Office of Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, SW
Room 509F, HHH Building
Washington, D.C. 20201

Re: HHS-OCR-2021-0006-0001: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

On behalf of the CARIN Alliance, we thank you for the opportunity to provide feedback on Proposed Modifications to the HIPAA Privacy Rule. We appreciate your consideration of our comments.

The CARIN Alliance is a multi-sector group of stakeholders representing numerous hospitals, thousands of physicians, and millions of consumers, individuals, and caregivers. We are committed to enabling consumers and their authorized caregivers easy access to their personal health information. Specifically, we are promoting the ability for consumers and their authorized caregivers to gain digital access to their health information via open APIs.

We have included responses to the proposed rule that are pertinent to patient access to their health information. We believe the technology and policy have evolved to enable patients to receive their health information more efficiently and with less friction than ever before and would request the HIPAA individual right of access, and the regulations that facilitate that access, be updated to ensure patients receive better and more efficient access to their health information through their individual right of access.

Section A: Individual Right of Access

As outlined above, CARIN was founded to advance consumer-directed health information exchange. Facilitating consumer access to more data with less friction is critical to individual engagement in personalized health care. Ensuring that regulatory frameworks are consistent, rights are clear, and responsibilities are well-defined, when coupled with the significant advances in technology, is critical to advancing consumer engagement and empowerment.

- Definition of Electronic Health Record in the HIPAA context.
    - CARIN appreciates the work done by OCR to address the unique nature of electronic information stored across systems, which expand beyond the ONC-regulated Certified Electronic Health Record Technology products. We believe that consumers want to, and expect to, access information from a number of sources using a number of "back-end" technologies. Therefore, we encourage OCR to maintain a definition that is as broad as possible mirroring the right of access.
- Definition of Personal Health Application:

- CARIN appreciates OCR's work to distinguish applications and services that give consumers access to, and control over, their personal health information. However, we believe that the definition proposed is not comprehensive enough to capture all of the ways that individuals could aggregate their information for personal use. Therefore, we propose a new definition for personal health application. OCR should adopt a functional definition that focuses on the use of an application and its related technology and services by individuals to exercise their right of access. As a predicate, OCR should look to ONC's approach in defining HIN/HIEs.
- We also believe that OCR should eliminate distinctions about the entity that has "primary" control over the ability to control, manage, and share data (in other words, the owner of the application or service). We believe that lies outside of OCR's statutory authority to regulate data practices between individuals and app developers. Instead, OCR should maintain neutrality, recognizing that some consumers will choose apps from independent developers and others will choose apps from covered plans providers or even business associates, including EMR vendors. In a competitive marketplace, consumers will differentiate which apps they will use as their PHA, based on their different data practices and functionalities. Enabling the right of access is the appropriate context for defining a PHA under HIPAA. It does not need to conform with the definition of PHR under HITECH. A proposed alternative definition follows:

> "Personal health application, service, or tool means an electronic application that enables an individual (or personal representative) to choose to open an account or connect with the application, service, or tool; determine with whom the information can be shared and under what circumstances; to use (or facilitate use) of the information in the record for health, wellness, and other personal purposes; and has the capability to shut down the account or disconnect with the application, service, or tool and take the information with them."

As noted above, we commend OCR for how the proposed rule only uses the defined term "personal health application" in context to individuals requesting access for themselves. It is not used at all in the proposed provisions applicable to third party directives. We believe that this is the right approach because the provisions applicable to the individual right of access (164.524(b)) reinforce that a request for access through a PHA is made by the individual (rather than by the app developer). As a result, it strengthens an interpretation of 164.524 that use of PHAs to fulfill access requests are individual access requests, not third-party directives. It means requests for PHI using a PHA should be handled as individual access requests, whether the PHA is made available to individuals by independent developers, covered entities or business associates. It also means the

scope of PHI that can be accessed by a PHA will not be limited by ePHI in an electronic health record, under the new definition. It means all such individual requests will receive the same protections in terms of fees that can be charged.

  - We also believe that the new pathway for directed access through covered plans or providers might be accomplished through PHAs or services offering PHRs. One of the foreseeable market trends from the changing regulatory landscape is that more covered plans and health care providers will offer PHAs to their members and patients. Under the proposed provisions for third party directives – especially under the new pathway allowing covered plans and health care providers to facilitate their members and patient's access requests – it would be helpful to add clarifying language in the rule that access requests effectuated through a PHA are always considered individual access requests, and not third-party directives. This clarifying language would not limit the ability of covered plans and providers from using the new third party directive pathway through other means.

- Timelines and format for access:
  - CARIN believes that the 15-day timeframe as outlined in the rule is a laudable goal. However, we also encourage OCR to further highlight additional guidance to require covered entities to respond to requests as soon as practicable, with an outside bound for request response (no more than currently allowed under law). For purposes of digital record requests, this would create the expectation that records would be delivered sooner.
  - Additionally, CARIN reiterates our comments above on the utility of the PHA route for information delivery with the supplements to the definition as recommended.
- Proposal to prohibit fees for ePHI:
  - We endorse HHS' position that fees cannot be imposed by the covered entity when individuals access ePHI through a PHA, or more precisely, when accessing ePHI maintained by or on behalf of a covered entity through an internet-based method. We believe that this means fees can't be imposed when individuals access their ePHI through patient portals or patient-access API endpoints. Of note, individuals would not be charged for accessing their ePHI through non-standard proprietary API endpoints or similar technologies. We encourage OCR to confirm this understanding in final regulation or conforming guidance.

Section B: Reducing Identity Verification Burden for Individuals Exercising the Right of Access

CARIN appreciates OCR's ongoing work to facilitate individual access to health care information, including covered entities' unreasonable requests for identity verification. However, we believe that all actors will benefit from additional information and direction on reasonableness in this context. CARIN proposes several potential frameworks for this activity:

- It would be helpful for the rule to adopt a conceptual framework for evaluating the "reasonableness" of measures used by covered entities perform identity verification. An example of a conceptual framework is the "flexibility of approach" construct used in the HIPAA Security Rule to determine which security measures are "reasonable" and "appropriate" for different covered entities and business associates. See 45 CFR §164.306(b). This approach would allow the Dept to apply different standards on the identity verification practices of different covered entities based on non-regulatory factors such as: (i) the size, complexity, and capabilities of the covered entity or business associate; (ii) the covered entity or the business associate's technical infrastructure, hardware and software-security capabilities; (iii) the costs of enabling digital identity verification measures ; and (iv) the probability and criticality of potential risks of unauthorized disclosures.
- Another conceptual framework OCR could use for guidance is found in the Content and Manner exceptions of the Information Blocking rule. Under §161.301(b)(2) of the IB Rule, a covered actor will not violate the Information Blocking rule if it follows an order of precedence in the manner in which it decides to fulfill a request:
    - Using technology certified to standards adopted in Part 170 that is specified by the requestor
    - Using content and transport standards specified by the requestor and published by:
        - The Federal Government; or
        - A standards development organization (SDO) accredited by the American National Standards Institute
    - Using an alternative machine-readable format, including the means to interpret the electronic health information, agreed upon with the requestor
- Another advantage of defining a conceptual framework for interpreting "reasonableness" is that it allows the standard to rise over time. A good rule here would preserve the "floor" specified by proposed 164.524(c)(2)(iii), while allowing the "ceiling" to rise. Potential language OCR could use in this space is:
    - The covered entity may require an individual to make a request for access in writing (in electronic or paper form), provided that it informs the individual of such a requirement and does not impose unreasonable measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity. In determining what measures to verify the individual's identity and authority to make the request, a covered entity must take into account: (i) the size, complexity, and capabilities of the covered entity or business associate; (ii) the covered entity or the business associate's technical infrastructure, hardware and software-security capabilities; (iii) the cost and availability of digital identity verification services certified to standards published by the Federal Government or a standards developing organization accredited by the American National Standards Institute; and (iv) the probability and criticality of

potential risks of patient harm and (v) the probability and criticality of potential risks of unauthorized disclosures.

- CARIN also supports OCR's provisions intended to improve patients' ability to get access to their health information, even when they are not using an app or service. For apps going through FHIR APIs, these should be non-issues – but they are obstacles patients face, and it would be good for us to generally support patient access regardless of the mechanism. For example:
    - We support proposal to prohibit requirement for a notarized signature (particularly when the request is from a personal representative, although not limited to that);
    - We support proposal to prohibit entities from requiring that people come in person for their records;
    - We support the right to inspect; and
    - We support that a covered entity making a broadcast query to get PHI from an HIE to fulfill patient access request should be permitted by the regulations.
- We also encourage OCR to consider additional recommendations aimed at helping patients get their records, such as:
    - Accepting a digital signature, including explicit authorization allowing for the patient to use an OAuth 2.0 process (e.g., SMART Application Launch Framework as required by the CMS and ONC rules) as an OCR-approved means for a patient to digitally access their health information using their individual right of access
    - Allowing individuals to e-mail record requests and also to submit them through the API, for records not available via the API—there should be a range of avenues available for patients (right now many facilities require fax, mail, or in person)
    - Allow any written request from the patient vs. making the patient fill out a particular form.
- OCR specifically asks if entities should be required to – or encouraged to – provide a warning before an individual sends information to a personal health application. We believe that it is important for consumers to understand the implications of using PHAs and have done extensive work to ensure, through attestation to the CARIN Code of Conduct, that PHAs are transparent with their users. However, we are also aware of "warning labels" that seemingly seek to intimidate or scare individual users. If a "warning" is required, the label should be standardized and focus on education for individual consumers, consistent with requirement in the CMS Interoperability and Patient Access Rule, rather than a "poison label" that would dissuade consumers from taking an active role in accessing and managing their health record.
- OCR specifically asks if entities should be required to accept a patient's "form and format" request if the patient is requesting to use technology that is required by other law (like the certification rules) and if entities whose EHRs have technical functionalities that facilitate greater patient access to data, they should be required to turn them on. We support this requirement.

- OCR proposes to clarify in regulations that business associate responsibilities with respect to the right of access are governed by the business associate agreement. We believe that is important that OCR's regulations on business associates account for the responsibilities of actors (who are also business associates) under the information blocking rules. In other words, OCR should take care to ensure that both OCR and ONC are taking consistent approaches with respect to patient access and business associate responsibilities for business associates subject to higher expectations under the Information Blocking rules.

Section D: Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management

The Proposed Rule proposed to establish an exception to the HIPAA Privacy Rule ''minimum necessary'' standard for individual-level care coordination and case management uses and disclosures. The "minimum necessary" requirement requires covered entities to, with some exceptions, limit uses and disclosures of PHI to the minimum necessary needed to accomplish the purpose of each use or disclosure. The proposal would eliminate the minimum necessary requirement for uses by, disclosures to, or requests by, a health plan for care coordination and case management activities with respect to an individual, regardless of whether such activities constitute treatment or health care operations.

The CARIN Alliance supports this proposal for the reasons articulated by HHS, with the focus on individual-level PHI, care coordination, and case management. These latter activities are critical to a digitally-enhanced health care system. We note that this regulatory modification would not directly affect HIPAA patient right of access, which is the primary focus of the CARIN Alliance. Nonetheless, reducing the uncertainty and restrictions under current regulations and policy associated with electronic data access for these activities will improve patient care and will enhance data liquidity. In particular, we expect that this proposal will enable the healthcare system to better take advantage of standards-based API and app-enabled authorized health data access and exchange.

Section E: 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

While CARIN does not take a position on the specific modifications to standards for sharing information with third parties for the purposes of care coordination and case management, we would like to highlight the ability for third-party applications and technology-assisted record services to help in information sharing. Many applications, and the CARIN Alliance through our Code of Conduct, have made significant inroads for consent management, proactive information sharing, and general patient AND care-partner access. We believe that accelerating the adoption of these technologies and the proactive consent management that this new paradigm enables, can help with innumerable use cases, including sharing for social service or social determinants of health use cases.

Notwithstanding the great progress made in this space through consumer consent protocols and technology-assisted personal health records, divergence in regulations (including HIPAA, Part 2 regulations, CMS and ONC information sharing requirements, and state laws) muddy the waters for allowable sharing and appropriate access. We encourage all relevant federal agencies, including OCR, to harmonize regulations to increase clarity and access.

Again, we appreciate your work here and your consideration of our comments. If you have any questions or additional follow-up, please contact me at david.lee@leavittpartners.com.

Thank you for considering our comments and recommendations.