 per violation.

Law enforcement officials have asked us to delay notifying people about the breach. What should we do?

If law enforcement officials determine that notifying people would impede a criminal investigation or damage national security, the Rule allows you to delay notifying them, as well as the FTC and if required, the media.

Where can I learn more about the FTC's Health Breach Notification Rule?

Visit www.ftc.gov/healthbreach.

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumers spot, stop and avoid them. To file a complaint or get free information on consumer issues, visit ftc.gov or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a new video, How to File a Complaint, at ftc.gov/video to learn more. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

Your Opportunity to Comment

The National Small Business Ombudsman and 10 Regional Fairness Boards collect comments from small businesses about federal compliance and enforcement activities. Each year, the Ombudsman evaluates the conduct of these activities and rates each agency's responsiveness to small businesses. Small businesses can comment to the Ombudsman without fear of reprisal. To comment, call toll-free 1-888-REGFAIR (1-888-734-3247) or go to www.sba.gov/ombudsman.

[Note: Edited January 2021 to reflect Inflation-Adjusted Civil Penalty Maximums.]

April 2010

ftc.gov