August 8, 2023

The Honorable Lina M. Khan, J.D.
Chairperson
Federal Trade Commission
Washington, DC 20580

Dear Chairperson Khan:

On behalf of the Healthcare Information and Management Systems Society (HIMSS), we are pleased to provide written comments to the Federal Trade Commission proposals for amending the Commission's Health Breach Notification Rule. HIMSS appreciates the opportunity to leverage our members' expertise to share feedback on the movement to align privacy compliance requirements for health information. We look forward to continued dialogue with the Federal Trade Commission on this topic.

HIMSS is a global advisor and thought leader and member-based society committed to reforming the global health ecosystem through the power of 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 driven by health equity. 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. 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 125,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations. Our global headquarters is in Rotterdam, The Netherlands and our Americas headquarters is in Chicago, Illinois.

As we see attention shift to a consumer-based approach regarding integrated care, with greater incorporation of technology into the healthcare setting, we are witnessing more information becoming readily available and its access critical to coordinated, efficient, and quality care. As result, there are two competing truths that need to be reconciled: patient information must be treated respectfully and unequivocally needs to be protected, for both privacy and security purposes; and healthcare delivery and coordination of care cannot be achieved without reliable information shared in an interoperable manner across various, sometimes competing, systems. Thus, a careful balance must be made between the need to keep the information private and secure, while remaining shareable across various environments to help ensure that patient health and care is not impeded.

As a matter of principle, HIMSS firmly believes that seamless, secure, ubiquitous, and nationwide data access and interoperable health information exchange should ensure the right people have the right access to the right health information in a usable format at the right time to provide the optimal level of care. The reduction of barriers to the

appropriate exchange of health information through harmonizing privacy and security laws, regulations, directives, and industry-led guidelines is paramount to transforming the health ecosystem, modernizing care delivery, driving health innovation at the institutional and personal level, and enabling health research.

HIMSS commends the FTC attempt to provide clarity about how the FTC Health Breach Notification Rule translates and applies to technologies today, especially clarifying that application developers, even if the application is marketed for wellness, fall under the purview of and must adhere to breach notification requirements. Regulatory certainty from FTC about what actions and entities are covered by the Health Breach Notification Rule will help guide market-driven development of innovation in patient-facing API technologies. Ensuring robust, up to date privacy and security standards and frameworks, including breach notification requirements, is critical to encourage widespread adoption, acceptance, and trust of new, innovative, patient-facing technologies that support information for patients and providers. The intent of these revisions, to ensure that all entities outside of HIPAA's purview, are covered by federal oversight and have responsibilities to protect health information, update impacted parties when a breach occurs, and take appropriate action to mitigate the impact of the breach, are huge wins for consumers and is strongly supported by HIMSS.

We emphasize that privacy and security are not simply about avoiding breaches, but also keeping information private and secure in the first place. HIMSS encourages FTC to explore and encourage proactive, instead of reactive, privacy and security practices for personal health information in future rulemaking cycles.

Clarifying the Rule covers websites, mobile applications, and interconnected devices.

Accordingly, HIMSS supports the FTC modification of the Breach Notification Rule language to clarify that the Rule's scope for breach notification compliance includes any online service, such as a website, mobile application, or internet-connected device that provides mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools. HIMSS also supports the clarification that applications specifically marketed for wellness would still be required to meet Rule compliance requirements, provided the application utilizes identifiable health information on an individual and the application has the technical capacity to draw information from multiple sources and the application is managed, shared, and controlled by or primarily for the individual. HIMSS community observes entities entrusted with potentially identifiable health information should have privacy responsibilities and compliance requirements consistent with those of HIPAA-covered entities. The intent of this proposal is a significant win for consumers.

However, HIMSS community has pointed out that revising definitions of "personal health records," "PHR identifiable health information", and "vendors of personal health records" to clarify that manufacturers of online services, such as a website, mobile application, or internet-connected devices that provide mechanisms to track diseases, health conditions, diagnoses or diagnostic testing, treatment, medications, vital signs, symptoms, bodily functions, fitness, fertility, sexual health, sleep, mental health, genetic information, diet, or that provides other health-related services or tools raised potential

challenges. In the community, the term "Person Health Record" is rarely utilized as patients more frequently utilize websites, web applications and mobile applications, including those that relate to wellness and desktop applications for one's own personal health information.

Accordingly, we respectfully propose that the FTC, in conjunction with Congress, works towards constructing appropriate legislative language that more aptly encompasses the evolving scope of the industry. This involves formulating functional definitions that supersede the usage of outdated terms like "Personal Health Record" and can accommodate the rapidly changing landscape of the health application market. We also urge the FTC and Congress to co-develop guidelines which cover those entities not yet under HIPAA's purview, but which handle and share electronic health information. By ensuring these definitions are purely functional, we can better adapt to the industry's rapid evolution and maintain adequate regulation to safeguard consumer health information.

HIMSS recommends FTC should ensure that the data regulated by this Rule is personal health information, regardless of whether such data is transacted by way of a mobile app, website, desktop application, API, or otherwise, and should have the appropriate privacy and security framework and breach notification responsibilities.

HIMSS recommends FTC align the proposed definition of personal health information 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 continues 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.

HIMSS supports FTC's proposed revisions to the definition of a "breach of security" as and event encompassing the unauthorized acquisitions that occur as a result of a data breach or an unauthorized disclosure.

Mechanism and Timeline for Reporting a Known Data Breach

In the proposed rule, HIMSS noted the following breach notification requirements for "Personal Health Record vendors" experiencing a "breach of security must:

- must notify (within 60 days/10 days depending on size of the breach) the following entities when a breach of identifiable health information has occurred:
    - notice to consumers whose unsecured PHR identifiable health information has been breached;
    - notice to the Commission; and

    - notice to prominent media outlets serving a state or jurisdiction in cases where 500+ residents are confirmed or reasonably believed to be affected by breach
- must provide written notice at the last known contact information of the individual and such written notice may be sent by electronic mail, if an individual has specified electronic mail as the primary contact method, or by first-class mail
- must include a brief description of the potential harm that may result from breach (ie. medical or other identity theft)
- must include full name, website, and contact information (public email address or phone number) of any third parties that acquired unsecured PHR identifiable health information as a result of breach, if this information is known to the vendor of personal health records or PHR related entity
- must include contact procedures must include two or more of the following: toll-free telephone number; email address; website; within-application; or postal address
- must include a description of the types of unsecured PHR identifiable health information involved in the breach (ie. full name, date of birth, Social Security number, account number, or disability code, health diagnosis or condition, lab results, medications)
- must include a description of what the entity that experienced the breach is doing to protect affected individuals, such as offering credit monitoring or other services

HIMSS supports these proposed provisions. However, as recommended in HIMSS 2020 response to the FTC 10-year review of the Health Breach Notification Final Rule, the FTC should 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. To improve consumer and vendor awareness of the Rule, if or when these provisions are finalized, HIMSS recommends FTC undertake 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.

We look forward to the opportunity to discuss these issues in more depth. Please feel free to contact Alana Lerer at alana.lerer@himss.org and Evan Dunne at evan.dunne@himss.org with questions or for more information.

Thank you for your consideration.

Sincerely,

Harold F. Wolf III, FHIMSS
President & CEO