CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of CDT for the HIT Privacy and Security Work Group Virtual Hearing

December 5, 2013

I want to thank the Health IT Privacy and Security Working Group for the opportunity to testify today. CDT has long advocated for balanced policy and technical solutions to privacy and security concerns, and we believe that the application of Big Data to health information presents several unique challenges in these areas.

Governments

The era of big data poses special considerations for governments, as they increasingly may have the technical capacity to access external data sources about the health of their citizens. For example, government health agencies may want access to health data generated by commercial gadgets and applications, such as Jawbone and Fitbit, or may enter into partnerships with such device and application developers. Care will need to be exercised in establishing these data flows to ensure that individuals are aware of what data is being collected and how it is going to be used. Likewise, governments can access commercial data broker services or even publicly available data to glean information about their constituents lifestyle choices and habits to inform decisions about benefit programs. As a general rule, governments should consider this kind of collection when it is useful for a specific goal, securely stored, and includes individual informed consent.

Most states have enacted their own laws and regulations pertaining to the use, collection and disclosure of health information outside of public health, with many focused on providing protection for sensitive information, such as disease diagnosis, mental health and substance abuse issues, and family planning activities. States each have their own reporting requirements for diseases and conditions that must be reported to the state health department and to disease-specific registries. These registries, when created and maintained by government agencies, are covered by HIPAA and the Federal Information Security Management Act (FISMA), which both require strict privacy protections for the information.

Commercial

From a commercial perspective, probably the largest privacy and security issue on the horizon is the collection and use of unregulated data from wearable devices. Individuals are increasingly sharing data on health and wellness using personal health record tools, mobile health applications, search engines and social networking sites. The health data shared by consumers using such tools can range from detailed clinical information, such as downloads from an implantable device and details about medication regimens, to data about weight, caloric intake, and exercise. Privacy questions arise due to the volume of health data that apps and devices can collect, and the sensitive information that may be used and inferred by the use of big data analytics.

Many of the challenges facing traditional health care providers in the big data era also apply to app developers and wearable device manufacturers. Notice and consent remains a problem, especially given the decreased ability to read notices on mobile device screens or via a wearable device. Security can be a critical issue for developers and device manufacturers, just as it is for clinical providers. However, because HIPAA not apply to most app developers or device manufacturers, the regulatory framework that applies to clinical providers may not apply to developers or manufacturers. This has benefits to innovation, as the complicated HIPAA framework will not apply to smaller entities that would otherwise struggle with compliance but without a clear set of legal guidelines to abide by, non-HIPAA covered developers and device manufacturers may guidance on how to appropriately and effectively protect their users' health data. Developers and device manufacturers should consider incorporating privacy and security protective measures, based on the FIPPs, into the product at early design stages. Striking the proper balance is of prime importance in this context, given the promise of health apps and devices and the sensitivity of the data that they collect.

Laws

The Privacy Act of 1974 was designed to be an overarching law to give Americans some control over personally identifiable information — including health information — collected about them by the federal government and its agencies. It gives people the right to know what information was collected about them, to see and have a copy of that information, to correct or amend that information, to exercise some (limited) control over disclosure of that information to other parties. The law applies to any federal agency that provides healthcare services for the government, such as the Veterans Administration, as well as agency contractors that are considered HIPAA-covered entities. There are exceptions for disclosure in the Act for administrative uses and public health and safety emergencies. When information is de-identified, government entities do not need patient consent to collect and use it and it is not covered by the Privacy Act; however, many federal and state agencies choose to guide privacy and disclosure for de-identified data on ethical guidelines that review the implications of revealing data, regardless of law or policy.

As the law currently stands, American citizens and permanent residents have a right to access, inspect and potentially amend health records maintained by the government. This may be accomplished through HIPAA, the 1974 Privacy Act, or both depending on the structure of the government program. The Privacy Act also prohibits government agency disclosure of records to third parties unless the agency has obtained the data subject's consent. However, one concern with current legal regulation of government use of health data is that non-citizens' only means of access and amendment is HIPAA, which arguably provides less privacy protections that the Privacy Act.

FIPs

Invoking the concept of big data may appear to dramatically alter our traditional understanding of privacy of information; after all, the defining characteristics of big data, volume, velocity, and variety, represent the capacity of machines to process information in a novel way. The Fair Information Practice Principles (FIPPs), however, provides a framework that has managed to stand the test of time and technology time and again. The framework is flexible yet structured, and informs most modern privacy regimes inside and outside healthcare. CDT believes the FIPPs offer governments seeking to use big data with regard to health information a strong, standardized structure that promotes responsible and efficient use of data while allowing for innovations in analytics and application.

The foundational principle of openness or transparency is perhaps the most important component of the FIPPs for all entities using big data. Transparency should guide any health data collection and use regime, from the first point of contact with data to any subsequent use. Information about data practices can be done in different ways. It can be provided in a standalone legal notice that provides complete information about information practices, and it can be messaged contextually to a user in a way that the user is likely to notice and understand. Both play an important role. Today, unfortunately, privacy policies tend to be inscrutable, risk-averse compliance obligations, in which the primary goal is to avoid making an incorrect statement that could serve as the basis for FTC liability. Thus, notices tend to be overly broad and vague. It's particularly important to get notice right when using data collection methods that are less visible, such as collection from mobile health applications that typically involve individuals inputting their own health data. To mitigate the opacity of this collection, entities are obligated to make full disclosure to those they collect from about data practices via contextual notice. Also, when entities will be the beneficiary of patient data, they should require partner doctors and other healthcare entities provide information to patients on how and why their data will be used.

Any collection and use of health data, even when de-identified, must be detailed in a statement accessible to individuals in one place. Entities using health data should provide notice to individuals when they might consider the intended usage or collection to be unexpected or objectionable and this should be done at a time that is relevant. Contextual notice, or just-in-time notice, is a critical component of meeting an individual's collection and sharing expectations. Fundamentally, it should be clear to a consumer using a health app or wearable device when data is being collected, what types of data are being collected, what it is used for (by the entity and by any partners or vendors it may have), what secondary uses of the data are contemplated, how long data is retained, and what security measures are put into place in order to protect the data.

Communicating those practices effectively is of critical importance for governments, health app developers and providers. A high percentage of Americans are "somewhat" or "deeply" concerned about the privacy and security of their medical records, according to a survey released by OCR. Promoting consumer trust through transparency is essential not just to improve privacy but also to promote the adoption of services and important new technological tools. Without that trust, governments, industry, and patients as a whole will be unable to harness big data's potential benefits.