U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
OFFICE FOR CIVIL RIGHTS

Sharing Consumer Health Information?

Look to HIPAA and the FTC Act

Does your business collect and share consumer health information? When it comes to privacy, you've probably thought about the Health Insurance Portability and Accountability Act (HIPAA). But did you know that you also need to comply with the Federal Trade Commission (FTC) Act? This means if you share health information, it's not enough to simply consider the HIPAA regulations. You also must make sure your disclosure statements are not deceptive under the FTC Act.

HIPAA

Let's start with HIPAA. The HIPAA Privacy Rule requires certain entities to protect the privacy and security of health information. The Rule also provides consumers with certain rights with respect to their information. This Rule applies to you if you are a *HIPAA covered entity*— a health plan, most health care providers, or a health care clearinghouse. It also applies if you are a *business associate* – a person or company that helps a covered entity carry out its health care activities and functions. Here are some highlights of the HIPAA Privacy Rule requirements for covered entities and business associates:

- In order for you to use or disclose consumer health information for commercial activities besides treatment, payment, health care operations, or other uses and disclosures permitted or required by the Privacy Rule, the consumer must first give you written permission through a **valid HIPAA authorization**.

- HIPAA authorizations provide consumers a way to understand and control their health information. The authorization must be in **plain language**. If people can't understand it, then it isn't effective. Think about who, what, when, where and why. Explain who is disclosing and receiving the information, what they are receiving, when the disclosure permission expires, where information is being shared, and why you are sharing it.

- The authorization must include **specific terms and descriptions.** For example, if you want consumers to authorize you to share their health information, you need to tell them specifically how it will be used – for example, by a pharmaceutical company for marketing purposes, a life insurer for coverage purposes, or an employer for screening purposes.

If you are a business associate, there's a crucial first step: **the covered entity must give you explicit permission** through a HIPAA business associate contract to use or disclose health information. This means you cannot ask a consumer to sign a HIPAA authorization if your business associate contract does not expressly permit you to do so.

FTC Act

Once you've drafted a HIPAA authorization, you can't forget the FTC Act. The FTC Act prohibits companies from engaging in deceptive or unfair acts or practices in or affecting commerce. Among other things, this means that companies must not mislead consumers about what is happening with their health information.

What does that mean, in practice? You need to do more than just meet the requirements for a HIPAA-compliant authorization. Your business must consider all of your statements to consumers to make sure that, taken together, they don't create a deceptive or misleading impression. Even if you believe your authorization meets all the elements required by the HIPAA Privacy Rule, if the information surrounding the authorization is deceptive or misleading, that's a violation of the FTC Act.

What can you do to comply with the FTC Act?

- Review your entire user interface. Don't bury key facts in links to a privacy policy, terms of use, or the HIPAA authorization. For example, if you're claiming that a consumer is providing health information only to her doctor, don't require her to click on a "patient authorization" link to learn that it is also going to be viewable by the public. And don't promise to keep information confidential in large, boldface type, but then ask the consumer in a much less prominent manner to sign an authorization that says you will share it. Evaluate the size, color and graphics of all of your disclosure statements to ensure they are clear and conspicuous.

- Take into account the various devices consumers may use to view your disclosure claims. If you are sharing consumer health information in unexpected ways, design your interface so that "scrolling" is not necessary to find that out. For example, you can't promise not to share information prominently on a webpage, only to require consumers to scroll down through several lines of a HIPAA authorization to get the full scoop.

- Tell consumers the full story before asking them to make a material decision – for example, before they decide to send or post information that may be shared publicly. Review your user interface for contradictions and get rid of them.

- The same requirements apply to paper disclosure statements. Don't give consumers a stack of papers where the top page says that their health information is going to their doctor, but another page requests permission to share that health information with a pharmaceutical firm.

For additional guidance on creating effective disclosures, check out the FTC's .com Disclosures report. If you have a health app, don't forget to consult the mobile health apps interactive tool, the FTC's best practices guidance for mobile health app developers and the OCR developer portal. And when you're telling consumers about how you share consumer health information, always remember the FTC Act as well as HIPAA.