May 5, 2021

Robinsue Frohboese, Acting Director and Principal Deputy
Office for Civil Rights, U.S. Department of Health and Human Services
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue SW
Washington, DC 20201.

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

Re: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement (RIN 0945-AAOO)

Dear Acting Director Frohboese,

On behalf of the Strategic Health Information Exchange Collaborative (SHIEC), which represents seventy-six (76) health information exchanges and health information networks (collectively, "HIEs") across the nation, we appreciate the opportunity to provide feedback on the proposed changes to the HIPAA Privacy Rule (45 C.F.R. 164, Subpart E). SHIEC understands the primary goal of the proposed rule change is to further the Department of Health and Humans Services' (HHS) goal of achieving value-based health care. SHIEC supports this goal and believes that HIEs can be a key partner in achieving it.

HIEs are integral to supporting secure and HIPAA-compliant data sharing among health care providers, health plans, public health authorities, community-based organizations, and other legally authorized individuals. SHIEC's member HIEs serve 92% of the United States population and they also power the nationwide interoperability framework for admission, discharge, and transfer (ADT) alerts—called Patient Centered Data Home (PCDH)—which alerts a patient's home care team of an ADT event no matter where in the United States the care occurred.

We have collected feedback from our membership on the proposed rule, which we outline below. We welcome an opportunity to discuss these comments in more detail with the Office for Civil Rights (OCR):

1. **Support for including data exchange with Community Based Organizations (CBOs) and a request for clarification on the scope of permissible disclosures.**

Proposal: OCR proposes to clarify when a covered entity's disclosures to CBOs are part of that covered entity's treatment and care coordination/case management activities. (See proposed 45 C.F.R. § 164.506(c)(6).) OCR seeks comments on the appropriate recipients of protected health information (PHI) under this proposal, as well as the activities and purposes for which PHI should be used and disclosed.

Comment: SHIEC strongly supports OCR's clarification that a covered entity may disclose PHI to CBOs for the covered entity's own treatment, payment, and health care operations activities. SHIEC agrees with OCR that the HIPAA Privacy Rule, as it exists today, already permits covered entities to disclose PHI to CBOs if the disclosure is for the covered entity's own treatment or certain health care operations.

However, OCR's current proposal may have the unintended effect of limiting the scope of disclosures currently permitted under existing subsection (c)(1)—which broadly permits a covered entity to disclose PHI for its own treatment, payment, or health care operations—because the proposed subsection (c)(6) limits such CBO-recipient disclosures to individual-level care coordination and case management purposes only. This limiting effect may occur because of current judicial principles of regulatory construction, such as the principle that requires a more specific regulatory provision to be given precedence over a more general provision, and the principle that each regulatory provision be given meaning so as not to render other provisions superfluous. We do not believe that this limiting effect is what OCR intends.

Indeed, as OCR notes in its proposal, the addition of subsection (c)(6) is intended to "provide greater regulatory clarity"[1]; not to limit the scope of subsection (c)(1). Thus, SHIEC respectfully requests that OCR move the content of the proposed subsection (c)(6) to a new subsection (d) titled "Activities Included," which would list illustrations of the types of uses and disclosures permitted under Section 164.506. For example:

> (d) Activities Included: Disclosures under this Section may include, but are not limited to:
> (1) Disclosures of individual's protected health information to a social services agency, community-based organization, home, and community-based services provider, or similar third party that provides health or human services (whether such activities constitute treatment or health care operations as those terms are defined in § 164.501).
> (2) [Reserved.]

SHIEC also respectfully requests that OCR consider the following changes that would improve the quality of care and health-related services that individuals receive through enhanced data sharing among covered entities, CBOs and the HIEs that provide the data sharing infrastructure:

- Clarify that business associates may facilitate the full range of requests and disclosures of PHI to CBOs for the purposes permitted under Section 164.506;

[1] 86 Fed. Reg. 6446, 6477 (Jan. 21, 2021).

- Expressly permit in Section 164.506 disclosures for purposes of a CBO-recipient's own health-related services, which depending on the circumstances may constitute treatment or health care operations as those terms are defined in Section 164.501; and
- Expand on the illustrative list of CBO-related uses, disclosures, and requests for PHI.

Incorporating these changes will have the benefit of (i) permitting CBOs to participate in HIEs in a more meaningful way; and (ii) ensuring that all members of a patient's care team have access to the minimum amount of information that they need to support patient care and treatment goals.

2. Support for creating a care coordination/case management exception to the minimum necessary requirement and a request that population health activities also be included in the exception.

Proposal: OCR proposes to add an express exception to the minimum necessary standard for disclosures to or requests by a health plan for care coordination and case management activities with respect to an individual. (See proposed 45 C.F.R. 164.502 § (b)(2)(vii)).

Comment: SHIEC strongly supports lifting the minimum necessary requirement on health plan requests for PHI for care coordination and case management activities with respect to individuals. For too long, the inability to offer technical solutions to implement the minimum necessary requirement with respect to requests from, and disclosures to, health plans stood as a barrier to full health plan participation in HIEs. This change undoubtedly will result in better care for patients, whose health plan care coordinators and case managers will now have the same level of access afforded to their health care provider counterparts who are part of the patient's care team.

SHIEC further requests that OCR consider removing the minimum necessary requirement on disclosures to, or requests by, health plans and health care providers for similar activities conducted at the population health level for their patient and member populations. Performing these activities at the population health level is necessary to identify needed actions at the provider delivery or payer level to improve care at a facility or for a specific population.

3. Support for individual access rights and request for burden reduction and clarification regarding these rights (including timeliness requirements).

Proposal: OCR proposes to reduce the timeframe covered entities respond to individual access requests from thirty (30) calendar days to fifteen (15) calendar days after receipt of the request, with the possibility of one fifteen (15) calendar-day extension. (See proposed 45 C.F.R. § 164.524(b)(2)(i)-(iii).

Comment: SHIEC is in favor of HHS' efforts to expand patient access rights, but SHIEC is concerned that this proposed change will place an undue burden on covered entities and business associates to the extent (i) an access request is received by a business associate; or (ii) the designated record set (DRS) is maintained by a business associate. In these circumstances, covered entities and business associates will need to review and, in many cases, revise the access provision in its business associate agreements because the provision was based on the current thirty (30) calendar-day response requirement. For example, if a business associate agreement currently requires a business associate to forward an access request to a covered entity (or fulfill an access request) within twenty (20) calendar days, that provision would need to be revised to less than fifteen (15) calendar days. This type of wholesale contract review is onerous, particularly for entities like HIEs that have entered into numerous business associate agreements. Further, processing an access request usually takes more time if a business associate maintains the DRS, particularly if the covered entity needs to coordinate with a business associate (or multiple business associates) on what records are part of the DRS, and not duplicative of the records maintained by the covered entity. For these reasons, SHIEC respectfully asks OCR to consider retaining the 30-day response time for access requests when (i) an access request is received by a business associate; or (ii) the designated record set (DRS) is maintained by a business associate.

4. **Support for use of common technologies to facilitate individual access requests and comment for how to achieve this goal without placing undue burden on covered entities and business associates.**

Proposal: OCR proposes to add a new definition of "personal health application" and to treat an individual's personal health application as an extension of the individual (or merely the form/format of how PHI is disclosed) and not as a third party or third-party designee for purposes of HIPAA's individual right of access rule. (See proposed 45 C.F.R. § 164.524(c)(3).) OCR proposes to define "personal health application" 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." (See proposed 45 C.F.R. § 164.501.) OCR also seeks comments on this proposed definition.

Comment: SHIEC supports HHS' efforts to make it possible for individuals to access and direct the disclosure of their health information through use of common technologies, such as smartphones and tablets, without special effort. SHIEC also strongly supports HHS' goal of improving interoperability while maintaining the privacy and security of health information.

It thus bears emphasizing here that the applications individuals use on their devices—including personal health applications—are not an extension of the individual. Nor do they function like other forms of electronic communication, such as email or fax. The owners of these third-party applications have their own data practices that may include reselling data on secondary markets. Resold data could be used for purposes that the individual did not intend, including unwanted marketing or use of the data in research studies that the individual does not support. Many of these third-party application companies are not subject to data privacy and security requirements as stringent as HIPAA, and often cannot even be held accountable in the U.S. jurisdictions where patients reside. Accordingly, and consistent with the HIPAA Privacy Rule, third-party applications historically have been treated as "third-party" requestors and provisioned with access only if the individual directs that access be given consistent with the requirements of Section 164.524 as a third-party directive, pursuant to a valid HIPAA authorization, or under another exception. This framework has proven to harmonize the competing goals of easy access for individuals through use of common technologies and privacy and security by ensuring that a process is followed so that the individual makes a meaningful decision about releasing the individual's highly sensitive health information to a third party, including personal health applications.

Creating a preferential status among third-party applications for "personal health applications" will create additional work and confusion and a host of potential problems. For example:

- Who will be responsible for determining whether a third-party application qualifies as a "personal health application" and thus should be treated as an extension of the individual (and not a third-party designee) under Section 164.524?

- If responsibility lies with the covered entity or is delegated to their business associate, how will a covered entity or business associate determine whether an application is, in fact, a "personal health application"?

- What will be a covered entity's or business associate's liability under the HIPAA Breach Notification Rule[2] and/or the new no Information Blocking Rule[3] if their determination regarding the application's status is wrong? For instance, will there be a good faith presumption available to covered entities and business associates who rely upon an individual's representation that an application requesting access meets the proposed definition of a "personal health application"?

[2] 45 C.F.R. Part 164, Subpart D.
[3] 42 U.S.C. § 300jj-52 and 45 C.F.R. Part 171 (collectively, the "Information Blocking Rule").

- How will an application's status as a "personal health application" under HIPAA interact with other state and federal health information privacy laws (like 42 C.F.R. Part 2) that may not restrict "individual" access" but restricts when disclosures may be made to third parties. For instance, will HIPAA preempt these more stringent laws such that "personal health applications" must be treated as an extension of the individual and not a third party?

For these reasons, SHIEC respectfully requests that HHS preserve the status quo and continue to treat all applications, including personal health applications, as third parties and not an extension of the individual (or mere form/format of disclosure) for purposes of giving access under Section 164.524.

5. Support for patient notice and education about third-party application privacy and security practices and comments for how to achieve this without placing an undue burden on covered entities and business associates.

Proposal: OCR seeks comment on whether covered entities should be required to inform an individual who requests that PHI be transmitted to a third-party application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules.

Comment: SHIEC strongly supports OCR's proposal to permit covered entities and business associates to give patients notice and education about the privacy and security practices of third-party applications. However, SHIEC respectfully requests that HHS not require that covered entities—which have already been heavily taxed over the last year in committing resources to meet the demands of the COVID-19 pandemic—shoulder the burden of providing this notice and education.

There are an infinite number of applications in the marketplace. Their data practices vary widely and are often subject to unilateral change by the application company. Other regulations, such as the new no Information Blocking Rule, may penalize health care providers and HIEs if their notice and education about a particular application is not factually accurate. Thus, if patient notice and education is mandatory, it will be incumbent on health care providers (and HIEs to whom providers may delegate this responsibility) to vet applications routinely to ensure that any patient notice and education about a particular application's privacy and security practices is accurate. This would impose a heavy burden on an already resource-strained industry.

However, to the extent this becomes a mandatory requirement, SHIEC proposes that HHS reduce the burden on covered entities and their business associates by:

- Permitting covered entities and business associates to discharge this obligation by providing a patient education page that generally discusses privacy and security

considerations relating to third-party applications in lieu of application-specific notice and education, similar to current CMS requirements for CMS-regulated payers who are required by law to provide third-party applications with access to certain health information at the direction and with the approval of current members or their personal representatives (*see, e.g.*, 42 C.F.R. § 422.119(g)); and

- Permitting covered entities (and their business associates to whom they delegate this obligation) to reasonably rely upon industry groups that might provide specific application vetting and/or certification.

6. Support for expanding the "good faith belief" standard and presumption of compliance, as well as a request for clarification that this also applies to business associates.

Proposal: OCR proposes to amend five (5) provisions of the Privacy Rule to replace "exercise of professional judgment" with "good faith belief," including with respect to verifying a requestor's identity when disclosures are made under 45 C.F.R. § 164.510 (disclosures requiring an opportunity for the individual to agree or object) or 45 C.F.R. § 164.512(j) (disclosures to avert a serious threat to health or safety), and to presume that a covered entity has complied with the good faith requirement. (See proposed 45 C.F.R. § 164.514(h)(2)(iv) and *id.* § 164.502(k).) OCR further seeks comment on whether OCR should apply a presumption of good faith and compliance to all fourteen (14) provisions of the Privacy Rule that allow covered entities to use or disclose PHI based on the exercise of professional judgment, such as for disaster relief, law enforcement, and for victims of abuse, neglect, or domestic violence.

Comment: SHIEC supports the good faith belief standard and presumption of compliance. As integral partners in data exchange relationships across the United States, it's our membership's collective observation that HIEs, health care providers, health plans, public health authorities and others who participate in trusted exchange networks place the highest priority on the security and privacy of health information exchange. Recognizing this commitment with a presumption of good faith is not only well founded but a show of trust in the people and organizations who power our health care system. SHIEC thus encourages OCR to extend the standard and presumption to apply to business associates and to other disclosures permitted under the HIPAA Privacy Rule, including disclosures made pursuant to a HIPAA authorization or to facilitate individual access requests where a covered entity or business associate acted in good faith to verify the identity and authority of the person or entity requesting access. Extending this presumption to include business associates and other disclosures permitted by the HIPAA Privacy Rule is an act that will strengthen HHS' goal of establishing national trust connections for data exchange. This presumption will also provide some relief for covered

entities and business associates who must balance verifying identity and authority with not imposing unreasonable verification measures on those persons and entities requesting PHI.

7. Request for further guidance on what constitutes unreasonable access and verification measures.

Proposal: OCR proposes to prohibit covered entities from imposing unreasonable measures on individual access to records, including unreasonable verification measures. (See proposed 45 C.F.R. § 164.524(b)(1)(ii) and *id.* § 164.514(h)(2)(v).)

Comment: SHIEC supports OCR's intent to break down barriers to individual access requests. However, SHIEC seeks clarification from OCR on how covered entities and business associates, particularly in circumstances where the covered entity or business associate might not have a direct treatment relationship with the individual and the access request is made remotely (such as through use of a third-party application), may discharge their identity and authority verification obligations without such measures being deemed unreasonable. For example, requiring that a patient or patient's personal representative notarize a release of information form has been a common method of verifying that person's identity and authority when the organization responsible for disclosing the PHI does not have direct treatment relationship with the individual and does not have the resources to hire full-time staff to perform such verification measures or pay a credit agency to provide electronic identity verification. However, OCR's proposal would deem requiring notarization under any circumstances unreasonable.

SHIEC respectfully requests that OCR provide examples of reasonable identity and authority verification measures that will satisfy the HIPAA Privacy Rule and HIPAA Security Rule[4] requirements for remote access requests when the covered entity or business associate lacks a direct treatment relationship with the individual. For example, would it be reasonable for a covered entity or business associate to assume that a person using a third-party application who has the name, date of birth, address and health plan ID or medical record number of a minor patient is the parent/guardian of the minor patient for purposes of verifying that person's identity and authority for access?

8. Support for clarifying the scope of third-party directives and a request for clarification regarding the definition of "Electronic Health Record," as well as further burden reduction and confidentiality protection measures.

[4] 45 C.F.R. Part 164, Subpart C.

Proposal: Consistent with the federal court decision in *Ciox Health, LLC v. Azar, et al.*, No. 18-cv-0040 (D.D.C. January 23, 2020), OCR proposes to limit the scope of third-party directives (that is, when an individual uses the HIPAA right of access to give access to a third-party designee) to health information maintained in the "Electronic Health Record." (See proposed 45 C.F.R. § 164.524(d)(1).) OCR proposes to allow such requests to be made orally, so long as they are clear, conspicuous, and specific. OCR proposes to define "Electronic Health Record," in pertinent part, as "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, as defined at §164.501, such as physicians, nurses, pharmacists, and other allied health professionals." (See proposed 45 C.F.R. § 164.501.) HHS also seeks comment on whether the proposed definition of "Electronic Health Record" is too broad or not broad enough.

Comment: SHIEC supports aligning the HIPAA Privacy Rule with the *Ciox* decision by including a definition of "Electronic Health Record" and limiting it to the electronic medical record maintained by or on behalf of covered health care providers who have a direct treatment relationship with individuals. SHIEC further suggests that OCR delete the phrase "but are not limited to" from the definition so the definition is better aligned with OCR's intent to limits its scope to clinicians with a direct treatment relationship with the patient. This deletion will also best reflect the court's holding in *Ciox*.

SHIEC also encourages OCR to eliminate the expansion of the third-party directive right to include oral requests. Electronic health records contain sensitive health information about individuals. Providing access to third parties that are not subject to HIPAA or other state and federal privacy laws can have dire consequences for individuals who, in many cases, will not know that the recipient of their health information may not be subject to these laws. Requiring that such requests be made in writing provides individuals with the opportunity to think and reflect before authorizing such disclosures. It also reduces the chance of human error between what is said in a conversation and what is acted upon, by giving the covered entity and/or business associate written direction regarding the individual's approval for third party access. SHIEC believes maintaining the writing requirement for third-party directives serves as an important safeguard for honoring patient choice.

9. Response to request for comment on broadcast queries.

Proposal: OCR seeks comment on approaches it may take to clarify that the HIPAA Privacy Rule permits covered entities to use HIEs to make "broadcast" queries on behalf of an individual to determine which covered entities have PHI about the individual and request copies of that PHI. Section 164.506(c)(1) permits a covered entity to disclose PHI for its own health care

operations purposes, including customer service activities, which could include forwarding an access request to other providers using a trusted exchange network. OCR is considering approaches to clarifying this permission to enhance the right of access and seeks comment on how to do so effectively.

Comment: SHIEC supports OCR's efforts to clarify an HIE's ability to support covered entities in fulfilling individual right of access requests via broadcast queries. SHIEC agrees that the HIPAA Privacy Rule as currently written would allow HIEs to support broadcast queries made by covered entities who are seeking to fulfill individual access requests. OCR could add the following clause to 45 C.F.R. § 164.506(c)(1) to further clarify such exchange.

> "A covered entity may use or disclose protected health information for its own treatment, payment or health care operations, including to initiate a query for additional protected health information from other covered entities for these purposes."

SHIEC would like to note that not every HIE will be permitted under their business associate agreements with covered entity participants ***to disclose PHI*** in response to such a broadcast inquiry. Covered health care providers and health plans may choose to restrict an HIE's ability to respond directly to individual access requests. This is often necessary to ensure compliance with more restrictive state and federal laws—such as minor/parental access laws in which a minor (and not the parent/guardian) holds the right of access or other state laws that require a provider to verbally communicate medical information with the patient before making it electronically available to the patient. It may also be necessary to allow a covered provider to make patient safety and confidentiality determinations with respect to health information that may be shared with the patient's other providers and plan for treatment, payment and health care operations purposes through a trusted HIE connection, but which may cause a substantial risk of harm if disclosed to the individual—such as in instances where the provider believes the individual who holds the right of access may be abusing the patient or the individual's abuser may be improperly accessing the individual's accounts. Thus, acknowledging a covered entity's ability to make broadcast queries in support of an individual access use case may not be the same as providing access to that individual's records. Additional regulatory or legislative action—such as requiring HIPAA preemption of state laws that place legal preconditions on individual access rights—may be needed.

10. Additional request for consideration regarding HIPAA's self-pay restriction on disclosures to health plans and the barrier it poses to care coordination.

SHIEC further wishes to share with OCR comments from the health care community regarding the requirement that covered entities agree to a request by an individual to restrict the disclosure of PHI about the individual to a health plan for payment or health care operations

purposes not required by law if the PHI pertains solely to a health care item or service for which the individual has paid the covered entity in full. *See* 45 C.F.R. § 164.522(a)(1)(vi). The health care community understands that the motivation for this restriction in 2013 was to mitigate the harmful effect of coverage or payment denials for pre-existing conditions.

However, there have been significant changes since 2013. Health plans today cannot refuse to cover individuals or charge more for pre-existing conditions. Health plans also play a critical role in care coordination and case management efforts that lead to better patient outcomes and reduce the costs of care. There is also much greater interoperability and electronic data exchange but implementing this restriction in an electronic environment requires administrative, technical, and financial resources that might not be available to all health care providers. Accordingly, the community expresses interest in whether OCR may undertake efforts to lessen the burden of this restriction to improve patient care and coordination.

11. Supporting comment letters

Several our HIE members, which are listed below, wish to add their individual support for the items raised in this comment letter. We would also like to draw your attention to the comment letters from other HIE members which have been separately submitted, including by the New York eHealth Collaborative and Manifest MedEx. As you will see, the SHIEC HIE community is deeply engaged in HIPAA-compliant health information exchange across the country, and we stand ready to collaborate to support and achieve the goals of this proposed rule.

Thank you for the opportunity to provide feedback and for your continued commitment to improving interoperability and health information exchange. If you have questions, please do not hesitate to reach out to SHIEC's interim CEO, Lisa Bari at lisa.bari@strategichie.com.

Sincerely,

Lisa Bari
CEO (Interim)
Strategic Health Information Exchange Collaborative (SHIEC)

SHIEC HIE MEMBERS WHO JOIN THIS COMMENT LETTER (and primary state/region)

Colorado Regional Health Information Organization (CORHIO)
CyncHealth (Nebraska; Iowa)
Delaware Health Information Network (DHIN)
The Health Collaborative (Ohio)
Hawaii Health Information Exchange
Health Current (Arizona)
HealthInfoNet (Maine)
Indiana Health Information Exchange
Manifest MedEx (California)
Michigan Health Information Network Shared Services (MiHIN)
Midwest Health Connection (Missouri)
MyHealth Access Network (Oklahoma)
North Carolina Health Information Exchange Authority/North Carolina HealthConnex
Reliance eHealth Collaborative (Oregon)
Rochester RHIO (New York)
SYNCRONYS (New Mexico)
Vermont Information Technology Leaders (VITL)
Wisconsin Statewide Health Information Network, Inc. (WISHIN)