April 12, 2021

Robinsue Frohboese
Acting Director and Principal Deputy
HHS Office for Civil Rights
Hubert H. Humphrey Building, Room 509F
200 Independence Ave., SW
Washington, DC 20201

SUBJECT: Attention: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945-AA00

Submitted electronically to http://www.regulations.gov

Dear Acting Director Frohboese:

The Sequoia Project is pleased to submit comments to the Office for Civil Rights (OCR) on the *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement* proposed rule published in the Federal Register on January 21, 2021. We appreciate OCR's continued commitment to health information privacy and demonstrated record of responding thoughtfully to the comments that it receives on such proposed rules from its many stakeholders.

The Sequoia Project is a non-profit, 501(c)(3) public-private collaborative that advances the interoperability of electronic health information for the public good. The Sequoia Project previously served as a corporate home for several independently governed health IT interoperability initiatives, including the eHealth Exchange health information network and the Carequality interoperability framework. The eHealth Exchange and Carequality now operate under their own non-profit organizations. The Sequoia Project currently supports the RSNA Image Share Validation Program and the Interoperability Matters Cooperative. We are also honored to have been selected by the Office of the National Coordinator for Health IT (ONC) to be the Recognized Coordinating Entity (RCE) for the Trusted Exchange Framework and Common Agreement (TEFCA).

These comments reflect our experience supporting large-scale, nationwide health information sharing, including active work with several federal government agencies. Through these efforts, we serve as an experienced, transparent, and neutral convener of public and private sector stakeholders to address and resolve practical challenges to interoperability. Our deep experience implementing national-level health IT interoperability, including our track record of supporting and operationalizing federal government and private sector interoperability initiatives, provide a unique perspective on the proposed rule.

Overview

The Sequoia Project supports OCR's goals of addressing burdens that may impede the transition to value-based health care by limiting or discouraging care coordination and case management

8300 Boone Blvd STE 500 | Vienna, VA 22182| 571.327.3640 | **sequoiaproject.org**

communications among individuals and covered entities, while continuing to protect the privacy and security of individuals' protected health information (PHI). As we continue to move toward interoperable, digital health information we encourage OCR to coordinate and align its efforts with other relevant regulatory agencies, including the Centers for Medicare & Medicaid Services (CMS), the Office of the National Coordinator for Health Information Technology (ONC), and the Federal Trade Commission (FTC).

Detailed Comments

Based on our years of experience we provide below detailed comments on selected OCR regulatory proposals and requests for information.

Individual Right of Access – New Definition of Electronic Health Record and Personal Health Application

To better support the individual right of access, OCR proposes two new definitions – one for electronic health record and one for personal health applications.

Proposal: Electronic Health Record means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff. Such clinicians shall include, but are not limited to, health care providers that have a direct treatment relationship with individuals, such as physicians, nurses, pharmacists, and other allied health professionals. For purposes of this paragraph, "health-related information on an individual" covers the same scope of information as the term "individually identifiable health information."

Comment: Stakeholders are challenged by the multiplicity of definitions for health information across agencies within the Department of Health and Human Services (HHS). For example, how does this proposed definition of EHR relate to the definition of Electronic Health Information put forward by ONC? We encourage OCR to work with other agencies, such as ONC and CMS to align definitions to the greatest extent possible. We also note that, increasingly, health plans gather and hold clinical information about enrollees, which may be used for payment, case management and other payer operations or shared with clinicians for treatment and care coordination purposes.

Proposal: Personal Health App is defined as an electronic application used by an individual to access health information about that individual in electronic form, 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.

Comment: To ensure coordination across agencies within HHS, it would be helpful to understand whether OCR believes its definition of Personal Health App is consistent with the concept of the "application of the patient's choice" that is used by CMS in it rules regarding the Promoting Interoperability Program and Interoperability and Patient Access, as well the ONC's 21st Century Cures Act regulations. We would also recommend that OCR ensure that its

8300 Boone Blvd STE 500 | Vienna, VA 22182| 571.327.3640 | **sequoiaproject.org**

definition appropriately accounts for the role of a covered entity in facilitating patients' access to Personal Health Apps via other electronic applications that may be controlled by a covered entity. Specifically, to facilitate an app's access to PHI, a covered entity portal frequently plays a role in authenticating the individual and authorizing access. Thus, the technology generally requires that the covered entity play a role in managing access to health information.

Informing Individuals About Personal Health App Privacy and Security Risks

OCR notes in the proposed rule that a personal health app is not acting on behalf of, or at the direction of a covered entity, and therefore would not be subject to the privacy and security obligations of the HIPAA Rules. The agency asks whether covered entities should be required to inform individuals about the privacy and security risks associated with transmitting data to a non-HIPAA-covered entity, and about mechanisms for doing so (such as specific educational requirements or advisory language).

Comment: Personal Health Apps can provide important mechanisms for individuals to access their health information. Given the sensitive nature of individual health information, we strongly recommend that OCR work with CMS, ONC and the FTC to ensure that consumers have meaningful information to understand and act on an app's privacy policy and meaningful recourse should an app developer act in a manner inconsistent with its privacy policy. This collaboration could include both a public education campaign and creation of voluntary model language for use by covered entities to inform individuals that a personal health application is not covered by the HIPAA Privacy and Security Rules. Covered entities should be allowed to provide factually accurate, unbiased, objective and non-discriminatory education about the risks and benefits to individuals of sharing their PHI with a personal health application. However, they should not be required to do so. Any education a covered entity chooses to offer should not serve as a barrier to individuals' ability to share their information with a personal health application.

To address these challenges in a more systematic way, The Sequoia Project urges OCR to work with stakeholders and other policymakers in support of a national privacy framework that more clearly addresses privacy protections for health information and other personal information based on the sensitivity of the data rather than who holds the data (e.g., not limited to HIPAA covered entities). Additionally, we recommend providing resources and guidance to individuals regarding safeguards that they may want to be aware of concerning protection of their individual health information.

Strengthening the Access Right to Inspect and Obtain Copies of PHI

OCR proposes to add a new right that generally would enable an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set as part of the right to inspect PHI in person.

Comment: The Sequoia Project is supportive of individuals' right of access to their health information included in the Designated Record Set (DRS), including through use of personal resources. We encourage OCR to address how this new right of access can be scoped to limit the

capture of information to that contained in the DRS without undoing the benefit for individuals – for example, ensuring that an individual is not filming providers or their staff without consent. We encourage OCR to also consider how this access right would work during a telehealth visit – for example, could an individual record telehealth visits or capture screens shot without the provider's consent?

Modify the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

OCR proposes to prohibit a covered entity from imposing unreasonable measures on an individual exercising the right of access that create a barrier to or unreasonably delay the individual from obtaining access (such as requiring the individual to obtain notarization of his/her signature or limiting the format for making an access request). OCR also proposes to shorten the timeframes for providing access to 15 days (from 30 days) with the possibility of one 15 calendar-day extension (shortened from 30).

Comment: The Sequoia Project supports these proposals to make it easier for individuals to access their health information in a timely fashion, particularly in the event of urgent requests. In a digital environment, the 30-day timeline does not seem necessary or appropriate. In many instances, records can be queried automatically, and results transmitted immediately, consistent with applicable state and federal law. This model of access is occurring every day in the U.S., to the benefit of individual patients and their healthcare providers. Consistent with existing OCR guidance, covered entities are encouraged to respond to individuals' requests as soon as possible, with the proposed 15-day timeframe as an outer limit.

Addressing the Form of Access

The HIPAA Privacy Rule requires a covered entity to provide an individual with access to their PHI in the form and format requested, if readily producible in that form and format. OCR proposes that if another federal or state law requires an entity to implement a technology or policy that would have the effect of providing an individual with access to his or her PHI in a particular electronic form and format, it would be deemed "readily producible" for compliance purposes in fulfilling requests for PHI under HIPAA. OCR offers provision of access via secure, standards-based API as one example.

Comment: The Sequoia Project supports the proposed alignment between HIPAA and other federal rules. However, as noted earlier, definitions of health information vary across federal agencies. Therefore, the technology required by another federal or state law may not facilitate access to the full scope of information contained in a DRS. We also ask OCR to clarify whether this proposal would apply to all covered entities, or just health care providers. CMS currently has rules in place requiring both providers and plans to maintain a patient access API. Finally, we note that health information networks can also be used as a vehicle to provide individuals with access to their health information.

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

8300 Boone Blvd STE 500 | Vienna, VA 22182| 571.327.3640 | **sequoiaproject.org**

OCR proposes to create a separate set of provisions on the right of an individual to direct copies of PHI to a third party (as distinct from the process of a disclosure with the patient's authorization). The proposal has three parts:

a. Requests to direct electronic copies of PHI to a third party will be limited to only electronic copies of PHI in an EHR.
b. Requests would need to be "clear, conspicuous, and specific" – and may be made orally, in writing, or via electronic means.
c. OCR proposes to create a requirement for a covered health care provider or health plan to facilitate an individual's request for a copy of PHI in an EHR and receive the information on behalf of the individual.

Comment: The Sequoia Project supports steps to facilitate the individual right of access. To that end, we support OCR's proposal of a more flexible approach to how requests can be made by creating a standard of "clear, conspicuous, and specific" requests that can be made in alternative manners. This more flexible approach will provide better access than the current requirement of a written request.

With respect to the proposal to require that covered health care providers and health plans facilitate an individual's request for a copy of PHI in an EHR, we urge OCR to acknowledge that health information networks can play a key role in fulfilling requests for information. Regional and national health information networks and frameworks are an efficient mechanism for information sharing. OCR specifically seeks comment on whether and how the agency should clarify that the Privacy Rule permits covered entities to use health information networks to make "broadcast" queries on behalf of an individual to determine which covered entities have PHI about the individual and to request copies of the PHI. We concur with the agency that this data access approach should be allowed and could be considered part of the customer service activities covered entities perform as part of their health care operations. We caution the agency, however, in limiting its language to "broadcast" queries and suggest that OCR use the broader term of "query," as it would then include both broadcast and targeted queries, each of which may be appropriate to a given set of circumstances.

We support individuals' right of access to their health information and believe that covered entities should do their best to facilitate that access. However, we note that a right of access under HIPAA generally becomes an obligation to respond to a request under the Information Blocking provisions included in the 21st Century Cures Act. Therefore, if a covered entity fails to meet the proposed new requirement, there is a potential that the covered entity could also be out of compliance with the ONC Information Blocking rules. We ask OCR, therefore, to address how it would coordinate with ONC and the Office of the Inspector General in these situations. We note that the Information Blocking provisions of the 21st Century Cures Act include a provision on Nonduplication of Penalty Structures [Sec. 4004 - 3022(d)(4)].

<u>Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-level Care Coordination and Management</u>

The Privacy Rule generally requires that covered entities use, disclose or request only the minimum PHI necessary to meet the purpose of the use, disclosure, or request (outside of

treatment purposes). OCR proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a covered health plan to a covered health care provider for care coordination and case management at the individual level.

Comment: We support this provision, as it will reduce some of the confusion and regulatory uncertainty that currently limit information sharing. The Sequoia Project is concerned that covered entities often act to limit the amount of information that they disclose because of confusion about the appropriate and applicable interpretation of the minimum necessary standard. Compliance officers for covered entities are required to take all reasonable steps to assure that the covered entity does not violate HIPAA, even if this action means that some PHI that could possibly be disclosed is not disclosed. Overall, we believe that all stakeholders would benefit from this and additional clarifications on how to interpret the minimum necessary standard for payment and healthcare operations.

In addition, OCR should be aware that this proposal could have an impact on the responsibilities of actors under the Information Blocking rules. In general, what is permissive under HIPAA becomes an obligation to share under Information Blocking. In addition, Minimum Necessary is a factor in meeting the preconditions of the Privacy Exception to Information Blocking. We encourage OCR to work with ONC to provide guidance on how changes to the Minimum Necessary provisions affect obligations under the Information Blocking rules.

Finally, we respectfully request that OCR update its guidance to health care providers on what information can be shared with public health agencies during a declared public health emergency. During COVID-19, providers have been unsure whether they can use existing information sharing infrastructure and the summary record standards established by ONC -- such as The Consolidated Clinical Document Architecture (C-CDA) and related electronic document templates -- to provide clinical data to public health agencies without violating HIPAA's minimum necessary standard.

In OCR's December 18, 2020 Guidance on HIPAA, Health Information Exchanges, and Disclosures of Protected Health Information for Public Health Purposes, the agency stated: "When a PHA requests a summary record or other specified data set, the covered entity may rely, if such reliance is reasonable under the circumstances, on the request being the minimum necessary information the PHA needs for its stated public health purpose if the PHA so represents." By implication, a covered entity can only share a summary record if it has been requested by a PHA that "represents" it contains the minimum necessary information. This requirement limits the ability of covered entities to use health information exchange mechanisms to send summary documents to public health without first assessing whether the PHA has represented that this mechanism meets the minimum necessary standard. We believe that sharing a CCDA or related electronic document templates should be deemed to meet the minimum necessary standard for the duration of a declared public health emergency.

<u>Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management that Constitutes Treatment or Health Care Operations.</u>

OCR proposes to add a new subsection that would expressly permit covered entities to disclose PHI to social services agencies, community based organizations, Home and Community-Based Services providers and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a health care operations activity of a covered health care provider or health plan.

Comment: We generally support this change and agree with OCR that it would facilitate and encourage greater wraparound support and more targeted care for individuals, leading to better health outcomes while retaining existing limits on population-based disclosures. We encourage OCR to provide guardrails around this subsection, given that the recipient entities may not, in many cases, be HIPAA covered entities and may not, therefore, be covered by the Privacy and Security Rules. This could include, for example, limiting the proposed permission to disclose PHI to circumstances in which a particular service need has been identified in an individual's care plan or via a screening assessment.

Implementing this change will require careful balancing of privacy for individuals and burden on covered entities. OCR may choose to require an agreement between the parties that describes and/or limits the uses and further disclosures allowed by the recipients and consider allowing individuals to opt out of this kind of sharing. In our experience, the trust frameworks underlying health information networks could also provide the reassurances needed regarding permitted purposes. For example, many state and national health information networks and trust frameworks require any Participant submitting an electronic request for PHI to assert a valid Permitted Purpose and represent that it has obtained the requisite permissions, under HIPAA or other applicable law, from the individual whose PHI is being sought. We have found that having a set of permitted purposes that are known by, and agreed to, by all those who request information is essential to developing a sustainable trust framework.

As previously noted, information sharing that is permissive under HIPAA can become an obligation to share under Information Blocking rule. This proposal could potentially expand the range of entities that could make a request for information to include social service and community-based organizations. We encourage OCR to work with ONC to provide guidance on how this new subsection affects obligations under the Information Blocking rules.

<u>Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances.</u>

OCR proposes to amend five provisions of the Privacy Rule to replace "the exercise of professional judgment" standard with a standard permitting certain disclosures based on a "good faith belief" about an individual's best interests. In addition, the Department proposes to replace the Privacy Rule provision that currently permits a covered entity to use or disclose an individual's PHI based on a "serious and imminent threat" with a "serious and reasonably foreseeable threat" standard. The agency's goals in making these changes are to encourage the disclosures of PHI to family members and other caregivers when needed to help individuals

experiencing use disorder (including opioid use disorder), serious mental illness, and in emergency circumstances.

OCR further requests comment on whether the Department should apply the good faith standard to any or all of the other nine provisions in the Privacy Rule that call upon health care providers to exercise professional judgment.

Comment: *We note that many of the HIPAA Privacy Rule provisions that call upon health care providers to exercise professional judgment are referenced in the ONC Information Blocking rule's Preventing Harm and Privacy Exceptions, including:*

- *Reviewable grounds for denying individual access to records. 45 CFR 164.524(a)(3)*
- *Safety or endangerment. 45 CFR 164.524(a)(3)(i)*
- *References another person. 45 CFR 164.524(a)(3)(ii)*

In the Information Blocking context, these provisions determine whether information can be withheld and not whether it may be shared and changes regarding the latter may not be fully appropriate for the former.

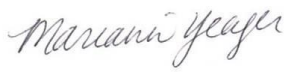
As it considers changes to the standards for provisions that are referenced in the Information Blocking rules, we urge OCR to consult with ONC to understand the implications for affected Actors. To minimize confusion and burden across stakeholders, we ask that the agencies work together to minimize differences between the HIPAA Privacy Rule requirements and the Information Blocking Exceptions and provide guidance on how they interact.

Conclusions

We thank OCR for providing the opportunity to comment on this proposed rule. Again, we strongly support OCR's goals of promoting individual's access to their health information and addressing burdens that may impede the transition to value-based health care by limiting or discouraging care coordination and case management communications among individuals and covered entities, while continuing to protect the privacy and security of individuals' protected health information (PHI).

The Sequoia Project stands ready to assist OCR in advancing a privacy framework that appropriately balances access to information with privacy and security.

Most respectfully,



Mariann Yeager
Chief Executive Officer
The Sequoia Project
8300 Boone Blvd, Ste 500, Vienna, VA 22182