July 20, 2022

Melanie Fontes Rainer
Acting Director, Office for Civil Rights (OCR)
U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Acting Director Rainer:

We write to ask for your help in clarifying how the breach notification regulations under the Health Insurance Portability and Accountability Act (HIPAA) will apply when health care providers share protected health information (PHI) with individuals, and use applications for such purposes, including through health information networks and exchanges as defined in the information blocking regulations established by the Office of the National Coordinator for Health IT (ONC). We describe below how certain interpretations of the breach notification rules are causing obstacles to interoperability and the adoption of electronic PHI (ePHI) with individuals, and we request a meeting with you and relevant staff to discuss this issue in more detail, and to consider ways to address it. **We want to strongly emphasize that without OCR providing formal guidance or enforcement discretion on this topic, there will be significant adverse consequences to achieving nationwide interoperability and patient access.**

The CARIN alliance is a multi-sector collaborative working to advance consumer-directed exchange of health information that was convened in early 2016 and now has more than 70 organizations as members. CARIN's vision is to rapidly advance the ability for 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. In this letter, we join with fellow collaborative organizations who we are working with to advance health care interoperability across the country.

Today, individuals (or personal representatives acting on their behalf) are increasingly accessing ePHI by connecting a chosen personal health application to their ePHI through open, standard application programming interfaces (APIs) available through certified electronic medical record systems used by their health care providers. In addition, the information blocking regulations and the Trusted Exchange Framework and Common Agreement (TEFCA) are expanding possibilities for individuals to be able to access their electronic health information (EHI) directly from health information exchanges/networks (HIEs). Although participation in TEFCA is voluntary, entities participating in TEFCA will be required to respond to requests for EHI for treatment and for access by individuals (referred to as "individual access services"). These 21st Century Cures Act initiatives should enable individuals to quickly access key health information across multiple providers through a single query, which we believe will be a game-changer for patients.

As HIEs and large national HIE networks begin to prepare for individual access, they are raising questions about how to assure, to the extent possible, they are accurately matching individuals to their EHI and to understand their potential liability under the HIPAA regulations for sending an inaccurate match. Recent draft guidance by the recognized coordinating entity (RCE) solidified recommendations made by the CARIN Alliance in 2017[1] and 2020[2], that individual access service providers should ensure that consumer-facing applications follow a reasonable standard that matches the NIST 800-63-3[3] guidelines of IAL2. Our fellow collaborative organizations have already shown how this could work and the CARIN Alliance is currently working with stakeholders from across the industry, including the Department of Health and Human Services, on how a digital identity federation proof of concept[4] could work in a networked environment.

[1] https://www.carinalliance.com/wp-content/uploads/2019/04/ONC_trust_framework_comments_FINAL_v2.pdf
[2] https://www.carinalliance.com/wp-content/uploads/2020/12/LPCA_CARIN-Alliance-Federated-Trust-Agreement_FINAL-12.3.2020.pdf
[3] https://csrc.nist.gov/publications/detail/sp/800-63/3/final
[4] https://www.carinalliance.com/our-work/digitalidentity/

Today, HIEs predominantly disclose or facilitate disclosure of information for treatment purposes. Most HIE treatment disclosures are done in response to queries, and matching information to the correct patient occurs by attempting to match demographic variables such as full name, address, full date of birth, phone number, and in some cases the last four digits of a social security number, using a variety of deterministic and probabilistic matching algorithms.

In conversations with large national HIE networks, we have learned that these networks typically return only one patient's records in response to a treatment query, or if there is insufficient data in the query to yield a unique match, no records will be returned. TEFCA standards similarly mandate that only unique matches be returned.

Notwithstanding efforts to assure return of only the correct patient's records in response to a given query, the possibility exists that the wrong patient's records will be sent. In such a case, HIEs and participants in existing large networks rely upon the following exception to the HIPAA breach definition:

"Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in future use or disclosure in a manner not permitted [by the Privacy Rule]." 45 C.F.R. 164.402.

The exception was an important element in the regulatory framework because it addressed potential liability for Covered Entities and their Business Associates related to circumstances beyond their control for benign disclosures of PHI, and as such, helped lead to the adoption of national exchange networks for treatment purposes. Like the treatment use case, we believe the exception is as important to the future success and adoption of individual access services. It reflects a reality about the difficulty in achieving 100% matching accuracy, despite ongoing efforts by ONC and industry to improve matching accuracy.

However, it is not as clear that the HIPAA breach notification rules are as supportive of the responsible exchange of digital health information through HIEs when patients choose apps or services that are not covered by HIPAA. When a non-HIPAA app offering individual access services queries an HIE or national network for individual access using some of the same demographic data fields, the return of records is not subject to a clear exemption from breach liability. As a result, and based on discussions with national networks, we have been told that the networks are seeking to establish an even higher threshold for matching a query to a unique patient in terms of number of demographic data fields and the source of those data fields - a threshold for which is there is no standard definition and that may be difficult to operationalize. The threat of potential penalties in the event of a breach - and having to inform individuals and HHS (on an annual basis) - is an obstacle to facilitating individual access through HIEs and the TEFCA using the same infrastructure used today to support treatment queries.

Given the 21st Century Cures Act initiatives supporting expanded data access for patients through their chosen application, we believe further guidance from your office would be welcomed to address this matching issue. In developing this guidance, we think an important consideration that can be borrowed from current practice is that data recipients (providers of individual access service) be held to a similar, common standard of responsible behavior (reviewing and returning or securely destroying non-matching records). While HIPAA does not apply to non-HIPAA participants offering individual access services, existing HIPAA breach regulations could be interpreted to exclude from breach any inadvertent disclosure of an inaccurately matched patients to providers of individual access services that agree through participation agreements to maintain similar standards of behavior in reviewing and returning/destroying mismatched records before they are populated in the wrong patient's record.

To illustrate, we suggest consideration of the following options (and of course are open to exploring others) to help address the matching issue:

1) Extend applicability of the exception set forth in 45 CFR §164.402(1)(iii) to participants involved in the delivery of individual access services: in the instance of a disclosure where the discloser has a good faith belief that the recipient would not reasonably have been able to retain the PHI.

For example, the preamble to the Breach Interim Final Rule provides a case study where an explanation of benefits is mis-addressed and returned by the Post Office to the sender, unopened. In this circumstance, the Post Office was aware that an individual was a member of a health plan, but that was not considered to be a breach because the contents were not accessed. If a provider of individual access services (such as an app vendor) reviews demographic information and returns or securely destroys non-matches without accessing the underlying records or sending them to the wrong patient, we believe there is a similar result.

2) Issuing guidance and/or enforcement discretion for situations where an app vendor reviews or securely destroys non-matches prior to populating them in the wrong patient's record under the "low probability of compromise" analysis, set forth in 45 CFR §164.402(2).

In such a case an exception to the definition of breach provides the highest level of certainty to Covered Entities and Business Associates, but failure to meet an exception does not mean a disclosure of PHI is a breach. Covered Entities and Business Associates must consider whether there is a low probability that the PHI has been compromised, based on the following factors:

- The nature and extent of the information involved, including the types of identifiers and likelihood of re-identification;
- The unauthorized person who used the information or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the information has been mitigated.

In circumstance where a potential match is sent in good faith by a Covered Entity or Business Associate (whether directly or via an HIE or national network), but the recipient app vendor evaluates the demographic data from those matches and determines that the information was sent on the wrong patient and securely returns or destroys the incorrect record, it is conceivable that under current regulations, a Covered Entity or Business Associate could conclude there was a low probability that sensitive medical record information was compromised. However, entities will likely fear penalties for being wrong in this assessment. But if OCR were to signal that implementation of such policies for dealing with incorrect matches would or should meet the low probability of compromise, that might remove this potential obstacle to nationwide interoperability for individual access services through HIEs and the TEFCA. TEFCA policies and agreements (such as through flow down provisions) could reinforce or require such practices on the part of app vendor recipients.

We appreciate your consideration of these issues and look forward to further discussing them in more detail with you. As needed, please feel free to contact Ryan Howells (ryan.howells@leavittpartners.com) as the point of contact related to this topic. We have copied both ONC and Sequoia on this letter, as we believe addressing this issue is essential to leveraging the TEFCA since it applies flow down of applicable HIPAA privacy and security provisions to all participants whether Covered Entities, Business Associates, or not, to facilitate nationwide individual access services.

Sincerely (and on behalf of our respective organizations),

Ryan Howells
CARIN Alliance

Paul Wilder
Commonwell Health Alliance

Jay Nakishima
eHealth Exchange

Lisa Bari
Civitas Networks for Health

Scott Stuewe
DirectTrust

cc: Micky Tripathi, National Coordinator for Health IT, Office of National Coordinator
Mariann Yeager, CEO at the Sequoia Project