October 21, 2022

Submitted via the Federal eRulemaking Portal: http://www.regulations.gov

The Honorable Lina M. Khan
Chairwoman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

RE: Trade Regulation Rule on Commercial Surveillance and Data Security; Advance Notice of Proposed Rulemaking; Request for Public Comment [FTC-2022-0053]

Dear Chairwoman Khan:

The College of Healthcare Information Management Executives (CHIME) respectfully submits our comments to the Federal Trade Commission (FTC or Commission) in response to the "Advance Notice of Proposed Rulemaking" (ANPR) regarding the *Trade Regulation Rule on Commercial Surveillance and Data Security*, as published in the *Federal Register* on August 22, 2022 (Vol. 87, No. 161).

Background

CHIME is an executive organization dedicated to serving chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. With over 5,000 members, CHIME provides a highly interactive, trusted environment enabling senior professional and industry leaders to collaborate; exchange best practices; address professional development needs; and advocate for the effective use of information management to improve the health and healthcare in the communities they serve.

Key Recommendations

In our comments, CHIME provides responses to address the specific questions included in the ANPR – *Trade Regulation Rule on Commercial Surveillance and Data Security*.[1] We are broadly supportive and appreciative of the FTC's approach to implement new trade regulation rules concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. Additionally, we offer feedback and recommendations to constructively improve the advance notice of proposed rulemaking.

By creating this opportunity for stakeholders to engage – especially those that prioritize partners and communities served and impacted throughout the policy development and implementation process, we believe invaluable input will be garnered. We thank the Commission for encouraging input from a wide variety of voices – including healthcare providers – on the questions listed in this ANPR.

Detailed Recommendations

CHIME appreciates the FTC's request for public comment on the prevalence of commercial surveillance and data security practices that harm consumers. Our members have and continue to support the Commission's ongoing focus on the commercialization of consumer data – in particular, healthcare data – which is now an even more valuable commodity, with mobile applications that use this data continuing to multiply. In 2020,

[1] United States, Federal Trade Commission. Trade Regulation Rule on Commercial Surveillance and Data Security. Vol. 87 Fed. Reg. 51273. Published August 22, 2022. https://www.federalregister.gov/documents/2022/08/22/2022-17752/traderegulation-rule-on-commercial-surveillance-and-data-security

CHIME advocated directly for the expansion of the personal health record definition and for the utilization of the FTC enforcement authority in comments to the Health Breach Notification Regulatory Review; request for public comment.

CHIME has consistently supported the FTC's efforts to protect consumer's health information. Specifically, we applauded the Commission's Policy Statement *On Breaches by Health Apps and Other Connected Devices* issued on September 15, 2021.[1] This Policy Statement provided much needed clarity and recognition of the FTC's authority under the Health Breach Notification Rule[2] ("the Rule") as a result of the proliferation of apps and connected devices that capture sensitive health data. It further provided that under the Rule's requirements, vendors of personal health records ("PHR") and PHR-related entities must notify U.S. consumers and the FTC, and, in some cases, the media, if there has been a breach of unsecured identifiable health information, or face civil penalties for violations.

Subsequently, CHIME was extremely encouraged that the FTC stated that, "although the Rule was issued more than a decade ago, the explosion in health apps and connected devices makes its requirements with respect to them more important than ever." Furthermore, we were and remain encouraged by the FTC communicating their strong intent to hold non- Health Information and Privacy Protection (HIPAA) covered third-parties responsible under the Rule's requirements.

A recent estimate by IQVIA Institute for Human Data Science[3] pegged the number of health-related apps at 350,000. Given the explosion in mobile apps and data aggregation practices, it entirely possible that the amount of health data held by entities who are not required to comply with the HIPAA exceeds the data held by those who are HIPAA covered entities, certainly a concerning development.

As one of only a handful of federal privacy laws protecting consumers' health information, the Rule plays a vital role in holding companies accountable for how they disclose consumers' sensitive health information. "Since the FTC first issued the Rule more than a decade ago, consumers have turned to apps, wearables, and other technologies for health advice, information, and tracking. It is imperative that the FTC's enforcement of its Rule keep pace with changing technology."[4] **CHIME strongly agrees with these statements.**

The Commission is inviting comment on whether it should implement new trade regulation rules or other regulatory alternatives concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. **While CHIME is broadly supportive of new trade regulation rules to utilize the FTC's existing authority to protect consumers – we are strongly encouraging the FTC to push further into this space by utilizing and enforcing the clear, concise and existing authority under the Health Breach Notification Rule to hold non-HIPAA covered third-parties (i.e., vendors of PHR and PHR-related entities) responsible when they illegally disclose – intentionally or not – covered information.**

The Commission has already reminded "entities offering services covered by the Rule that a "breach" is not limited to cybersecurity intrusions or nefarious behavior. Incidents of unauthorized access, including sharing of covered information without an individual's authorization, triggers notification obligations under the Rule. As many Americans turn to apps and other technologies to track diseases, diagnoses, treatment, medications, fitness, fertility, sleep, mental health, diet, and other vital areas, this Rule is more important than ever. Firms offering these services should take appropriate care to secure and protect consumer data. ***The Commission intends to bring actions to enforce the Rule consistent with this Policy Statement [emphasis added]***. Violations of the Rule face civil penalties of $43,792 per violation per day."[2]

Consumers as patients can use both mobile medical apps and mobile apps to manage their own health and wellness, such as to monitor their caloric intake for healthy weight maintenance, while other apps are created to help

[1] Federal Trade Commission. (September 15, 2021). Statement of the Commission: On Breaches by Health Apps and Other Connected Devices [Policy Statement]. https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf

[2] Federal Trade Commission's Health Breach Notification Rule, 16 C.F.R. Part 318

[3] Murray Aitken & Deanna Nass. (2021, July). Digital Health Trends 2021: Innovation, Evidence, Regulation, And Adoption. In https://www.iqvia.com/.

[4] *Complying with FTC's Health Breach Notification Rule*. (2022, January 28). Federal Trade Commission. Retrieved October 12, 2022, from https://www.ftc.gov/business-guidance/resources/complying-ftcs-health-breach-notification-rule-0

healthcare providers improve and facilitate patient care.[5] CHIME members understand that the "privacy protections for health information shared outside of HIPAA (e.g., when an individual downloads information into a medical application marketed to consumers), [inherently means that there is a] "possibility of consumer technology companies' taking advantage of patients to sell and misuse data for the companies' commercial gain."[61] Furthermore, the FTC has stated that "many companies that collect people's health information – whether it's a fitness tracker, a diet app, a connected blood pressure cuff, or something else – aren't covered by HIPAA. Does that mean this sensitive health information doesn't have any legal protections? Not at all."[4]

The FTC acknowledged – over one year ago – in the Policy Statement that the Commission "has never enforced the Rule, and many appear to misunderstand its requirements." Therefore, in issuing the Policy Statement, it served "to clarify the scope of the Rule, and place entities on notice of their ongoing obligation to come clean about breaches." **CHIME stated in response, and still believes, that actions from the FTC will make a consumer's data more secure and help ensure that those entities who have a breach of this crucial private data are held accountable. Not only does it hold bad and unsecure actors accountable, but it also creates a disincentive that urges all businesses with PHR and PHR-related entities to strengthen their data security practices.**

CHIME appreciates that the FTC has thoroughly clarified via numerous guidance documents and the Policy Statement that the Rule does not apply to HIPAA-covered entities (e.g., hospitals and doctor's offices). HIPAA-covered entities (CEs) and those that act only as a HIPAA business associate (BA) have existing legal responsibilities that are in the Health and Human Services (HHS) Breach Notification Rule.[8]

While we are encouraged by this ANPR, CHIME members would appreciate clarification regarding the intersection of the potential future proposed rule regarding "Commercial Surveillance and Data Security", the FTC's existing authority under the Health Breach Notification Rule, and data held by HIPAA covered entities (CEs) which does not fall under HIPAA (i.e. de-identified data). The FTC has also had authority under "the Rule" for over a decade, and despite authority to hold vendors of PHR and PHR-related entities accountable, there has been an apparent need for ongoing education and clarity. Therefore, we can only assume that a tremendous amount of additional clarity will be required – especially for those that fall under a potential new regulation, the FTC's Health Breach Notification Rule, and under the HIPAA law.

A business is a vendor of personal health records if it "offers or maintains a personal health record." A personal health record is defined as an electronic record of "identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual." FTC offers this specific example: "[…] if you develop a health app that collects information from consumers and can sync with a consumer's fitness tracker, you're probably a vendor of personal health records. You're not a vendor of personal health records if you're covered by HIPAA."[4] **The Rule requires that notice be provided when there has been an unauthorized acquisition of unsecured PHR identifiable health information.** The Commission has stated that unauthorized acquisition is defined as "if health information that you maintain or use is acquired by someone else without the affected person's approval, it's an unauthorized acquisition under the Rule." **CHIME strongly urges the FTC to utilize its existing authority to protect American consumers and patients who are often unaware of how their data is being used, and in some cases, may be under the false impression that it is still safeguarded under HIPAA. Clear, transparent communication to consumers about how their data is being used, monetized, and secured will be critical in future rulemaking.** Our members take the protection of their patients' healthcare data as not only a legal obligation, but their mission. Patient data safety is crucial for maintaining trust in the patient-provider relationship; ensuring that patient data remains safe even when they are outside of the four walls of the hospital or other healthcare setting only helps strengthen that bond. The FTC "placed entities on notice of their ongoing obligation to come clean about breaches" over a year ago. **CHIME believes it is time for vendors of PHR and PHR-related entities with lax data security – and sometimes blatant disregard of the law**

[5] *Device Software Functions Including Mobile Medical Applications*. (2022, September 29). U.S. Food And Drug Administration. Retrieved October 12, 2022, from https://www.fda.gov/medical-devices/digital-health-center-excellence/device-software-functions-including-mobilemedical-applications

[6] *Breach Notification Rule*. (2021, June 28). HHS.gov. Retrieved October 12, 2022, from https://www.hhs.gov/hipaa/for-professionals/breachnotification/index.html

– to receive these notices and penalties under the existing authority provided to the Commission under the Rule.

The FTC has acknowledged that "health apps and other connected devices that collect personal health data are not only mainstream – and have increased in use during the pandemic – but are targets ripe for scammers and other cyber hacks. Yet, there are still too few privacy protections for these apps."[7] Our members believe more education is needed so that consumers are fully aware of the benefits and risks associated with their data being held without adequate security practices or sold without their knowledge.

CHIME believes that there is more that can be done before a consumer's data is sold or a breach happens, and we encourage the FTC to enforce real-world and stringent privacy and security protections on companies to better protect consumer data. That includes making sure consumers understand what they are agreeing to prior to using a company's technology. Additionally, CHIME believes the following questions should be considered in any future rulemaking:

1) Do you sell or monetize from consumer information?
2) How is consumer information that is sold used (i.e., marketing, used only for research)?
3) What is your documented consumer consent process?
4) How long do you store consumer data; where is it stored; what are your security practices (e.g., cyber hygiene); and do you securely destroy data – if so, how and when?
    a. Additionally, we believe this information should be available on the FTC website for consumers to search before and after purchasing a product or service.

CHIME looks forward to supporting the FTC in its efforts to implement new policies to protect consumers. We have long stood as staunch supporters of all efforts in both Congress and the federal agencies that ensure patient data stays secure and is never compromised in a way that could jeopardize patient care or trust in the American healthcare system. CHIME will continue to support new and continued efforts to build on these important policies and in general, welcome FTC action. We continue to draw awareness to these issues and launched the Think Before You Click campaign earlier this year.

Conclusion

CHIME appreciates the FTC's issuance of this important ANPR on ways to implement new trade regulation rules concerning the ways in which companies collect, aggregate, protect, use, analyze, and retain consumer data, as well as transfer, share, sell, or otherwise monetize that data in ways that are unfair or deceptive. We are especially thankful to the Commission for encouraging input from a wide variety of voices – including healthcare providers – on the questions listed in the ANPR. CHIME believes that adding more healthcare data to the existing data streams available for purchase without adequate and enforced safeguards will erode consumer trust and create more privacy challenges.

In closing, we would like to thank the FTC for providing the opportunity to comment on this important Advance Notice of Proposed Rulemaking (ANPR). Should you have any questions or if we can be of assistance, please contact Chelsea Arnone, Director, Federal Affairs at carnone@chimecentral.org.

Sincerely,

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

[7] *FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule*. (2022d, March 4). Federal Trade Commission. Retrieved October 18, 2022, from https://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-warns-health-appsconnected-device-companies-comply-health-breach-notification-rule