SIIA Comments on The Proposed Modifications
To the HIPAA Privacy Rule To Support, and Remove Barriers To,
Coordinated Care and Individual Engagement

On behalf of SIIA, thank you for the opportunity to submit comments and suggestions on the Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers To, Coordinated Care and Individual Engagement (HIPAA NPRM). Last year, SIIA launched a Health Data Policy Initiative to encourage the modernization health data privacy regulation from HIPAA and beyond.[1] SIIA represents more than 600 companies in the global information industry, including companies that innovate to create health benefits on an individualized and societal-wide scale. We support bringing United States health data privacy standards into the 21st Century by updating the Health Insurance Portability and Accountability Act (HIPAA) and enacting a national data privacy standard for health data that falls outside of HIPAA.

The 21st Century has seen major transformations in healthcare, driven primarily by technology and consumer demand. Healthcare is no longer centered solely around providers. Consumers expect to be active participants in their healthcare and to have access to the data driving their care decisions. Tech has risen to meet these demands by providing consumers with innovative tools to capture, track, analyze, and share their personal information.

The next step for individual engagement is to build privacy-protective pathways to ensure that patients can securely receive the full potential of data-driven healthcare. We support OCR's intention through the HIPAA NPRM to balance privacy protection with mechanisms for individuals to access their PHI and to direct the disclosure of their PHI to third parties. We provide several suggestions to help improve this balancing with respect to individual access to PHI, and to ensure that the proposed modifications align with other aspects of the HIPAA regulatory framework.

[1] More information on SIIA's Health Data Policy Initiative is available at: https://www.siia.net/health/.

Expand the Definition of Personal Health Application (§164.501)

As noted above, we support OCR's proposal to strengthen an individual's right to access and to direct disclosures of their PHI. This right is critical to empowering patients and to facilitating coordinated care. OCR can enhance individual empowerment by expanding the definition of "personal health application" to maximize the ability of individuals to direct a covered provider to transmit electronic copies of the patient's PHI in an electronic health record to a third party designated by the individual.

The current proposed definition is limited to electronic applications that are used by individuals to access their health information. This narrow definition excludes applications that individuals use to manage their health information and/or to generate insights from such information. These application uses are important to empower individuals and promote coordinated care, particularly to meet consumer expectations for active participation in their health care. Moreover, expanding the definition to include these other uses would align the proposed modifications with the goals of the Interoperability Rule from the 21st Century Cures Act and the HITECH Act, which defines "personal health record" to reach an individual's health information "that is drawn from multiple sources and that is managed, shared, and controlled by or primarily for the individual."

To expand the definition of "personal health application" to incorporate these uses, we suggest the following:

- Personal health application means an electronic application used by an individual to access***, manage, or generate insights from*** health information about that individual, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.

Ensure Flexible and Secure Authentication for Individual Access (§ 164.514, and §164.524)

We support OCR's goal to balance a right for individuals to both access and direct the disclosure of their PHI. We support, for instance, OCR's decision to prohibit unreasonable verification measures on individuals that would impede their access rights or other rights under HIPAA. We encourage OCR, however, to consider several changes to foster a more flexible approach and to ensure individuals have reasonable, timely, and fair access to their data.

Ensuring reasonable authentication for individual access requests is a delicate balance. Authorizing authentication measures that are too strident can result in overreliance on those measures by covered entities and thwart reasonable requests for access to the detriment of the individual. Moreover, it can impede rather than promote interoperability, thereby obscuring the intent of the Interoperability Rule. We encourage OCR to make several changes relating to APIs to promote better individual access to electronic PHI and interoperability.

First, the modifications should not overly focus on permitting covered entities to require written requests, even within the parameters set forth by the NPRM. Even though this is framed as a permissible mechanism for access, the likely result is that it will impede individual access requests made through consumer-facing applications. To avoid this, the proposed modification should expressly contemplate that a request made by a standard, mandated, scalable, and

secure API is a valid mechanism for an individual access request.

Second, the modifications should clarify an individual request made by a standard, mandated, scalable, and secure API is an access request when the application serves as an extension of the individual. This reflects the reality that individuals often use applications to control and access their data, and in such circumstances, the API is merely the vehicle for an access request. OCR can account for this by clarifying in the text that an individual accessing their electronic PHI through an application of their choice is an access request.

Third, and finally, we recommend that OCR modify the timeframe for covered entities to respond to an access request to electronic PHI made via a standards-based API from 15 calendar days to 1-2 calendar days. Allowing access requests to pend for up to 15 calendar days could have detrimental impacts, as individuals often make access requests for needs within a shorter timeframe to help them making important and time-sensitive health care decisions. Moreover, shortening the timeframe to 1-2 calendar days would align the proposed modifications more closely with the Interoperability Rule and the Promoting Interoperability Rule, which impose 1 day and 48-hour timeframes, respectively. Shortening the timeframe also would avoid a potential conflict with the information blocking rules and reduce confusion for entities that are subject to both rules.

Conclusion

In conclusion, we thank OCR for its thoughtful proposed modifications that seek to both empower individuals and improve coordinated care. SIIA is a strong support of both and interoperability, and we look forward to working closely with you on these issues.

Respectfully Submitted on May 6, 2021,

SIIA HEALTH

Sara DePaul
Associate General Counsel & Senior Director, Technology Policy
SIIA - The Software & Information Industry Association
202-789-4471 Office / 614-439-4392 Mobile / @saracdepaul Twitter
https://www.siia.net/health/