



FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

Collecting, Using, or Sharing Consumer Health Information? Look to HIPAA, the FTC Act, and the Health Breach Notification Rule

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

Does your business collect, use, or share consumer health information? When it comes to privacy and security, you've probably thought about the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Privacy, Security, and Breach Notification Rules (HIPAA Rules). But did you know you also may need to comply with the Federal Trade Commission Act and the FTC's Health Breach Notification Rule? Learn more about your obligations under these laws to maintain the privacy and security of consumers' health information and provide notification if you experience a breach.

HIPAA

Let's start with HIPAA. The HIPAA Rules apply to you if you are a HIPAA [covered entity](#) – a health plan, a health care provider that conducts standard health care transactions electronically, or a health care clearinghouse. Parts of the HIPAA Rules also apply if you are a [business associate](#) – a company or other entity that helps a covered entity carry out its health care activities and functions or provides certain services to a covered entity or another business associate involving access to individuals' "protected health information" (PHI). PHI is most "individually identifiable health information" held or transmitted by a

covered entity or its business associate, in any form or medium, whether electronic, paper, or oral.

The [HIPAA Privacy Rule](#) sets limits and conditions on the uses and disclosures of PHI that covered entities and business associates may make without an individual's authorization and provides individuals with rights with respect to their health information. Under the Privacy Rule, a covered entity or business associate must obtain an individual's valid HIPAA authorization to use or disclose the individual's PHI for marketing purposes. Here are some highlights of the Privacy Rule's requirements for an authorization when one is required:

- **Get the individual's signed authorization before making the use or disclosure.** You can obtain an individual's authorization electronically or in non-electronic form. With limited exceptions, you cannot condition your provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the individual providing an authorization for the use or disclosure of their PHI.
- **Put it in plain language.** HIPAA authorizations provide individuals a way to understand and control uses and disclosures of their health information. The authorization must be in **plain language**. If people can't understand it, it is not effective. Explain who is being authorized to make the use or disclosure, what information will be used or disclosed, who will receive the information, when the permission expires, and the purpose for which the information will be used and disclosed.
- **Be specific in your description of how you want to use or disclose health information.** The authorization must describe the specific purpose for a requested use or disclosure. For example, if you want an individual to authorize you to share their health information, you need to tell them specifically how it will be used and disclosed – for example, by a pharmaceutical company for marketing purposes, a life insurer for coverage purposes, or an employer for screening purposes.
- **If you will benefit financially from a disclosure, clearly say so in the authorization.** The Privacy Rule prohibits you from selling PHI unless you obtain an authorization stating that you will receive remuneration from making the disclosure.

If you are a business associate, there's a crucial first step. **The covered entity must give you permission through a [HIPAA business associate agreement](#) for any use or disclosure of PHI.** This means you cannot ask an individual to sign a HIPAA authorization unless your business associate agreement permits you to do so.

The [HIPAA Security Rule](#) requires HIPAA covered entities and their business associates to implement safeguards to protect the confidentiality, integrity, and availability of all electronic PHI (ePHI) the covered entity or business associate creates, receives, maintains, or transmits. Examples of safeguards established by the Security Rule include:

- Identifying potential risks and vulnerabilities to ePHI and implementing security measures to reduce those risks and vulnerabilities.
- Providing security awareness and training to all workforce members.
- Establishing contingency plans that include backing up ePHI data and disaster recovery.
- Identifying and responding to suspected or known security incidents.
- Using access controls to limit access to ePHI to only authorized workforce members.
- Implementing encryption to protect ePHI where reasonable and appropriate.
- Maintaining audit controls and reviewing information system activity.

The [HIPAA Breach Notification Rule](#) requires HIPAA covered entities to [provide notification](#) to affected individuals, [the Secretary of HHS](#), and, in some cases, the media, following a breach of unsecured PHI. The Breach Notification Rule also requires business associates to notify the covered entity if the business associate experiences such a breach. Unsecured PHI is PHI that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in [guidance](#).

Breach reports to the Secretary of HHS must be submitted through [OCR's breach portal](#). The breach portal also includes a [list of breaches affecting 500 or more individuals](#).

FTC Act

The FTC Act prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce. This means that companies must not mislead consumers about – among other things – what’s happening with their health information. It also means you must ensure your health data practices aren’t causing more harm than good. The FTC Act’s obligations apply to HIPAA-covered entities and business associates, as well as to companies that collect, use, or share health information that aren’t required to comply with HIPAA.

Practically speaking, what does that mean? Your business must consider everything you say or imply to consumers about the use, collection, retention, or sharing of their health data – and anything material you *fail* to say – to make sure you don’t create a deceptive or misleading impression. For example, if you’re covered by HIPAA and the information surrounding your HIPAA authorization is deceptive or misleading (such as by implying that to receive treatment, the consumer must agree to have their data used for advertising purposes), that’s a violation of the FTC Act. If you claim that you’ll delete personal information upon request, but in fact fail to deliver on that promise, that’s a violation of the FTC Act.

In addition, your business should consider whether your practices cause harm to consumers or are likely to harm them. Where consumers can’t reasonably avoid the likelihood of substantial injury and the benefits to consumers or competition don’t outweigh it, the FTC can challenge the practice as unfair. For instance, failing to take reasonable steps to protect and secure health information from unauthorized use or disclosure may be an unfair practice.

WHAT CAN YOU DO TO COMPLY WITH THE FTC ACT?

- **Review your data policies, procedures, and practices.** The FTC Act requires you to take privacy and security into account in your collection, use, retention, and disclosure of consumers’ health information. The first step is understanding your data flows. What health information are you collecting? From what sources? How are

you using it? To whom are you disclosing it? For what purposes? How long are you retaining it and why? The second step is ensuring you are implementing robust safeguards to protect the privacy and security of the health information, such as a written program, training and supervision, data retention, purpose, and use limitations; and (where appropriate) mechanisms to obtain the consumer's affirmative express consent. You also need to make sure that your representations to consumers are clear and conspicuous and consistent with your practices. The third step is periodically reviewing your practices (including a reconsideration of the first two steps) to make sure your safeguards are working effectively and your current practices still line up with the claims you've made.

- **Review your entire user interface, including any claims you make, from the consumer's point of view.** For example, as we've noted in [other guidance](#), don't make false or misleading claims that you are "HIPAA Compliant," "HIPAA Secure," "HIPAA Certified" or the like. Also, don't bury key facts in a privacy policy, a Terms of Use section, or other places where consumers aren't likely to read and understand them. Keep it simple for consumers so that where you ask for consent, that consent is meaningful. Evaluate the size, color, and graphics of all of your statements to consumers to ensure they are clear and conspicuous.

FTC's Health Breach Notification Rule



The [Health Breach Notification Rule](#) applies to certain businesses that aren't covered by HIPAA – specifically, vendors of personal health records (PHR), PHR related entities, and third party service providers. Does your business or organization have a mobile app, website, Internet-connected device, or similar technology that holds consumers' electronic health information in a personal health record? Do you provide products or services or send or receive data to or from that kind of product? Do you deal with health information while providing services to companies that offer those products? If so, you may be required to comply with this Rule.

The FTC's Health Breach Notification Rule requires companies that experience a breach of security of consumers' identifying health information to notify affected consumers, the FTC, and, in some cases, the media. A "breach of security" under the Rule includes an

unauthorized acquisition of identifiable health information that occurs as a result of a data security breach *or* an unauthorized disclosure by the company itself.

The FTC's Health Breach Notification Rule applies only to identifying health information that is not secured through technologies specified by the Department of Health and Human Services.

WHAT CAN YOU DO TO COMPLY WITH THE FTC'S HEALTH BREACH NOTIFICATION RULE?

- **Understand your obligations under the Health Breach Notification Rule.** Review [Complying with the FTC's Health Breach Notification Rule](#), which explains who's covered by the Rule and offers guidance on what to do in case of a breach.
- **Report breaches in a timely fashion.** Companies must timely report breaches to the FTC using this [standard reporting form](#) . The FTC periodically posts a [list of breaches](#)  involving the information of 500 or more individuals. Failing to make the necessary notifications or failing to make timely notifications as required by the Rule could result in an enforcement action and significant civil penalties.

If you have a health app, consult the [mobile health app interactive tool](#), the [FTC's best practices guidance for mobile health app developers](#) and the [HHS Office for Civil Rights' resources for mobile health apps developers](#). And when you're telling consumers about how you share consumer health information, keep the FTC Act, the FTC's Health Breach Notification Rule, and the HIPAA Rules in mind.

About the FTC

The FTC works to prevent fraudulent, deceptive, and unfair practices that target businesses and consumers. Report scams and bad business practices at [ReportFraud.ftc.gov](#). We also provide guidance at [business.ftc.gov](#) to help companies comply with the law. Regardless of the size of your organization or the industry you're in, knowing – and fulfilling – your compliance responsibilities is smart, sound business. Looking for a quick take on recent cases and other initiatives? Subscribe to the FTC's Business Blog.

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.

September 2023