



Complying with FTC's Health Breach Notification Rule

Tags: [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#) | [Health Privacy](#)

Related Rules: [Health Breach Notification Rule](#)

As more consumers use health apps and connected devices like fitness trackers, information about our health is increasingly collected and shared 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 companies that collect people's health information – whether it's a fitness tracker, a diet app, a connected blood pressure cuff, or something else – aren't covered by HIPAA. Does that mean this sensitive health information doesn't have any legal protections? Not at all.

The Federal Trade Commission (FTC), the nation's consumer protection agency, enforces Section 5 of the FTC Act, which prohibits companies from misleading consumers or engaging in unfair practices that harm consumers. In addition, the FTC enforces the [Health Breach Notification Rule](#), which requires certain organizations (both businesses and nonprofits) not covered by HIPAA to notify their customers, the FTC, and, in some cases, the media, if there's a breach of unsecured, individually identifiable health information. An [FTC Policy Statement](#) makes clear that makers of health apps, connected devices, and similar products must comply with the Rule.

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. 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 develop a health app that collects information from consumers and can sync

PHR related entity. If you're using a third party app that connects to your personal health records with a consumer's fitness tracker, you're probably 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. For example, a company that offers a fitness tracker is likely a PHR related entity if it sends information to health apps (which are likely personal health records, as described above). Your company is 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 company 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 unsecured PHR identifiable health information. 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. Keep in mind, though, that a "breach" is not limited to cybersecurity intrusions or nefarious behavior by hackers or insiders. Incidents of unauthorized access, including a company's disclosure of covered information without a person's authorization, triggers notification obligations under the Rule.
- **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. Consider two examples. First, suppose you share your users' medical information along with their mobile identifiers with an ad network for the purpose of targeted marketing without first getting the person's consent. Second, say an intruder hacks into your database that contains email addresses, dates of birth, and medication information. Names weren't disclosed in either example. But the information disclosed could still readily identify individual consumers, so it counts as PHR identifiable health information. By contrast, consider a hack of a database containing city and common medication data that reveals 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

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. For example, if your employee loses a laptop containing only encrypted personal health records, you wouldn't be required to notify people.

- Personal health record. A personal health record (PHR) 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. If your product draws information from multiple sources – let's say a diet app that allows users to enter daily weights and an API for pulling calorie counts from restaurant menus – there's a good chance you have a PHR covered by the FTC's Rule.

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 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, using [this form](#); 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 would be 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 (use [this form](#)), 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 [this form](#) 

If the breach involves the information of fewer than 500 people, you have more time. 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. This media notice is a supplement to the individual notice you must give to people whose information was breached. It's 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. It isn't enough just to 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 for 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 website 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 must be active for at least  30 days so people can call to learn 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. You may want to refer people to the FTC’s page within [IdentityTheft.gov](#), [When Information Is Lost or Exposed](#). 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, check the Explanation of Benefit forms from their insurance company for irregularities, and review their medical records for errors. If people spot anything unusual, they should contact their insurance company about 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 credit freeze on their credit report. If they spot suspicious activity, they should visit [IdentityTheft.gov](#) to report it and get a personalized recovery plan.
 - 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.
 - If the breach involved an app or connected device, you might suggest that people review the app’s or device’s privacy settings and download the latest updates to fix any privacy or security glitches.
- 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 and issue its recent Policy Statement?


Congress directed the FTC to implement the Health Breach Notification Rule, which non-HIPAA covered businesses must follow if there's a breach of consumers' unsecured, individually identifiable health information. The FTC issued the [Policy Statement](#) because, as one of only a handful of federal privacy laws protecting consumers' health information, the Rule plays a vital role in holding companies accountable for how they disclose consumers' sensitive health information. Since the FTC first issued the Rule more than a decade ago, consumers have turned to apps, wearables, and other technologies for health advice, information, and tracking. It is imperative that the FTC's enforcement of its Rule keep pace with changing technology.

What is considered a "breach of security" under the Rule?

Under the rule, a "breach of security" is defined as the acquisition of unsecured PHR identifiable health information of an individual in a personal health record without the individual's authorization. A breach is not limited to cybersecurity intrusions. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, trigger notification obligations under the Rule.

It looks like we accidentally sent some of our users' health information to a social media platform. It also looks like someone accessed our database without our consent. We don't know if the social media company used the information and we don't know if anyone downloaded anything. Are these the kinds of "unauthorized acquisitions" that would trigger the Rule's notification requirements?

Both incidents should trigger an examination on your part to determine your obligations under the Rule. Importantly, with respect to the first incident, the [FTC's Policy Statement](#) makes clear that the Rule does not just apply to cybersecurity intrusions or other nefarious behavior. To the contrary, if you disclose consumers' unsecured, individually identifiable health information without their consent, a breach has occurred.

In the second incident – the database access – it's not clear 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 that requires an employee who inadvertently accesses a health record not to read it or share it, to log c  immediately, and to 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.

My company makes a fitness app, in which consumers input their height, weight, age, and other information. The app, which consumers can download from the app store, can sync with wearable fitness trackers. Some of our users use this syncing feature, but others don't. Is my company required to comply with the FTC's Rule?

You are likely a vendor of personal health records. Your app includes identifiable health information, such as information about your health, weight, and steps taken; that information can be drawn from multiple sources – the consumer's inputs of height and weight and the information from the fitness tracker; and the user manages, shares, and controls the information in the app.


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 doesn't 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 [Health and Human Services \(HHS\) Breach Notification Rule](#).

The HHS Rule requires HIPAA-covered entities to notify people whose unsecured protected 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 develop an app that people can download from an app store and upload their health information. Separately, 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 your app. In addition, you must notify the insurance company so 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 separate 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 \$46,517 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 the FTC's [Health Breach Notification Rule page](#).

The FTC works to prevent fraudulent, deceptive and unfair business practices in the marketplace and to provide information to help consumer spot, stop and avoid them. To file a complaint, visit [ReportFraud.ftc.gov](#) or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. Watch a video, [How to File a Complaint](#), 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](#).



