September 9th, 2017

**Statement for the National Committee on Vital and Health Statistics**
As requested by the Subcommittee on Privacy, Confidentiality and Security
Prepared by Fatemeh Khatibloo, Principal Analyst, Forrester Research

## Introduction

Healthcare data is widely understood to be highly sensitive and deeply personal. This data, more than nearly any other, tells a person's life story from childhood to old age. It captures an individual's traumas and successes, and it is highly predictive of future behaviors and attitudes. In many ways, our health information knows us better than we know ourselves.

Currently, the most significant protections of health information in the United States fall under the HIPAA regulation[1]. However, HIPAA's purview is limited and, I believe, insufficient to protect emerging types and uses of health data. As individuals increasingly wear, use, ingest, and interact with sensor-laden devices (aka "the internet of things") they create data that should rightfully be considered "sensitive health data," but this information isn't defined as protected health information (PHI) today.

As an example, let us consider sleep monitoring data. Today, the collection of this data can take many forms: "prescribed" tracking by a physician to help manage illnesses like depression or COPD; "self-quantified" tracking with apps and wearables to monitor one's own physical and mental wellness; and "incidental passive" collection, where a user may connect her phone to a Bluetooth-enabled alarm clock every night. Although the method of data collection may differ, the nature of the data in all three cases is sensitive and a potential marker of health conditions. However, these three kinds of data are protected very differently – and some not at all.

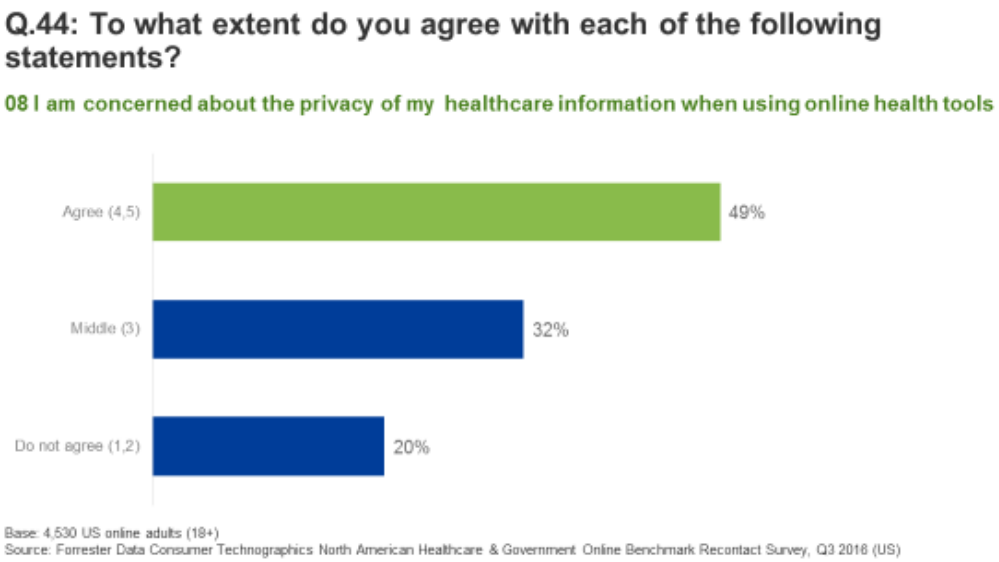
## The consumer/patient perspective:

In our research, we found that 49% of US online adults are concerned about the privacy of their healthcare information when using online health tools, but the majority of these individuals don't realize there is a legal difference between their medical doctor's website and, say, an app for monitoring their blood glucose levels[2]. (Figure 1)

In fact, three-quarter of these individuals believe that health-related apps *should be* governed by HIPAA regulations. This matters, because 24% of US adults actively want to share wellness data from a wearable device with their primary care physician, fully 55% of them are comfortable with the idea of doing so.

However, fewer than one-quarter are comfortable with that data being shared with their health insurer (22%), pharmacist (20%) federal agencies like NIH (11%) or even the maker of the device (6%)! In other words, the average US adult does not expect wellness data from wearables or mobile apps to be sold – as is as already happening -- for purposes of behavioral analytics and ad targeting. This gap between consumer perception and the reality of non-protected health data use will only continue to widen as more consumer devices come to market.

**Figure 1:**




**We must future-proof the protection of citizens' health data.**

In the future, the need to define and protect sensitive health- and wellness-related data will be even more crucial, because the use cases for these kinds of data are exploding. For example:

- Employer-recommended "health improvement apps" can already predict the number of female employees who are likely to become pregnant within a year. Without guardrails, this insight could result in a firm changing its hiring practices or benefits.

- Artificial intelligence and deep learning technologies use "big data" to make decisions in a relative black box. Without restrictions on the use of certain kinds of health data – from health and wellness purchase behavior to online research about particular medical conditions -- industries from insurance to pharma could make business decisions that are discriminatory, or otherwise socially damaging[3].

- "Intelligent agents" – like Amazon Alexa and Apple Siri -- are increasingly being used by individuals to simplify their lives and communications. Consumers already say they want to be able to make doctor's appointments using their calendar-connected Echo, or have their iPhone read them a transcribed message from their health practitioner. While some onus falls on the individual to use common sense, we believe it's also crucial for the providers of these IAs to comply with privacy and security requirements to protect potentially sensitive PHI.

- DNA testing services, like ancestry.com and 23andme, can offer powerful insights for individuals – about one-third of the individuals in ConsumerVoices expressed interest in using them to learn about their genetic history and potential health risks. Since none of this data is currently protected as PHI, these services could change their terms of use at any time, to more easily monetize the data they've collected. While the risk to individuals may seem minimal if the data has been stripped of personally identifiable information, these datasets are so rich that it would not take much to reidentify a significant number of users.

**Conclusion**

The proliferation of data about health and wellness is, fundamentally, a great thing for individuals and society. Researchers, clinicians, and public health organizations can use this data to create tools for high-risk individuals; to get better insight into clinical efficacy of medical treatments; and to improve healthcare for all.

However, there is also tremendous risk if the collection and use of these data sources goes unchecked.

We believe that, in order to maximize its potential for society, without risking individual privacy and security, the spirit of a healthcare data protection regulation should:

1. expand the definition of PHI to include wellness and behavior data;
2. further define specific classes of PHI, based on their potential risk and sensitivity;
3. require proportionally appropriate protection and handling of each class of data
4. limit the use of sensitive data, irrespective of provider or practitioner;
5. subject all firms collecting health data to the same privacy and security standards;
6. provide meaningful control of healthcare data to the individual

Sincerely,

Fatemeh Khatibloo
Principal Analyst, Forrester Research
fkhatibloo@forrester.com

[1] There are some protections under the Federal Trade Commission's Section 8 "unfair and deceptive business practices" rules, but these are not written specifically to protect healthcare data.

[2] We also found that nearly half of Forrester Research's ConsumerVoices community believes that cash payments to a non-medical wellness provider are covered by HIPAA.

[3] Consider Google's "Flu Trends," for example. The algorithm predicted outbreaks incorrectly due to noise in the data it ingested; while there was no harm at the time, a pharmaceutical company might easily have used that data to distribute vaccine to areas that did not, in fact, need the extra doses.