How smartphone apps can—and should—protect users' health info

JAN 10, 2022

Tanya Albert Henry
Contributing News Writer

From tracking diet, sleep, mood, blood pressure and more, health apps have become a huge repository of patient's personal health information.

But unlike other health information, HIPAA doesn't protect this sensitive information. These apps weren't a reality when HIPAA was created in 1996. And, while the California Consumer Privacy Act has attempted to address some patient privacy concerns, there's nothing at the federal level that has established comprehensive data privacy rules.

Based on the AMA's Privacy Principles (PDF), a recently released AMA-developed guide makes the business case for why developers should be designing their apps with privacy at the forefront. The AMA also is offering a road map on how to implement important privacy protections for patients who are sharing information such as their height, weight, exercise routines, eating habits and glucose readings.

"This kind of information may not seem like medical data when the user was entering it into the app, but as a picture of a person's health begins to evolve from the information submitted, it starts to look more and more like what be found in a medical record. A marketer, an insurance company, or an employer could have access to that information and use it in ways that the consumer may not have imagined," according to the guide, "Privacy is good business: A case for privacy by design in app development" (PDF), which is part of the AMA health data privacy framework.

Health insurers could use such data for health scoring and pricing; employers could factor the information into hiring, firing and promotion decisions. Big data can potentially target educational, credit, health care and employment opportunities to historically marginalized communities and those with low income—or it can be used to withhold such opportunities from such communities. Potential inaccuracies and biases in the data can lead to additional detrimental effects.

The guide tells app developers and physicians that “apps can differentiate themselves by building trust with consumers that their personal private data will not be shared with unknown or unwanted parties.”

The role physicians can play

Patients sometimes ask their physicians for recommendations about apps and a recent Pew Survey found that 90% of respondents said they preferred apps that their physician had pre-approved.

The AMA encourages the physician community to ask app developers whether they are following the AMA principles and to encourage their patients to ask those questions of apps as well.

The AMA-created checklist for app developers looks at privacy policy from several different angles, including a specific focus on how privacy intersects with health equity. The document also includes actions developers can take to implement the principles, some of which are outlined below.

Individual rights

Individuals have the right to control how entities access, use process and disclose their data, including secondary uses—and beyond. For example, systems need to provide configurable setting functions that allow a user to define which entities may have access to their personal data.

Individuals have a right to direct entities not to sell or otherwise share data about them. For example, the default app setting should be to deny sale of a user’s personal data.

Individuals and entities should be able to protect and securely share pieces of information on a granular, as opposed to a document, level. For example, systems should provide a configurable setting for each category of personal information that could potentially be shared.

Equity

Individuals should be protected from discrimination, stigmatization, discriminatory profiling and exploitation occurring during collection and processing of data, and resulting from use and sharing of data, with particular attention paid to historically marginalized racial and ethnic groups. App developers should have practices in place to protect users from sharing that would lead to such discrimination and profiling.

Law enforcement agencies requesting medical information should be given access only with a court order and if the law enforcement entity has shown by clear and convincing evidence that the information sought is necessary to a specific, legitimate law enforcement inquiry. App developers should take steps to ensure that such information is only released to law enforcement agencies in accordance with these processes.

Employers and insurers should be barred from unconsented access to identifiable medical information to assure that knowledge of sensitive facts does not form the basis of adverse decisions against individuals. App developers should prevent information from being shared with employers and insurers absent a user's specific consent and direction.

Entity responsibility

All entities that maintain an individual's health information should have an obligation or "duty of loyalty" to the individual, including the duty to maintain the confidentiality of that information. App developers should implement policies and procedures that protect the user above all other considerations.

Additionally, app developers should disclose to individuals exactly what data it is collecting and the purpose for its collection and should only collect the minimum amount of information needed for a particular purpose, in accordance with regulation or federal guidance.