College of Healthcare Information Management Executives

May 31, 2019

The Honorable Joseph J. Simons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Simons:

The College of Healthcare Information Management Executives (CHIME) is pleased to provide comments for the Federal Trade Commission's (FTC) hearings on "Competition and Consumer Protection in the 21st Century." In an era where more healthcare data is flowing, our members have a keen interest in ensuring that there is full transparency for patients concerning how their data will be used once it's released by a healthcare provider.

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief innovation officers, chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With more than 2,900 members in 51 countries and over 150 healthcare IT business partners, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate the effective use of information management to improve the health and healthcare in the communities they serve.

The FTC describes its work as intended to protect consumers and promote competition through vigorous enforcement, education, advocacy, and policy work, and by anticipating and responding to changes in the marketplace. As the nation's primary consumer protection agency, the FTC has a broad mandate to protect consumers from unfair or deceptive acts or practices in the marketplace, and to educate consumers and businesses about their rights and responsibilities. We appreciate the Commission's attention to the topic of privacy and believe it is an imperative that third parties with whom patients have shared their healthcare data are appropriately and adequately regulated. Daily headlines indicate citizens have little idea how their healthcare data is being used by third parties where they either intentionally shared their data or where it was shared without their knowledge. These incidents speak to the need for greater oversight. We are particularly concerned that as more citizens share their healthcare data with third parties, that data could be mishandled. Given the volume of data we are talking about, this is cause for concern.

Earlier this year, the Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC) released two rules intended to improve patient access to their data and implement certain provisions contained in the 21st Century Cures Act aimed at achieving this goal. Specifically, these rules call for advancing patient access to their data using application programming interfaces (APIs). CMS requires providers facilitate access to patient data at their request via APIs and ONC's rules both establish data blocking requirements that do not allow certain actors from inhibiting the flow of patient information except in very limited situations, and requirements for certified electronic health record vendor (EHR) products around API capabilities. Our members strongly support patient access to their medical data. However, they have significant privacy and security concerns associated with the transfer of this data to third parties. We are very worried that patients are unaware of how their data is being used once it is released and, in some cases, may be under the false impression that it is still

safeguarded under the Health Insurance Portability and Accountability Act (HIPAA). We outlined these concerns in detail our recent letter to CMS and ONC.

Given the speed with which CMS and ONC are moving to further facilitate patient access to their data via APIs, we worry that appropriate oversight must be in place to govern how patient data is not just accessed by third parties but also how it is being used. In short, patients must be able to trust the apps they are sending their data to and have full awareness of how their data will be used. Although we raise these concerns in our response to ONC and CMS, we must stress the dire lack of consumer and patient trust in apps which could be created if their data is misused. Further, once data is released, while data sharing can be revoked, there is no way to walk back what has already been shared. Moreover, the ability to monetize data is only growing. As aptly described in a recent article, "Personal data is the oil of the 21st century, a resource worth billions to those who can most effectively extract and refine it. American companies alone are expected to spend close to $20 billion by the end of 2018 to acquire and process consumer data, according to the Interactive Advertising Bureau."[1] Adding more healthcare data to the existing data streams available for purchase without adequate safeguards will erase consumer trust and create more privacy challenges.

Our members take seriously their responsibility to safeguard and keep private patient information as required by HIPAA. Once a patient's medical record is downloaded via an open API to an app at the patient's request, that information is no longer protected by HIPAA unless the app is sponsored by a HIPAA covered entity. Worrisome is that patients may not understand: 1) that HIPAA no longer applies; and 2) how the app intends to use their data. The terms and conditions may be lengthy, and patients may skip over them in favor of convenience. The terms and conditions also may or may not specify that the app developer could re-use or sell their data – including sensitive data – to others like third party data brokers. Our members are concerned that one bad actor could destroy consumer and patient trust in healthcare apps, dismantling efforts to further interoperability and improve patient access to their information. Our members believe more education is needed so that patients are fully aware of the benefits and risks associated with their data being reused without their knowledge.

Additionally, the ONC proposed rule does not, in its current form, appear to include those technology companies that manage apps, nor does it cover the third-party apps themselves under proposed data blocking policies as among the actors who must comply with these policies. Therefore, unless these policies are changed, a big chunk of the healthcare sector like providers and EHR vendors will have to abide by one set of rules governing promoting the sharing of patient information, and third-party apps and those managing the app ecosystem will not. This will create an unlevel playing field and further perpetuate the notion that healthcare apps are the Wild West.

In addition to what CMS and ONC have proposed, the Office for Civil Rights (OCR) is considering changes to HIPAA as they contemplate the current data-rich environment, patients' needs for their data, and the need to foster better care coordination. Recently, the agency published a series of questions concerning a patient's right to access their information making it clear in one answer (Q/A 4) that, "The HIPAA Rules do not impose any restrictions on how an individual or the individual's designee, such as an app, may use the health information that has been disclosed pursuant to the individual's right of access."[2]

As smart phones, social media and other apps become integral parts of everyday life, the definition of "healthcare data" is changing. Companies tracking location, payments, or both can easily discern if a patient is sick, how sick the patient is, or what type of illness the patient has. For example, a cancer patient drives to her specialist and has an hour-long appointment. She brings her phone, and in the waiting room, she may open her Facebook, Instagram and web search apps. All three apps collect location data, and all three apps can collectively know she is seeing a cancer specialist. That data is then aggregated and sold to third-party data brokers, making her extremely sensitive illness known to faceless companies and people. A recent story in the *New York Times* outlined just how much data apps are collecting – some of it health – and demonstrated how easy it was to ascertain the whereabouts of citizens using location tracking data,

[1] As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants, New York Times, December 18, 2018.
[2] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hippa-access-right-health-apps-apis/index.html

including visits to a family planning clinic and a dermatologist's office.[3] The article also noted just how lucrative the location data is – estimated to be $21 billion in 2018.

Considering the concerns outlined above, we believe a prudent approach would require an "informed consent" by apps seeking access to healthcare data at a patient's request that clearly and unambiguously informs a patient how their data will be used. The app developer should also address questions with the purpose of further educating patients on whether they truly want to trust this third party or not. For instance:

- Do you sell identifiable information?
- If yes, is it used only for research?
- Do you use the data for marketing?

Considering these concerns, we recommend the FTC:

1. Work closely with CMS, ONC and OCR to ensure that appropriate safeguards and adequate oversight of third-party apps occur, especially relative to the new requirements for providers to facilitate access to patient data via APIs;
2. Host a workshop devoted exclusively to data sharing involving healthcare data.

We appreciate the opportunity to share our perspective with the Commission and welcome the chance to discuss these issues in greater depth. Should you have any questions, please contact Mari Savickis, vice president of federal affairs, at msavickis@chimecentral.org.

Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

Shafiq Rab, M.D., CHCIO
Chair, CHIME Board of Trustees
SVP & CIO
Rush University Medical Health

[3] Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, New York Times, December 10, 2018.