August 20, 2020

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

Dear Chairman Simons:

On behalf of the Healthcare Information and Management Systems Society (HIMSS) and the Personal Connected Health Alliance (PCHAlliance), we are pleased to provide written comments in response to the Federal Trade Commission's (FTC's) Regulatory Review; Request for Public Comment on its Health Breach Notification Rule. We appreciate the opportunity to leverage our members' expertise in offering feedback on this Rule and look forward to ensuring that individuals' personally identifiable health data is protected, and that the appropriate actions are taken when a breach of unsecured information occurs.

HIMSS is a global advisor and thought leader supporting the transformation of the health ecosystem through information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology. Through our innovation engine, HIMSS delivers key insights, education and engaging events to healthcare providers, governments and market suppliers, ensuring they have the right information at the point of decision. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia Pacific. Our members include more than 80,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations.

PCHAlliance, a membership-based HIMSS Innovation Company, accelerates technical, business and social strategies necessary to advance personal connected health and is committed to improving health behaviors and chronic disease management via connected health technologies. PCHAlliance is working to advance patient/consumer-centered health, wellness and disease prevention. The Alliance mobilizes a coalition of stakeholders to realize the full potential of personal connected health. PCHAlliance members are a vibrant ecosystem of technology and life sciences industry icons and innovative, early stage companies along with governments, academic institutions, and associations from around the world.

HIMSS and PCHAlliance see this Rule as a critical piece in a broader, overarching health data privacy regulatory system. Review of this Rule, in conjunction with the updates underway to the Health Insurance Portability and Accountability Act (HIPAA) of 1996, are instrumental in how health information privacy is to be regulated at the federal

level, and how the security of that information is perceived by the consumer and healthcare ecosystem at large.

To encourage widespread adoption, acceptance, and trust of new, innovative technologies that support information between patients and providers, FTC should work with other federal agencies to foster the development of robust, up-to-date, privacy and security standards and frameworks.

For example, FTC should maintain its relationship with the Department of Health and Human Services (HHS) that was established in the Health Information Technology for Economic and Clinical Health (HITECH) Act, part of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), and expanded upon in the 21st Century Cures Act (PL 114-255). The resulting work has created a framework for patients to have private and secure access to their personal health data and encouraged the development of analytics tools that engage individuals to direct their own healthcare, and inhibits information blocking in the name of seamless care delivery.

Most recently, the interoperability regulations currently being implemented by the Office of the National Coordinator for Health IT (ONC) and the Centers for Medicare & Medicaid Services (CMS) have set a course for a healthcare paradigm that takes full advantage of the promise of standards-based application programming interface (API) technology, and capitalizes on the inherent opportunities for innovation while making allowances for encouraging new market entrants.

These concepts, as well as an infusion of existing and new innovative technologies, need to be part of the discussion around updates to the FTC Rule. With these factors in mind, HIMSS and PCHAlliance offer the following recommendations on this regulatory review and request for public comment:

Ensure this Rule is Retained and Working in Concert with Other Privacy and Security Regulations

HIMSS and PCHAlliance support the continuing need for the Rule and find that, given the widespread adoption and development of health information technologies in the past decade, the need for the Rule is more relevant than ever. Any updates need to reflect forward-thinking guidance that is consistent with advances in digital health. For example, as the ONC and CMS interoperability Rules place greater emphasis on APIs, an increasing number of organizations will be subject to the Rule's requirements.

We believe, as FTC acknowledges in the regulatory review, more consumer-facing technologies will require FTC to appropriately address newer and more innovative technologies, that as consumers turn towards direct-to-consumer technologies for health information and services (such as mobile health applications, virtual assistants, and platforms' health tools), more companies may fall under the scope of the Rule. FTC must provide clarity about how the Rule translates and applies to technologies today and in the intervening years before the Rule is reviewed again. Regulatory certainty from FTC about what actions and entities are covered by the Rule will help guide market-driven development of innovation in patient-facing API technologies.

Updated Terminology for Today's Environment
At the most fundamental level, we recommend FTC review terminology on privacy and security in an effort to better align with terminology being used by other federal agencies and across the healthcare market. HIMSS and PCHAlliance stress that updated terminology will provide greater clarity and eliminate any confusion for new market entrants and existing stakeholders in this area. Otherwise, the existing terminology cannot be retrofitted to today's environment in its current form.

We recommend the following terms and definitions be revisited and modified to better align with current definitions:

- *Personal Health Records (PHRs)*

Since the time this Rule went into effect, the health IT world has introduced a vast amount of new terminologies that providers, business entities, and consumers are regularly using today. Related to this Rule, we emphasize that the term "personal health record" software should be replaced, as many individuals are using websites, web applications, and mobile applications, including those that relate to wellness and desktop applications for one's own personal health data. As such, we recommend that the terminology and definitions in this Rule be expanded to reflect the growth in the industry.

- *PHR Identifiable Health Information*

This definition relates to a PHR entity that offers products or services through the website of a vendor of PHRs, through the website of a HIPAA-covered entity that offers individuals PHRs, accesses information in a PHR, or sends information to a PHR. Since PHRs have been replaced by other solutions, the definition needs to be updated to, instead, accommodate entities that may provide a mobile app, website, or desktop application that allows an individual to access his or her own personal health data. FTC should ensure that the data regulated by this Rule is personal health data, regardless of whether such data is transacted by way of a mobile app, website, desktop application, API, or otherwise.

In addition, further alignment of FTC terminology with the work of ONC and CMS may be warranted. ONC's Interoperability and Information Blocking Final Regulation advances interoperability and supports the access, exchange, and use of electronic health information (EHI), while minimizing the "special effort" necessary to access, exchange, and use EHI via certified API technology. Ensuring clarity and alignment of these definitions with FTC's definition of PHR identifiable health information is paramount.

Moreover, there is also an opportunity for FTC to align this definition of personal health data with the HIPAA Definition of Protected Health Information. Harmonization with HIPAA is critical such that there should be efforts in place or in development, to avoid bifurcated environments. The scenario in which an individual's provider could benefit from the information originating from a non-HIPAA protected source is not unrealistic. The seamless passage of that information is essential for their own health, as well as future use of the information. HIMSS and PCHAlliance continue to emphasize the importance of creating a healthcare ecosystem that reinforces the secure access to,

exchange of, and use of electronic health information. This includes building upon these existing protections and helping to ensure patient privacy and the efficient sharing of key health information of both HIPAA-regulated and non-HIPAA regulated data, to advance high quality, value-based care.

Mechanism and Timeline for Reporting a Known Data Breach
HIMSS and PCHAlliance recommend that FTC's review include an update of the mechanism and timeline for reporting a breach. We stress that a more user-friendly approach would be more effective and efficient in terms of notifying the agency without any unnecessary or potentially avoidable delays. To start, we suggest that FTC create an easily accessible, user-friendly, interactive form on its website to directly report breaches and other suspected violations of the Rule to the FTC.

Moreover, the agency should explore creating new reporting pathways for individuals to submit reports when they suspect a breach of their data has occurred, as well as what criteria individuals would be required to submit to FTC. ONC is embarking on a similar public reporting effort related to potential information blocking violations on its Information Blocking Portal. Such work from ONC could serve as a model for FTC.

In addition, stakeholders appear to be largely unaware about the Rule. To date, only three breaches have been publicly reported. FTC reasons that this is likely because most entities in violation have fallen under the HIPAA Breach Notification Rule. However, we would not necessarily dismiss that the small number of reports may indicate a significant undercount of breaches that have actually occurred, given the lack of awareness about this Rule and the current reporting mechanisms in place (such as the form located on this official FTC webpage). Better publicizing the existence of the Rule, as well as making the non-HIPAA covered entity reporting mechanisms more facile and user-friendly, illustrates an opportunity to advance the use of health information technology while strengthening the privacy and security protections for individuals' data.

HIMSS and PCHAlliance endorse FTC undertaking a robust public education campaign (both virtually and via various forms of media and venues across the country) to increase the awareness of and uphold the integrity of what the Rule intends to achieve. As mentioned above, we believe that the Rule is now more relevant than ever. This conclusion is further emboldened by expanded interoperability with the finalization of ONC's and CMS's final interoperability regulations, in addition to the regulatory flexibilities allowing for greater telehealth allowances nationwide as a response to the COVID-19 Public Health Emergency (PHE). The telehealth flexibilities introduced by CMS have driven more healthcare providers and consumers to communicate via non-HIPAA protected means.

We emphasize that privacy and security are not simply about avoiding breaches, but also keeping information private and secure in the first place. The Rule should encourage proactive, instead of reactive, privacy and security practices for personal health information. We recognize the fact that the healthcare sector is being held to a shorter timeline for breach notification to consumers, and that by consequence may create an undue burden on health systems. We encourage FTC to compare industry

standard times outside of healthcare and address the discrepancies and rationale in its final version of the Rule.

Harmonize Privacy and Security Laws, Regulations, Directives, and Industry-Led Guidelines

FTC Health Breach Notification Rule versus HIPAA Breach Notification Rule
In an effort to harmonize privacy and security laws, we strongly believe the distinction between the FTC Rule and the HIPAA Breach Notification Rule must be made clearer to the broader healthcare community. A main area of contention is the fact that the lines between what is considered non-covered *personal health data* and HIPAA *protected health information* are beginning to blur. It is becoming increasingly challenging for regulating agencies to keep up-to-date with the speed and scale of information shared, especially given rules and flexibilities promoting and allowing for greater flow of information across the healthcare ecosystem. Ultimately, what may begin as personal heath data at the outset, may eventually evolve into protected health information depending on who it is shared with or how it is shared. This lack of clarity only reinforces the importance of harmonizing these laws and ensuring that they are completely coordinated moving forward.

For these reasons, it may be beneficial to have a clear depiction of how these two rules operate side-by-side. We recommend FTC collaborate with HHS to develop an illustrated roadmap for providers and consumers that depicts the specific paths through which health information can be created, received, maintained, and transmitted within both the context of this Rule and HIPAA. Further, if HIPAA Breach Notification continues to be excluded from FTC Breach Notification, it must be made abundantly clear with the provisions and definitions included in this Rule.

Implications of COVID-19 on Privacy
HIMSS and PCHAlliance believe the current situation facing our nation with COVID-19 further bolsters the recommendation to consider stronger alignment with other laws and regulations. The patchwork of existing state laws focused on health information privacy makes for a challenging environment when attempting to share data. Most of these state laws are not preempted by HIPAA, so inter- as well as intra-jurisdictional information sharing is impacted by myriad regulations and uncertainty over what rules apply in particular circumstances. This has the potential to lead to hyper-interpretation as a means to achieve compliance as opposed to supporting the efficient sharing of key health information to advance high quality, valued-based care related to COVID-19.

In June 2016, ONC published a report entitled, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA*. It identified how large gaps in policies around access, security, and privacy continue, and confusion persists among both consumers and innovators. With new health-related technologies such as wearable fitness trackers, health social media, and mobile health apps gaining prominence in engaging patients, the Report details how our laws and regulations have not kept pace with these new technologies. The Report also identifies the lack of clear

guidance around consumer access to, and privacy and security of, health information collected, shared, and used by those entities not covered by HIPAA.

We believe these developments directly correlate with FTC's ask in this notice. The lack of clarity related to HIPAA, including interpretation and enforcement, as well as the Rule, has created significant gaps in compliance and enforcement, thus jeopardizing the privacy and security of personal health data.

Given the current environment, and the emerging roles of entities that handle personal health data but fall outside the scope of HIPAA, privacy and security requirements need to be broader and more encompassing to reflect today's current environment and the flow of personal health data. As broader health data privacy and security changes are considered across HHS, FTC, or by Congress, these issues need to be addressed. Under any scenario, the key principles are that the patient or consumer is involved, engaged, and at the center of any decision-making involving the sharing of their personal data.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Ashley Delosh, HIMSS Senior Manager of Government Relations, at Ashley.Delosh@himss.org, or Robert Havasy, Managing Director of PCHAlliance, at rhavasy@pchalliance.org, with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO