HealthInformation &theLaw
HealthInfoLaw.org
Fast Facts September 2014

What protections are applicable to patient-generated health data that is not maintained by a covered entity?

Health-related data that is created or gathered by the patient is known as "patient-generated health data" (PGHD). Patients are increasingly collecting and sharing PGHD with their providers, health plans, and patient support networks, through various e-health tools, such as mobile apps, personal health record (PHR) systems, and online patient-powered research networks (e.g., PatientsLikeMe) and registries (BioBank). PGHD may include symptoms, health history, treatment history, biometric data, patient-reported outcome measures, etc. The purpose of generating and sharing PGHD is to empower patients to play a more active role in and make more informed decisions about their health care. When PGHD is shared with providers outside a clinical setting, it also may reduce the need for office visits and emergency room use.

While ripe with potential to improve patients' health, generating and/or communicating health information using sources other than those operating in the traditional healthcare domain (e.g., health care providers, insurers, researchers, etc.) subjects this potentially sensitive information to privacy and security risks. This is because PGHD differs from traditional clinical information in two primary ways. First, patients – not providers – collect and record this data. Second, patients decide how and when to share or distribute their PGHD. These differences create separate and distinct legal protections for PGHD versus traditional clinical information, raising the issue of available privacy and security protections for PGHD once shared/uploaded by the patient onto a site such as PatientsLikeMe, 23andMe, or BioBank.

HIPAA governs healthcare providers, and the law details the safeguards that must be followed to protect the privacy and security of Protected Health Information (PHI) held in medical records. If a site or application is owned, operated, or controlled by a covered entity (e.g., provider, health insurer), as is the case when a provider offers a patient portal through its electronic health record (EHR) system, PGHD would be protected by HIPAA once it was collected by the covered entity. HIPAA, however, does not govern patients. Therefore, HIPAA does not protect PGHD uploaded by a patient to private website such as PatientsLikeMe. The privacy and security protections applicable to PGHD can only be found in state law as well as the "terms and conditions of use" agreement for any such site. Often such terms and conditions allow the selling of anonymized (or in some cases identifiable) PGHD, and the use of PGHD for research purposes.

For example, the privacy policy of health website PatientsLikeMe opens with the following: "This Privacy Policy outlines the type of information PatientsLikeMe collects from individuals who have registered to join PatientsLikeMe ("Members") and how it is shared with other third parties, including, but not limited to, pharmaceutical companies, medical device companies, non-profits, and research institutions ("Partners")." The policy then goes on to list the types of PGHD that may be "shared." The list includes the following:

- Biographical information, e.g. photograph, biography, gender, age, location (city, state and country), general notes;
- Condition/disease information, e.g. diagnosis date, first symptom, family history;
- Treatment information, e.g. treatment start dates, stop dates, dosages, side effects, treatment evaluations;
- Symptom information, e.g. severity, duration;
- Genetic information, e.g. information on individual genes and/or entire genetic scans;

Moreover, the federal Common Rule – which governs research involving human subjects – does not require informed consent from the patients for research using existing data and records. Thus, once a patient creates and shares PGHD online, the website may release or sell the information to researchers (depending on their terms of use) without the patient's consent, without violating the Common Rule or HIPAA.

The collection and sharing of PGHD holds great promise. Sharing real-world health experiences with other like patients and organizations involved in a patient's health care can improve the quality of care and open new care strategies, putting more information in the hands of patients. However, patients must review carefully the terms and conditions of use of any website to fully understand how their PGHD may or may not be shared.

See http://www.healthinfolaw.org/federal-law/HIPAA for more information on HIPAA and http://www.healthinfolaw.org/topics/63 for information on state and other federal laws related to privacy and confidentiality.

Follow us on Twitter at ***@HealthInfoLaw.***