FTC FACTS for Business

ftc.gov
For The Consumer
Federal Trade Commission
1-877-FTC-HELP

Complying with the FTC's Health Breach Notification Rule

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:

- a clear and conspicuous posting for 90 days on your home page; or
- 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 $16,000 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**.

For More Information

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**.

Federal Trade Commission	ftc.gov
1-877-FTC-HELP	For The Consumer

Federal Trade Commission
Bureau of Consumer Protection
Division of Consumer and Business Education

April 2010