Privacy in Retail Health Care Settings

Background

The growth in retail health care clinics make them a significant player in the $4 trillion United States health care system. Retail health care is a term used to describe two discrete models of care: 1) walk-in clinics that provide treatment from employed non-physician practitioners or 2) services that connect patients with participating online clinics. This distinction is important as it has implications in deciphering responsibilities of covered entities and business associates, respectively.

A 2022 AMA survey found that while 92 percent of people believe that privacy of their health data is a right, most are unclear about the rules relevant to their privacy. The AMA is concerned that health data are increasingly vulnerable and has called for regulations for an individual's right to control, access, and delete personal data collected about them.

Federal Privacy Laws

The Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1996, establishing a comprehensive set of standards for protecting sensitive patient health information. The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other individually identifiable patient health information (collectively defined as "protected health information" or PHI). It requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without an individual's authorization.

By law, the HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers that transmit any information in an electronic form in connection with a transaction for which the Department of Health and Human Services has adopted a standard. However, most covered entities use a variety of other persons or businesses to conduct their health care activities and functions. The HIPAA Privacy Rule allows covered entities to disclose PHI to these "business associates" only if the covered entity obtains satisfactory assurances that:

- The business associate will use the information only for the purposes for which it was engaged by the covered entity;
- The business associate will safeguard the information from misuse; and
- The business associate will help the covered entity comply with some of the covered entity's duties under the HIPAA Privacy Rule.

Covered entities may disclose PHI to a business associate only to help the covered entity accomplish its health care functions – not for the business associate's independent use or purposes, except as needed for the proper management and administration of the business associate.

The HIPAA Security Rule requires that both covered entities and business associates maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronically stored PHI.

Health care data that are not created, received, maintained, or transmitted by a covered entity or business associate are referred to as "health care adjacent data" and are not protected by the HIPAA Privacy Rule, nor subject to the

safeguards of the HIPAA Security Rule. However, the Federal Trade Commission's (FTC) Health Breach Notification (HBN) Rule requires vendors of personal health records and related entities that are not covered by HIPAA to notify individuals, the FTC, and, in some cases, the media of a breach of unsecured personally identifiable health data. In April 2024, the HBN Rule was expanded to include health apps, fitness trackers, other wearable devices, as well as online services that collect health care data, and vendors that access that data.

Challenging Retail Health Organizations' Privacy Policies & Consent Practices

In some cases, there is confusion regarding a retail health care company's HIPAA status, requiring patients to read and comprehend several documents together in order to understand their rights. Determining which organizations HIPAA applies to is a complex question, as HIPAA regulates not only the three types of covered entity (health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with a covered transaction), but also their business associates, which can be difficult for the layperson to identify.

Additionally, while retail health companies often contend that they have stringent customer privacy policies, they may still require customers to sign away some data protection rights. The consent forms that patients are asked to complete may state that after providing consent, the organization is then authorized to have access to the complete patient file, may re-disclose information contained in that file, and that the information disclosed will no longer be subject to HIPAA. While the terms may be voluntary, individuals may have no option of using the health care services if they do not agree to the terms and conditions. The fundamental problem is that once patients agree to the authorization, they agree their health information may no longer be protected by HIPAA. How retail health care companies decide to manipulate data and use it may not become apparent for many years. For this reason, it is essential that a "privacy wall" be established between the health business and non-health business of retail health care companies to eliminate sharing of identifiable PHI or re-identifiable PHI for uses not directly related to patients' medical care.

To ensure robust privacy protections, retail health care companies should be prohibited from utilizing "clickwrap" agreements, which are online agreements where the user assumes their acceptance by clicking a button or checking a box that states, "I agree." While the purpose of a clickwrap agreement is to digitally capture acceptance of a contract, they permit patients to assume assent through use of a service without actually affirmatively consenting to the data sharing. Common uses include asking website visitors to acknowledge that the website they are visiting uses cookies, installing a mobile app, or connecting to a wireless network.

It is also important that retail health care companies' Terms of Use do not require data sharing for uses not directly related to patients' medical care in order to receive care – unless required by law (e.g., reporting of infectious diseases). Operationally, this means that the Terms of Use should be distinct from the Notice of Privacy Practices, with clear indication that patients are not required to sign the latter in order to receive care. Retail health care companies should provide education on this concept to reduce patient vulnerability and achieve meaningful consent.

Several retail health care companies utilize opt-out consent, which assumes user consent unless they act to withdraw it. Opt-out consent requires users to take action to indicate non-consent, placing the responsibility on users to actively protect their data. When opt-out consent is coupled with deceptive wording, it may lead patients to agree to something without meaningful consent. Meaningful consent requires a patient to be given sufficient and understandable knowledge to make a valid decision. Requiring retail health care companies to use a default opt-in consent plus plain language is essential toward protecting patients' privacy and fostering health literacy. Once consent is given, it then becomes important to provide clear direction on how patients can withdraw consent.

Please see Council on Medical Service Report 7-A-24, Ensuring Privacy in Retail Health Care Settings for more information.