Joseph Simmons
Chairman
Federal Trade Commission
600 Pennsylvania Avenue NW, Suite CC5610 (Annex B)
Washington, DC 20580

RE: Health Breach Notification Rule, 16 CFR part 318, Project No. P205405

Dear Chairman Simmons,

On behalf of the CARIN Alliance, we thank you for the opportunity to comment on proposed updates to the rules for ensuring consumers' data is protected and that breach notifications are timely and comprehensive. We appreciate your consideration of our comments.

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, health plans, digital health organizations, millions of consumers, individuals, and caregivers. We are committed to enabling consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via open and secure application programming interfaces (APIs).

Expansion of Consumer-Facing Applications

Since passage of the HITECH Act, and even since passage of the Cures Act, the number of consumer-facing health applications has exploded. The initial wave of digital health apps and services for consumers, including fitness trackers, diet guidance applications, and personal health record applications tethered to digital health devices. The market has evolved to include a burgeoning supply of applications and services that allow consumers to access, use and share their clinical and claims data from their health plans and health care providers. Many of these apps and services facilitate this access through open APIs, which health care providers and health plans are being required to stand up and support under ONC and CMS rules that implement the 21st Century Cures Act and the current administration's MyHealthEData initiative.

The confluence of these market and regulatory drivers is accelerating consumer access to clinical and claims data, which CARIN and its members support. One of the consequences of this expanded consumer access, though, is confusion about consumers' rights, and obligations of consumer platforms and entities subject to the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA). As the FTC understands well, the consumer protections afforded by HIPAA may end after consumers use a consumer-facing app to access their clinical and claims data.[1] Unfortunately, some developers of consumer-facing applications, not subject to HIPAA, have not always been clear with their users about their data practices, or consistent in how they communicate with users' about their rights and recourses. Significant variation among covered entities about their

[1] Applications owned/operated by covered entities are currently subject to HIPAA.

ability or obligation to authorize or deny API access to consumer-facing applications that request digital access to consumers' clinical and claims data has also caused confusion.

The CARIN Alliance was formed because our members share an interest in creating clear standards for trusted consumer-directed exchange of clinical and claims data. One of its first acts was to develop a Code of Conduct for consumer-facing applications. The Code establishes data practice expectations and standards that consumer-facing applications can voluntarily adopt and become accountable for, through a self-attestation process. The Code provides clarity to covered entities, consumer-facing applications, and consumers around best practices, transparency, consent, privacy, security, and data use.[2] Many industry participants – of all sizes – embrace the Code. Numerous health applications have already attested to it, and many HIPAA covered entities – including the Veterans Administration with its Lighthouse API[3] -- integrate Code self-attestations into their right of access API workflows.

Health Breach Notification Rule and Updates

Again, CARIN members are committed to the highest standards of privacy and security for their users. We believe that there is an ongoing need for the Health Breach Notification rules. The establishment of a voluntary code of conduct is an important first step to support trusted consumer-directed exchange as clinical and claims data moves away from the protections of the HIPAA framework. However, given the expected growth of consumer-directed health data exchange, CARIN and its members believe there is not only a continued need – but a growing urgency – that the FTC enforce its Breach Notification Rules for personal health records. We believe that the FTC has an opportunity, and a responsibility, to ensure that developers of consumer-facing health data applications are aware of their obligations under the Health Breach Notification Rule.

As you look to update the Health Breach Notification Rule, we also encourage you to consider the following areas of enhancement or expansion:

1. Providing greater clarity on the amount of time to notify users of a breach, including aligning the timelines for notifying the FTC of major breaches,[4]
2. Aligning standards and increase consistency in FTC disclosures,
3. Allowing for breach notifications to be sent by email or within the application rather than only via certified mail, and
4. Providing more specificity on post breach mitigation requirements.

[2] The CARIN Code of Conduct is available here: https://www.carinalliance.com/our-work/trust-framework-and-code-of-conduct/. Among other things, companies attesting to the Code must designate an officer who is responsible for ensuring that their commitments to the Code's health information principles are publicly facing, to allow oversight enforcement by the FTC, state attorneys general and other applicable authorities.

[3] See https://developer.va.gov/explore/health

[4] CARIN Members are concerned that thresholds for FTC reporting (ie the number of impacted users) may not be known within 10 days. We ask that FTC align the timelines for notifying the FTC of breaches with the timelines for notifying users of breaches (without unreasonable delay and no less than 60 days after discovery of the breach).

We also believe that it is prudent for you to look at rule-making authority for opportunities to proactively strengthen privacy and security requirements around personal health information outside of HIPAA.

Conclusion:

Again, we appreciate the chance to provide these brief comments. We appreciate all that the FTC continues to do to ensure consumer privacy and security. Please let us know if you have any additional questions at any time. We would be particularly interested in discussing the CARIN Code of Conduct at your convenience.

Ryan Howells
Leavitt Partners
On behalf of the CARIN Alliance
www.carinalliance.com
Washington, D.C.