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

May 6, 2021

Secretary Xavier Becerra
Acting Director Robinsue Frohboese
U.S. Department of Health and Human Services, Office for Civil Rights
Attention: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement NPRM, RIN 0945–AA00,
Hubert H. Humphrey Building, Room 509F
200 Independence Avenue, SW
Washington, DC 20201

Re: Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement (RIN 0945-AA00)

Dear Secretary Becerra:

The Confidentiality Coalition appreciates the opportunity to submit comments on the "Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement" (Proposed Rule) issued by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

The Confidentiality Coalition is composed of a broad group of hospitals, medical teaching colleges, health plans, pharmaceutical companies, medical device manufacturers, vendors of electronic health records, biotech firms, employers, health product distributors, pharmacies, pharmacy benefit managers, health information and research organizations, patient groups, and others founded to advance effective patient confidentiality protections. The Coalition's mission is to advocate policies and practices that safeguard the privacy of patients and healthcare consumers while, at the same time, enabling the essential flow of patient information that is critical to the timely and effective delivery of healthcare, improvements in quality and safety, and the development of new lifesaving and life-enhancing medical interventions.

Our comments are organized into three sections:

Section I: General Comments. We provide here our overarching concerns and recommendations.

Section II. Accounting of Disclosures Rulemaking. We revisit the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH Act) Accounting for Disclosures rulemaking and provide our recommendation regarding HHS' next steps in this regard.

Section III: Specific Comments. We provide our specific comments and recommendations on the modifications included in the Proposed Rule.

I. General Comments

The Confidentiality Coalition commends HHS for proposing changes to the HIPAA Privacy Rule to remove barriers to the exchange of health information for important health care purposes, including coordination of care between health care providers, health plans and others involved in the patient's care. We believe that many of the proposed changes, such as those clarifying and incrementally expanding the permitted disclosures of protected health information (PHI) to those involved in an individual's care, will have a positive impact on patient care and health outcomes. We also commend HHS for its efforts to reduce regulatory burden where there are no offsetting patient benefits or protections, such as the proposed elimination of the written acknowledgement of the Notice of Privacy Practices (NPP).

The HIPAA framework, which has been in place for over 20 years, has gained widespread consumer trust and acceptance, and any changes must build on and strengthen that trust by facilitating the disclosure of PHI where this will lead to better care without compromising privacy. This is especially important for members of disadvantaged communities, who face greater socioeconomic and other barriers to care, and where trust in the health care system is therefore fragile. Only by assuring these communities that their health information will remain protected once disclosed for health purposes can we hope to make progress towards health equity and better health outcomes for all Americans.

The Confidentiality Coalition strongly supports efforts to give patients greater access to and control over their health information, and appreciates the steps taken by HHS in the Proposed Rule to achieve that end. However, we believe that it is important to recognize that until non-HIPAA entities, such as third-party application (app) developers, are subject to privacy and security requirements commensurate with those in HIPAA, there is an unacceptable trade-off between expanded patient access rights as envisioned by the Proposed Rule and patient privacy protections. We are concerned that the Proposed Rule makes such a trade-off in its decision to treat access by third-party apps at the direction of the individual as access by the individual, rather than what it is, namely, access by a third party. This is inconsistent with reality and a significant departure from HHS' prior position and existing OCR guidance. Yet there is no direct acknowledgement of this change in position in the Proposed Rule and, consequently, there is no discussion of the rationale for doing so, the implications for patient privacy, or the alternatives to this approach in the Proposed Rule. It should be noted that even with the extensive efforts supported by covered entities, many patients are today confused and uncertain as to when their PHI is no longer protected under HIPAA. The proposed change will only add to this confusion and uncertainty.

We believe it is imperative to consider not only the benefits, but also the risks, of facilitating greater sharing of PHI with entities not currently required to protect this data, and for purposes other than delivering health care. Only by doing so can appropriate measures be put in place to protect patients. These measures should put the onus on the recipients of the data, not on patients or HIPAA entities, to ensure not only that patients fully understand that they are transmitting their health records to third parties, but that the health records remain protected in the hands of those third parties and used and disclosed only for the health care purposes of the patient. As discussed in greater detail in our Specific Comments below, one way to do this is to require that third-party app vendors be contractually required not only to attest to certain privacy

and security standards, but to demonstrate compliance with such standards through an independent certification process.

Finally, we note that there are now multiple rules addressing access to health data and interoperability, including the Office of the National Coordinator for Health Information Technology's (ONC's) final rule on interoperability and information blocking (ONC Cures Act Final Rule)[1] issued pursuant to the 21st Century Cures Act, and the Centers for Medicare & Medicaid Services' (CMS') final rule on interoperability and patient access (CMS Interoperability Final Rule),[2] (collectively, the "ONC and CMS Interoperability Final Rules"). We urge HHS to better harmonize these rules by adopting a common regulatory framework with common terms, definitions and requirements wherever possible. This will not only improve compliance, be less confusing to health care organizations and patients alike, but also help reduce the operational burden on entities subject to a myriad of new rules, each with its own different scope, definitions and requirements. Foundational concepts such as electronic health record (EHR), electronic access and legal representative[3] to name but a few, should have the same meaning and be used for the same purposes under different HHS rules, and be faithful to and consistent with the statute and Congressional intent. Complying with the many new data exchange requirements is already a daunting task for most health organizations at a time when resources are stretched thin due to the ongoing public health emergency. Clear rules, with common terminology and concepts, will facilitate compliance and greatly reduce the implementation burden. To the extent that complete harmonization is not possible, we strongly recommend that HHS provide detailed and integrated guidance to health organizations that takes into account the various different HHS rules governing health information exchange that health care organizations may be subject to.

II. Accounting of Disclosures Rulemaking

HHS makes mention of implementing at some future time the requirement in the HITECH Act - now more than a decade old - to include disclosures by a covered entity for treatment, payment, and health care operations through an EHR in an accounting of disclosures. Specifically, HHS alerts Covered Entities and their business associates that, "[B]ased on the comments received in response to the 2018 RFI, and the history of previous rulemaking on this topic, the Department intends to address this requirement in future rulemaking."[4]

Having worked on this issue since 2009, the Confidentiality Coalition urges OCR to assess whether patient demand and currently available technology support any expansion of the accounting of disclosures requirement, particularly given the requirement in the HITECH Act for a balancing test weighing "the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and...the administrative burden of

[1] See 85 Fed. Reg. 85642 (May 1, 2020).
[2] See 85 Fed. Reg. 25510 (May 1, 2020).
[3] As HHS acknowledges in the Proposed Rule at 86 Fed. Reg. at 6456, footnote 91, the term "electronic health record" is not defined for purposes of the ONC Cures Act Final Rule, and the proposed definition for the Privacy Rule would not apply to the ONC Cures Act Final Rule, although both rules mandate the transmission of certain electronic health information to third parties. It also notes at 86 Fed. Reg. at 6461, footnote 116, that the term "access" is defined differently under the two rules. Similarly, the ONC Cures Act Final Rule uses the term "legal representative", with a different meaning, in addition to the term "personal representative" as defined in the Privacy Rule. For entities subject to both rules, these discrepancies create enormous operational and compliance challenges.
[4] 86 Fed. Reg. at 6454.

accounting for such disclosures."[5] The Confidentiality Coalition believes that such an assessment should result in a withdrawal of any accounting of disclosures rulemaking from the Regulatory Agenda.

The Confidentiality Coalition commends the Department for indicating some years ago that it would not finalize the 2011 Proposed Accounting of Disclosures Rule that would have created a new right to receive an "access report". As the Coalition noted in its comments to that proposed rule, we felt that the access log proposal was overly burdensome to covered entities, and unworkable with then available technology. Further, the Coalition does not believe that EHR technology has yet reached a point where it could capture and integrate into a single, human-understandable format all disclosures for treatment, payment and health care operations. Indeed, preparation of accounting of disclosures reports today (for non-routine disclosures) requires significant manual effort, including chart review and searches of spreadsheets received from various departments and business associates that make disclosures required by law, such as for communicable disease reporting. The reality is that most hospitals and health systems do not solely implement one EHR system, but rather multiple information systems, each tasked with maintaining records of treatment, payment, and/ or health care operations activities related to patients.

OCR should be extremely cautious about establishing an expanded accounting of disclosures requirement that would increase health care providers' costs significantly without providing a true benefit to patients. A few years ago, we performed a survey of our members to determine how often they receive requests for an accounting of disclosures request. Based on our members' experience, patients are not frequently requesting an accounting. To illustrate, one health system has received only 25 such requests over a 14-year period. Requiring covered entities to adopt special, expensive technology - that to our knowledge is yet to be developed and is not required in the most recent edition of certified EHR technology that hospitals and physicians are required to use in Medicare's Promoting Interoperability Program - to be able to accommodate a very small number of requests would increase providers' regulatory burdens and yield scant, if any, patient benefit.

Importantly, patients who do ask for an accounting of disclosures under current law often reverse course when they are told what an accounting of disclosures report would contain. Instead, what these patients typically are seeking is an investigation into whether a specific user of the EHR inappropriately viewed their record. Patients already have a right to understand how their information is used for treatment, payment and healthcare operations. Patients also have a right to know if their information has been used inappropriately through breach notification provisions. Patients additionally have recourse through the complaint process if they believe their PHI has been misused.

The Coalition urges OCR to drop its proposal to address the HITECH Accounting for disclosures requirement in future rulemaking. Should OCR decide to resurrect the accounting of disclosures rulemaking, the Coalition urges OCR to recall both:
(1) the Congressionally-mandated balancing test that calls for any implementing regulations to "only require such information to be collected through an electronic health record in a manner that takes into account the interests of the individuals in learning the circumstances under which their protected health information is being disclosed and takes into account the administrative burden of accounting for such disclosures" and

[5] See section 13405(c)(2) of the HITECH Act.

(2) the December 2013 work of the Health Information Technology (HIT) Policy Committee Privacy & Security Tiger Team that spent considerable time and effort reviewing all facets of the issue, including holding a lengthy virtual hearing. Ultimately, the HIT Policy Committee approved the Tiger Team's recommendations, which called for a step-wise approach to the issue focused on quality over quantity of data that would begin with the ONC conducting pilots of technologies and policies. No ONC pilots have been conducted and, accordingly and appropriately, no further action on the accounting of disclosures rulemaking has occurred, nor should any occur, until at minimum, pilot projects demonstrate both technological capacity and satisfaction of the balancing test included in the HITECH Act.

III. Specific Comments

A. Individual Right of Access (45 CFR 164.524)

1. Adding Definitions for "Electronic Health Record" or EHR and "Personal Health Application" or PHA (45 CFR 164.501)

a. Definition of Electronic Health Record (EHR)

Citing the definition in the HITECH Act[6], HHS states in the preamble to the Proposed Rule that it proposes to define the term "electronic record set" (EHR) to include the clinical and billing records of a health care provider that has a direct treatment relationship with patients.

The Confidentiality Coalition supports limiting the definition of an EHR to records held by covered health care providers that have a direct treatment relationship with the individual, since this is consistent with the definition in the HITECH Act. However, we ask that HHS revise the regulatory text to make clear that it applies only to the records of direct treatment providers, since the proposed regulatory text does not state this. Instead, it states merely that the term "clinicians" as used in the definition "includes, but is not limited to" health care providers that have a direct treatment relationship with the individual. The term "clinician" is also too broad and would result in confusion and inconsistent interpretations.

We do not support expanding the definition to include non-clinical records, such as billing records, and note that the regulatory text, as written, is even broader, including all "individually identifiable health information." Even if the definition were limited to clinical records and billing records as stated in the preamble, the term "billing records" is a broad and vague term, and its use would result in unintended negative consequences. It would impose a significant burden on affected health care providers because records related to billing, such as invoices, generally do not reside within EHR systems. Therefore, including "billing records" in the definition would require combining the records from disparate source systems, often in different formats and using different software. This would be costly and operationally challenging without a commensurate patient care or privacy benefit since these records are not consulted by clinicians for care coordination or delivery, and patients may access this type of information through their existing access rights.

Finally, it also goes beyond the clear language and intent of the HITECH Act definition, which is focused on records used by clinicians for health care delivery and decision-making. For the same reasons, we do not support defining an EHR as an electronic designated record set

[6] See 42 U.S.C 17921(5) ("The term "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.")

(DRS), since it was precisely this unsupported broadening of the definition in the HITECH Act that was vacated in *Ciox Health, LLC v. Azar et al (Ciox v. Azar).*[7]

***Recommendation*: HHS should revise the definition of an EHR, consistent with the definition in the HITECH Act, to state clearly in the regulatory text that it is limited to clinical records maintained by health care providers with a direct treatment relationship with patients.**

b. Definition of Personal Health Application (PHA)

HHS proposes to define the term "personal health application" (PHA) for purposes of expanding an individual's access rights to include transmitting an electronic copy of PHI to or through a PHA. HHS states that this definition is intended to be consistent with the HITECH Act definition of a "personal health record" and is a clarification of the existing access right of individuals.

The Confidentiality Coalition does not agree that disclosure of PHI through a PHA, which necessarily involves disclosure to the third-party vendor operating and maintaining the PHA, is merely a clarification of an individual's existing right of access. On the contrary, OCR has previously made clear through a series of FAQs[8] that transmission of PHI to a health app is a transmission to a third party. It therefore relied on the right contained in 45 CFR 164.524(c)(3)(ii), which allowed an individual to direct the transmission of PHI to a third party designated by the individual.

We understand that HHS may, through this proposal, be seeking to find a new avenue for requiring covered entities to transmit electronic PHI not held in an EHR to third parties after *Ciox v. Azar* held that HHS had exceeded its authority under section 13405(e) of the HITECH Act by having 45 CFR 164.524(c)(3)(ii) apply also to PHI not held in an EHR. However, we are concerned that this new attempt is similarly flawed as exceeding HHS' authority because it involves transmission of any electronic PHI in a DRS to a third party. Indeed, while HHS states in its discussion of PHAs that these are simply a mechanism for individuals to access their own PHI, in its request for comments, HHS effectively acknowledges that this is not the case by asking whether covered entities should be required to educate or warn individuals that they are transmitting PHI to an entity that is not covered by the HIPAA Rules. In addition, the proposed definition of a PHA is so broad that vendors acting on behalf of non-health entities, such as attorneys and insurance companies, are already offering portals by which they may obtain medical records for non-health care purposes for free and without patient authorization by

[7] No. 18-cv-0040 APM (D.D.C. January 23, 2020).

[8] See "The Access right, health apps and APIs" on OCR's website, which includes this FAQ, which states (emphasis added:

What liability does a covered entity face if it fulfills an individual's request to send their ePHI using an unsecure method to an app?

Under the individual right of access, an individual may request a covered entity to direct their ePHI to a third-party app in an unsecure manner or through an unsecure channel. See 45 CFR 164.524(a)(1), (c)(2)(ii), (c)(3)(ii). For instance, an individual may request that their unencrypted ePHI be transmitted to an app as a matter of convenience. In such a circumstance, the covered entity would not be responsible for unauthorized access to the individual's ePHI while in transmission to the app. With respect to such apps, the covered entity may want to consider informing the individual of the potential risks involved the first time that the individual makes the request.

utilizing the PHA mechanism.[9] This is in contrast to the long-standing Privacy Rule requirement that patients be asked to sign a written authorization before their PHI may be shared with third parties. The requirements for a HIPAA authorization are detailed and specific including, among other things, an explicit statement that, once disclosed, the PHI will no longer be protected by HIPAA.

It is critical that HHS explicitly recognize, including in the definition of a PHA, that it involves disclosure of PHI to a third party so that the appropriate Privacy Rule protections are applied. For example, for disclosures of PHI that is not held in an EHR through a PHA, this would require a valid HIPAA authorization, as HHS notes in Footnote 137 regarding "requests to direct non-electronic and non-EHR copies of PHI to third parties." In the case of PHI in an EHR transmitted to a third-party app vendor that is not subject to HIPAA, additional measures should be required to address the privacy and security risks of transmission to such an entity until such time as Congress enacts comprehensive privacy legislation that would protect health information held by non-HIPAA entities. This is especially important in light of HHS' recent steps to greatly increase health data exchange through the ONC and CMS Interoperability Final Rules, which will facilitate the flow of vast amounts of health records from HIPAA entities to non-HIPAA entities that today face few, if any, impediments to commercially exploiting that data.

In its request for comments, HHS suggests different options for covered entities to educate and "warn" the individual of the privacy and security risks, including through "an automated attestation and warning process." As discussed in our General Comments, the Confidentiality Coalition believes that education and warnings place the burden on covered entities and individuals to ensure that their data remains protected and ties the hands of covered entities that have concerns about such a transmission by making it mandatory (in contrast to transmissions pursuant to a HIPAA authorization). It is also not clear exactly what would constitute a sufficient "warning," and what the consequences would be for covered entities when individuals fail to heed the warning and suffer harm as a result. Finally, it flies in the face of experience to believe that most individuals will read, let alone act upon, such warnings. In many cases individuals simply click through these types of warnings and may not even realize that they are granting access to their records to third parties. Based on a recent survey by one of our members, approximately 80% of patients whose records were accessed through a third-party app ostensibly on their behalf were either unaware of the third party and/or did not believe they had provided the third party with the necessary documentation and electronic signature to access their medical records.

Instead, the onus should be placed on PHA vendors to meet minimum privacy and security standards before they may offer their applications to individuals, and to show that they do so by maintaining certification with independent certifying organizations. Such an approach would also address HHS' previously stated concerns that it does not have jurisdiction over non-HIPAA entities, since the HHS requirement would apply to covered entities to only allow the PHAs of

---

[9] See https://blog.cvn.com/latest-federal-plan-to-overhaul-medical-records-rules-promises-big-changes-for-law-firms ("[The] streamlined process means attorneys receive medical records more quickly and without the high fees charged by document centers….Attorneys sign up with ChartSquad for free and refer their clients to the company's easy-to-use online portal. Clients then request their medical records through the company's easy-to-use app and elect to share their records with whomever they choose, including their attorneys. ChartSquad does the rest, updating clients as records are delivered.")

certified PHA vendors to be used to access PHI. The actual certification process could be provided by independent industry-based organizations. HHS could maintain a list of approved certifying organizations, and require that such organizations verify that the PHA operator at least meets certain minimum privacy and security standards, such as those specified in the suggested privacy attestation referred to by the ONC Cures Act Final Rule preamble and mandated by CMS in its recent final rule on Improving Prior Authorization Processes, and Promoting Patients' Electronic Access to Health Information.[10] Requiring a certification in order to transmit PHI through the PHA would provide individuals with real and meaningful privacy protections as compared to education and warnings. Even an attestation process, which relies solely on the self-evaluation by the third-party vendor, provides only the illusion of protection if covered entities must ultimately allow access at the individual's request to a vendor that fails to provide the attestation. Unlike this approach, a certification process will ensure that PHI flows only to those non-HIPAA entities that have been verified to have in place minimum privacy and security protections.

Finally, while all the examples of PHA transmissions given in the preamble to the Proposed Rule involve transmission for health care purposes, this limitation is not included in the definition of a PHA. To avoid abuse by commercial entities seeking to use the data for non-health purposes, a PHA should be limited to an application created and used solely for health care purposes.

<u>Recommendation</u>: HHS should continue to treat transmission of PHI through a PHA as a disclosure to a third party, and only allow such transmission without a HIPAA authorization with respect to PHI held in an EHR. In addition, in the case of such transmissions to third-party apps not covered by HIPAA, the covered entity should be permitted to disclose the PHI only to those third-party app vendors that have been certified by an independent organization as meeting minimum privacy and security standards. Finally, in order to avoid abuse of access rights by non-health third parties, a PHA should be defined as an application created and used solely for health care purposes.

2. Strengthening the Access Right to Inspect and Obtain Copies of PHI

HHS proposes a new access right that would allow an individual to take notes, videos, and photographs, and use other personal resources to view and capture PHI. HHS states that it does not believe that such a right would be inconsistent with federal and state recording laws or intellectual property rights protections.

The Confidentiality Coalition commends HHS for seeking new ways to make health records accessible to individuals. This is especially important during the COVID-10 pandemic, when patients are often not allowed to bring a family member or caregiver to an appointment, making it difficult to capture the information communicated during the visit. Many health care providers have recognized this difficulty and been using digital tools in innovative ways, including video conferencing or livestreaming of patients where appropriate, and other similar mechanisms, to ensure that patients and their caregivers receive the information they need from health appointments to manage their care.

However, we are concerned that the proposal, which differs from current practice by eliminating any exercise of discretion by the covered entity and making access in this manner an individual

[10] This final rule was issued December 2020 but has not yet published in the Federal Register.

right, could have adverse consequences to both the delivery of care and patient privacy. Specifically, clinical workspaces, appointment schedules and staffing are all designed for the optimal and efficient delivery of care. There is very little, if any, excess capacity in the form of additional space, time or staffing, all of which would be necessary to accommodate this new proposed right. Allowing such a right would therefore, at a minimum, disrupt workflow and divert resources in the form of staff and equipment away from patient care. It would also significantly increase the privacy risks to other patient records, since this risk could not be mitigated without substantial logistical and operational system redesigns. It would also impinge on the privacy rights of others in the workspace. For example, some patients may seek to record or video entire appointments or procedures, including the voices and images of physicians and staff. This could be distracting and even unnerving for clinicians and their staff, jeopardizing care or, at the very least, resulting in a less open and helpful exchange of information with the patient. It would infringe on the privacy of the health care staff who would have no control over their own biometric information captured by patients in a non-public setting. Finally, in some states this would also be in violation of state recording laws unless the physician and staff consented to the recording, and it would not be clear which law would prevail in that situation.

For all these reasons we recommend that HHS not mandate this type of access as an individual right. Covered entities are already forging ahead to implement new methods of communicating with, and providing information to, patients and caregivers where this is operationally and logistically feasible for them and in order to enhance patient care. Imposing a mandate upon them to do so in any setting, at any time and using any modality (with the only limitation being that covered entities may refuse to allow a patient to connect a personal device to the covered entity's information system) is not only unnecessary but would be counterproductive and harmful to both patient care and privacy.

Recommendation: We recommend that HHS not proceed with this new mandate on covered entities to allow patients to use their own personal resources to capture their PHI. It is not only unnecessary but would interfere with the clinical workflow and care delivery, divert resources from patient care, and infringe on the privacy rights of other patients and health care staff.

3. Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

a. Prohibition on Imposing Unreasonable Measures for Access

HHS proposes to prohibit covered entities from imposing unreasonable access measures that impede the individual from obtaining access when a measure that is less burdensome for the individual is practicable for the entity.

We support prohibiting the imposition of unreasonable measures that serve as barriers to, or unreasonably delay the individual from, obtaining access to their health records.[11] However, in order to allow covered entities to establish uniform protocols that can apply to all requests, we recommend that the regulatory text follow the wording of the 2016 Access Guidance (to prohibit unreasonable measures that "serve as barriers to or unreasonably delay" the individual from obtaining access), rather than the proposed regulatory text (which would prohibit a measure whenever "a measure that is less burdensome for the individual is practicable for the entity"). The proposed regulatory text could have the unintended adverse consequence of requiring

[11] See OCR's 2016 Guidance on Access Rights.

covered entities to adopt any measure demanded by a particular individual that is less burdensome to the patient but is nevertheless "practicable" for the covered entity, even if it is considerably more burdensome for the covered entity and the measures adopted by the covered entity are not unreasonable. For example, a patient may ask to be allowed to submit a request in person to any clinician examining the patient rather than having to return to the front desk to do so. We believe the language used in OCR's 2016 Guidance appropriately balances the burden of individuals and covered entities and allows covered entities to establish and implement uniform policies across the organization. This in turn facilitates workforce training and will help ensure that individuals requests are handled quickly and efficiently.

<u>Recommendation</u>: The Confidentiality Coalition supports the prohibition on the imposition of unreasonable measures for individuals to access their PHI and recommends that HHS revise the regulatory text to text to follow the wording of its 2016 Access Guidance to prohibit the imposition of unreasonable measures that serve as a barrier to, or unreasonably delay, access, taking into account the burden imposed on both the individual and covered entity. This language strikes the right balance by considering the burden on both parties.

b. Timeliness

HHS proposes to shorten the time frame for responding to requests to require that access be provided as soon as practicable, but in no case later than 15 calendar days after receipt of the request, and that an even shorter time frame will be deemed to be practicable if it is required by another state or federal law applicable to the covered entity.

The Confidentiality Coalition supports efforts to improve patients' access to their records. Therefore, we would support language similar to that used for breach reporting, namely "without unreasonable delay but no later than" 30 days. This change would appropriately require that covered entities act with alacrity on access requests but is also inherently flexible in that there may be legitimate reasons for taking longer for some requests. We are concerned that the term "as soon as practicable" is not only too vague, leaving covered entities vulnerable to subjective judgments as to what is practicable for a covered entity, but also fails to account for situations where it may be prudent or in the patient's best interests to delay a response for a brief period, as long as there is a legitimate reason for the delay. For example, a clinical laboratory may, as a practical matter, be able to provide test results simultaneously to health care providers and patients but may choose to make the tests available to providers a day before releasing them to patients so that the health care provider may reach out to the patient first to explain the results.

The Confidentiality Coalition does not support additionally reducing the outer time frame by half to 15 calendar days, or potentially even less, by deeming the time frame imposed by other applicable state or federal laws to be practicable. As we pointed out in response to HHS's December 2018 *Request for Information on Modifying HIPAA Rules to Improve Coordinated Care* (2018 RFI),[12] there may be any number of situations where a longer time frame is necessary, such as requests for records stored remotely on physical back-up tapes, requests seeking email correspondence, and requests requiring records from different departments and housed in different systems or geographic locations, to name but a few. In addition, imposing this much shorter time frame of 15 days or less, may result in some covered entities being compelled to provide an incomplete record, since The Joint Commission, CMS, and state laws, allow for up to 30 days for record documentation to be completed post-discharge.

[12] 83 FR 64302 (December 14, 2018).

While we understand that HHS was strongly persuaded by comments that covered entities manage to comply with shorter time frames when required by other laws, we caution that such comments are merely anecdotal and, in any event, as HHS itself acknowledges, the majority of states do not require time frames as short as 15 days. Therefore, these comments cannot be relied upon as evidence of, or support for, the position that the proposed time frames will not impose an undue burden on covered entities. In addition, they fail to address the very real risks of hasty action to meet the new much tighter time frames, such as incomplete responses or errors, both of which could be detrimental to patient care and privacy. Most importantly, each state law is different, with very few being as broad and extensive as the HIPAA requirement. Therefore, we urge HHS not to deem a shorter time frame to be practicable simply because it is required by another law applicable to the covered entity. Each law is different in its scope and requirements and it would be an unwarranted oversimplification to equate all access laws with one another.

Finally, while the Proposed Rule would allow a one-time extension of 15 days if the covered entity establishes a policy for addressing urgent or high priority requests, we are concerned that such a policy would intrude on the privacy of patients, and place covered entities in the untenable position of having to make subjective judgments to rank individual requests and the veracity of requesters. We strongly recommend that HHS instead retain the existing provision allowing covered entities up to 30 days to respond to a request with a one-time extension of up to 30 days provided that the individual is notified before the end of the initial time frame of the reason for the extension and the date the response will be provided.

Recommendation: We support requiring covered entities to respond to access requests without unreasonable delay, since this makes clear that covered entities must act expeditiously while recognizing that each access request is different. We do not support reducing either the initial time frames or the one-time extension time frame from the current 30 days as long as the patient is notified during the initial time frame of the reason for the extension. We also do not support deeming shorter time frames imposed by other laws as practicable, since this assumes all access laws are the same. Finally, the ability to extend the time frame for a response should not be conditioned on a policy to address high priority or urgent requests, since this could have unintended negative consequences.

4. Addressing the Form of Access

HHS proposes that electronic PHI (ePHI) must be provided through a PHA when readily producible through such an application and asks how best to address individuals' privacy and security interests when providing access to PHI through a PHA, including options for educating individuals that do not delay or create a barrier to access.

As discussed in our General Comments and Section 1.a of our Specific Comments above, we do not believe that educating individuals about privacy and security risks is sufficient to protect their health data from such risks, and that such an approach places the onus entirely on the individual to ensure that their data remains protected. Access should not, nor should it need to, come at the expense of privacy and security protections. Instead, we urge HHS to consider a more robust approach to protecting privacy when health information is provided to a non-HIPAA entity, such as the certification approach we recommend above. In addition, we do not support the proposal to treat access through a PHA as access by the individual. This is not only factually incorrect but leaves patient records vulnerable to access by non-HIPAA third parties seeking

medical records for non-health purposes without obtaining patient authorizations, and often without patients even understanding that they have allowed such access.
HHS also proposes to require that a covered entity not delay in providing access to PHI when it is readily available at point of care in conjunction with an appointment. As noted in our earlier recommendation, we have multiple concerns with requiring health care providers to allow access at point of care simply because the health information may be "readily available" at that time. In most cases, the information would and should be readily available to the clinician, but that is not a valid criterion for mandating that it be made available to the patient there ad then. In addition to the reasons stated above, in many cases clinicians need to update the patient's record following an appointment, and often use the time between appointments do so. Requiring them to now use this time to allow patients to access their records will put pressure on clinicians to rush their documentation or delay it until later, both of which options are likely to result in more hasty and less comprehensive documentation with a greater likelihood of errors.

OCR asks whether it should require a health care provider to implement a secure, standards-based API if it could do so at little or no extra cost, and how to measure cost for this purpose. We do not support OCR requiring health care providers to implement a secure, standards-based API. We believe it would be difficult for HHS to measure or assess what costs a covered entity could afford, and therefore, strongly recommend that HHS not pursue this approach.

Finally, we ask that HHS harmonize its approach to access by third-party apps under this Proposed Rule with its approach under the ONC and CMS Interoperability Final Rules. Both ONC and CMS recognize and treat transmissions to such apps as disclosures to third parties and have shaped their requirements accordingly. OCR too should acknowledge this reality and modify its approach in the Proposed Rule to be consistent with the Privacy Rule requirements for disclosures of PHI to third parties, and the ONC and CMS Interoperability Final Rules.

<u>Recommendation</u>: Access through PHAs should only be allowed with respect to PHAs provided by third-party vendors that have been certified as meeting minimum privacy and security requirements and with respect to those applications that are used solely for health care purposes. Covered entities should not be mandated to provide access to PHI in person at point-of-care in conjunction with an appointment. Finally, HHS should treat access to PHI through a PHA as a disclosure to a third party, consistent with its approach in the ONC and CMS Interoperability Final Rules.

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

<u>Oral Requests</u>
HHS proposes to require covered health care providers to respond to oral requests by individuals to direct an electronic copy of PHI in an EHR to a third party designated by the individual, stating that this is consistent with the requirement in the HITECH Act that the request be "clear, conspicuous and specific."

We do not support this proposal, and believe it flies in the face of the plain meaning of the language in the HITECH Act. We believe that the proposed approach would increase privacy risks to individuals and create disputes with, and potential liability for, covered entities. Privacy risks are more likely to occur if covered entities are required to comply with oral requests, particularly since the individual may request that the PHI be sent to an individual or entity with which the covered entity has had no prior interaction. Errors, misunderstandings and misdirected records are much more likely to occur when relying on oral requests, and this would have adverse effects on both patients and covered entities. Oral requests are also inconsistent

with the plain language of the statute, which requires that such requests be "conspicuous," a term that would not apply to the spoken word. For these reasons, we recommend that requests to direct PHI in an EHR to a designated third party must be in writing.

Finally, we recommend that HHS limit this requirement to disclosures to entities involved in the provision of health care to patients. While the HITECH Act refers to "an entity or person" designated by the individual, the context, including limiting this to PHI in an EHR and requiring that the fees be limited to labor costs only, makes clear that this is intended to facilitate sharing of patient records for health care purposes. We therefore recommend that HHS define the term "third party" to be limited to health care providers, social service organizations with whom PHI may be shared for care coordination, and caregivers. This limitation would better protect patient privacy by ensuring that non-health commercial entities not exploit this access right to circumvent record retrieval fees and other required HIPAA protections, such as the need to obtain a written HIPAA authorization, in order to obtain patient records for non-health care commercial purposes.

Recommendation: We recommend that HHS require that individual requests to direct PHI to third party be in writing and be limited to third parties involved in the patient's care, consistent with the intent of the HITECH Act.

Requestor-Recipient Requests

HHS proposes to require that an individual may direct, orally or in writing, that his or her covered health care provider or health plan ("Requester-Recipient") obtain an electronic copy of PHI in an EHR from one or more covered health care providers ("Discloser").

The Confidentiality Coalition supports efforts to improve the sharing of PHI between health plans and providers to facilitate care coordination and case management. However, as stated in our comments to the 2018 RFI, we are concerned that mandating, rather than allowing, this type of data exchange could have unintended negative consequences to patients as well as covered entities. This is particularly the case if the PHI is required to be disclosed based solely on an oral request, and without any input from the Receiver-Recipient as to whether it needs the records in question. Requiring disclosing health care providers to act on these requests irrespective of whether the request will require manual interventions, could be extremely burdensome for Disclosers, and many providers may not have the staff to be able to respond in a timely fashion. While we appreciate HHS' intent in making this proposal, we believe that health information sharing between health care entities should be determined by the entities involved, not at the initiation of the patient. Health care entities know what information they need for care coordination and case management and, with the implementation of the ONC and CMS Interoperability Final Rules, have the ability to obtain it without the patient's intervention. In addition, it is only when there is true interoperability and the Trusted Exchange Framework and Common Agreement (TEFCA) has been finalized and implemented, that these types of data exchanges will be able to occur seamlessly and without significant effort on the part of the Discloser.

While the disclosure would be to another covered entity, this does not eliminate the risks to privacy, security, and potentially even health care delivery, from the unplanned receipt of significant amounts of health data. Covered entities may not have the resources to store the data or resolve inconsistencies with, or duplication of, data they already hold. The Proposed Rule does not make clear whether the Requestor-Recipient would be required to incorporate the information received into the patient's record, even if it is duplicative, redundant or inconsistent with records already held by the Requestor-Recipient. Transmitting and storing data that an

entity does not need creates very real privacy and security risks. It is these types of risks that minimum necessary and data minimization principles, which are now uniformly embraced in privacy legislation and best practices, seek to reduce, but such principles are not mentioned and so would have no limiting effect in the context of Requestor-Recipient requests as proposed.

We therefore recommend that if HHS proceeds with this proposal, it should, at a minimum, require that all requests be in writing, and that Requestor-Recipients be allowed to exercise reasonable judgment in deciding whether to act on such an individual request. This decision would be based on the nature of the data requested, the data the Requestor-Recipient already holds, its ability to integrate and use the data, and other relevant factors. In addition, Disclosers should be permitted to respond in accordance with their obligations to respond to other entities under the ONC and CMS Interoperability Final Rules, rather than treating such requests as an access right by a patient. Finally, we request that HHS provide additional clarity and/or guidance on who would qualify as a "prospective new patient."

Recommendation: We do not believe this new right is necessary in light of the ONC and CMS Interoperability Final Rules and seeks to mandate health data exchange prematurely before true interoperability has been achieved. If HHS decides to proceed with this proposal, we recommend that it require that all such requests be in writing, that a Requestor-Recipient be allowed to exercise reasonable judgment in determining whether to act on such a request, and that Disclosers be allowed to treat such requests as coming from the Requestor-Recipient, rather than as an access right by the patient. Finally, additional clarity and/or guidance should be provided on terms such as "prospective new patient."

6. Adjusting Permitted Fees for Access to PHI and ePHI

The Confidentiality Coalition supports limiting the fees that may be charged to individuals to access their health records to the reasonable costs of providing that access. We agree that it is important that cost not stand as a barrier to patient access. Far from seeking to "profit" from access requests as HHS appears to be concerned about[13], many covered entities currently choose not to charge any fee to individuals for standard access requests for this reason, instead absorbing the costs or funding them in other ways.

However, the Proposed Rule goes significantly beyond prohibiting covered entities from profiting from access requests and will in fact result in covered entities subsidizing record requests by commercial entities seeking health care records for non-health care purposes. Of greatest concern, HHS eliminates the distinction between individual and third-party access, and would require covered entities to provide PHI without cost to any third parties accessing PHI through a patient's PHA, irrespective of the costs incurred by the covered entity. It would also limit charges to other third parties seeking PHI held in an EHR to only the labor costs for copying the PHI. HHS seeks to justify these limitations by assuming that internet-based access is not "likely" to involve a covered entity's workforce members, and so covered entities are not "likely" to incur

[13] See 86 Fed. Reg. at 6465 ("The proposed approach, described in further detail below, also would allow covered entities to recoup their costs for handling certain requests to send copies of PHI to third parties, while ensuring that covered entities do not profit from disclosures of PHI made at the individual's request.")

allowable labor costs in connection with such requests.[14] It also appears to justify this on the basis that covered entity losses will be less than they would otherwise have been because some requests that would previously have qualified for the below-cost rate charged to patients (the "patient rate") will now be in the form of HIPAA authorization requests which are not subject to the patient rate.[15]

HHS is incorrect on both accounts, both vastly underestimating (or not appreciating) the manual costs involved in record retrieval and compilation, and by assuming that access requests will diminish under the Proposed Rule. Contrary to these assumptions, most EHR systems are not a single database or system, but involve many different systems, holding different data, and often in different legacy systems that are not fully or even partially integrated. It is therefore common for health care providers to have to access multiple systems in order to respond to an access request, even when all the records are held in an EHR (which is often not the case). Large health care systems with multiple hospitals and clinics may easily have dozens of systems,[16] and many receive thousands of requests every month. It is precisely because of the complicated and resource-intensive nature of record response and retrieval activities that many health systems outsource this activity to vendors with specialized expertise to handle these requests on their behalf.[17] This is by no means a no-cost endeavor.

Indeed, as written, the Proposed Rule would trigger a tremendous cost shift of more than $1 billion annually to hospitals, physician groups and other health care providers from commercial entities seeking health care records for non-health care purposes.[18] Consistent with the "fees exception" in the ONC Cures Act Final Rule, HHS should allow covered entities to charge a reasonable fee for access that takes into account any manual effort involved.[19] As noted earlier, HHS should seek to harmonize the terms, definitions and requirements in the Proposed Rule with the definitions in the Cures Act Final Rule. Failure to do so would mean, for example, that what is a "reasonable fee" under the fees exception in the Cures Act Final Rule may be impermissible under the Proposed Rule. This would create unnecessary confusion and complicate compliance, which HHS could avoid by harmonization.

Access requests for records to be provided to third parties are likely to increase exponentially under the Proposed Rule as commercial enterprises seeking to circumvent record retrieval fees take advantage of HHS' treatment of a PHA as access by an individual. Vendors of commercial entities such as law firms and insurance companies are already hailing this change as "monumental," and touting their applications as "falling squarely" within the language of the Proposed Rule, explaining that this "streamlined process means attorneys receive medical

[14] See 86 Fed. Reg. at 6466 ("The Department believes that access through an internet-based method likely occurs without involvement of covered entity workforce members, and thus believes that the covered entity likely incurs no allowable labor costs or expenses.")
[15] See 86 Fed. Reg. at 6467 ("Although covered entities would be restricted from recouping some costs that are allowed under the current rule, the effect of limiting the right to direct PHI to a third party to only electronic copies of PHI in an EHR would significantly reduce covered entities' burdens by increasing the number of requests based on an authorization.")
[16] One large health system for example has 41 different information systems.
[17] See attached Case Study by Ochsner Health System, which receives approximately 17,800 requests per month across its 40 owned, managed or affiliated hospitals and over 100 health centers.
[18] "Report on Economic Impact of HHS Proposal to Adopt 42 CFR §164.524(d) and Apply the Federal Patient Rate to Third-Party Directives," Hemming Morse, May 2021.
[19] See Cures Act Final Rule §171.302 at 85 Fed. Reg. at 25959.

records more quickly and without the high fees charged by document centers."[20] In *Ciox v. Azar*, the court noted that "the volume of Third Party Directive requests has increased *by nearly 700 percent*, as law firms and other for-profit entities realized they could use Third Party Directives to avoid the typically higher state-authorized fees that Ciox previously could charge for fulfilling HIPAA authorizations."[21] There is no reason to believe that this will be different under the Proposed Rule, which makes access by such third parties even easier than under the Privacy Rule prior to *Ciox v. Azar.*

It should also be noted that even when covered entities receive HIPAA authorization requests, they are in most cases limited to charging a reasonable cost-base fee or less because of state law constraints and to avoid the provision of the records being viewed as a "sale" of PHI under the Privacy Rule. Thus, while covered entities have relied on the revenue from authorization request to offset some of the costs of providing records at below-cost to individuals, in many cases their ability to do so is limited, and in most cases covered entities are not able to recover the full costs of providing access to individuals for free or below their costs involved in doing so.

Requiring HIPAA entities to subsidize the record retrieval activities of third parties is not only inappropriate and inequitable but diverts scarce resources away from building out the interoperability infrastructure and other activities beneficial to patients. While the negative impact will extend indefinitely into the future, it is particularly challenging at a time when HIPAA entities are devoting every spare resource to addressing the COVID-19 public health emergency.

Finally, HHS proposes, based on section 13405(e) of the HITECH Act, to limit charges for providing PHI on portable electronic media to individuals to only the labor costs involved, and so excluding costs for supplies or postage, where applicable. We do not believe that the plain reading of the statute precludes charging for these items, since it is clearly referring to situations where the access is provided electronically, which would not be the case where portable media is mailed to the individual. This is consistent with HHS' existing interpretation as reflected in the regulatory text, and we recommend that HHS retain its current language and interpretation. In all cases covered entities should be allowed to recover the reasonable costs of providing access, whether labor, supplies, media or postage.

Recommendation: Covered entities and their business associates should be permitted to recover their reasonable costs in providing access to patients and should not be required to transmit records to third parties at the same rate as charged to patients, including third parties who seek to obtain records by leveraging a PHA.

7. Notice of Access and Authorization Fees

HHS proposes to require covered entities to post a fee schedule on its website and make the fee schedule available to individuals at the point of service, upon an individual's request. Covered entities would also be required to provide an individualized estimate to an individual upon request, and to provide an itemization of the charges for labor for copying, supplies, and postage, upon request.

[20] See https://blog.cvn.com/latest-federal-plan-to-overhaul-medical-records-rules-promises-big-changes-for-law-firms (accessed March 7, 2021).
[21] See *Ciox v. Azar, p.23.*

The Confidentiality Coalition believes that individuals have the right to know what they will be charged for their records. However, unless HHS allows covered entities to charge third parties a different rate for records, we are concerned that the public posting of fees would simply incentivize more third parties to seek to circumvent record request fees by seeking to obtain records under the guise of an access request. We also believe that it is only fair that the time frame for responding to an access request be tolled when a covered entity prepares an individualized fee estimate and until the patient confirms that they wish to proceed with the request. Finally, we do not believe the additional resources involved in itemizing the components of the fee is either necessary or warranted, since patient decisions will be based on the total cost, not the components.

Recommendation: Covered entities should not be required to publicly post their fees unless they are permitted to charge third parties a different rate. In addition, the time frame to respond to access requests should be tolled when a patient requests an individualized fee estimate, and covered entities should not be required to provide a breakdown of the components of the fee, since this serves no practical purpose warranting the additional resources.

B. Reducing Identity Verification Burden for Individuals Exercising the Right of Access ((45 CFR 164.514(h))

HHS proposes to expressly prohibit the imposition of unreasonable identity verification measures, which the proposed regulatory text states are those that require an individual to expend unnecessary effort or expense when a less burdensome measure is practicable for the particular covered entity. HHS states that, in considering what is "practicable" for a particular covered entity, it would take into account the entity's security risks, capabilities and obligations, and the security costs to implement measures more convenient for individuals.

We appreciate the inclusion of examples of unreasonable measures provided by HHS in the Proposed Rule, and request that HHS also include examples and provide guidance on what it believes would constitute reasonable verification measures. This will help covered entities apply consistent standards and remove some of the subjectivity involved in deciding what is reasonable. Verification is particularly challenging for covered entities and their business associates in that, on the one hand, they need to be sure they are not providing access to unauthorized persons, but on the other, may not – and do not wish to – impose overly difficult, inconvenient or unreasonable verification measures that serve as a barrier to appropriate access. By providing examples of reasonable verification, HHS will give covered entities some assurance that if they use those or similar measures and there is nevertheless access by an unauthorized person, they will not be penalized for failure to implement reasonable verification measures.

Recommendation: The Confidentiality Coalition supports the prohibition on unreasonable verification measures, but requests that HHS provide guidance and examples of reasonable verification measures to help covered entities strike the right balance between taking sufficient measures to ensure that PHI is not disclosed to unauthorized person while not making these measures overly burdensome to patients.

C. Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management (45 CFR 160.103)

The Confidentiality Coalition supports HHS' proposed amendment to clarify that the definition of "health care operations" includes individual-level care coordination and case management.

D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management (45 CFR 164.502(b)(2))

The Confidentiality Coalition supports the proposal to create an exception to the minimum necessary standard for individual-level care coordination and case management. While we do not believe a proper application of the minimum necessary standard should pose as a barrier to the appropriate sharing of PHI with health plans for individual-level care coordination and case management, we understand that some covered entities may currently err on the side of sharing less PHI than is optimal due to minimum necessary concerns. The proposed exception would allay those concerns and is sufficiently narrowly tailored so that it is unlikely to result in the sharing of excess PHI and will allow for more complete information about a patient's condition to improve care coordination and case management.

However, we ask that the regulatory text refer specifically to "individual-level" care coordination and case management, rather than care coordination and case management "with respect to the individual," and also provide guidance on the meaning of "individual-level." This is based on the experience of health care providers who are increasingly receiving requests from health plans for real time access to the health records of their entire membership. We believe that such requests for information on an entire population would be subject to minimum necessary, even if the data is thereafter used for individual-level care coordination and case management. In light of this, we ask that HHS clarify that the minimum necessary exception is limited to individual-level care coordination requests and does not apply to requests for data for an entire population, irrespective of how that data is thereafter used

<u>Recommendation</u>: The Confidentiality Coalition supports the creation of a limited exception to the minimum necessary standard to allow the disclosure of PHI to a health plan for individual-level care coordination and case management. This will create consistency between health plans and health care providers when using PHI for the same purposes. We ask, however, that HHS make clear in the regulatory text that the exception applies only to "individual-level" care coordination and case management and provide guidance that requests for PHI on an entire population is subject to minimum necessary, irrespective of how that PHI is subsequently used.

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 (45 CFR 164.506)

The Confidentiality Coalition in principle supports HHS' efforts to clarify when PHI may be shared with social service agencies, community-based organizations and home and community-based (HCBS) services. These organizations provide important and beneficial services to individuals. Covered entities and business associates should not have to be concerned that they might be inadvertently violating HIPAA in sharing PHI with such organizations for individual-level care coordination and case management.

However, we are concerned that, as written, the proposal to expressly permit the sharing of PHI with such organizations is written too broadly, particularly by its reference to "similar third party" and "health or human services." This language could encompass a broad range of entities well beyond those whose primary functions involve performing the types of social service activities

contemplated by HHS and described in the preamble. Many commercial enterprises that provide services to individuals, ranging from transportation companies to food delivery services to pharmaceutical manufacturers may all have divisions that conceivably fit this description, although we do not believe this is HHS' intent.

Such broad terms could also result in health data that is intended to be used for social service purposes being used for other purposes contrary to the intent of covered entities and to the consternation of patients. This will erode patient trust which, as discussed in our General Comments, is essential in order for covered entities to obtain the data they need to deliver health care, particularly to disadvantaged communities in an effort to reduce health disparities and improve health equity. Since disadvantaged communities are more likely to rely on social service agencies and community organizations for support, it is their health data that is more likely to be shared with organizations professing to provide such services, and so with respect to whose data there is not only the greatest likelihood of abuse, but also the most significant adverse consequences.

Therefore, we recommend that HHS provide greater clarity and specificity as to the types of organizations that qualify and those that do not and restrict disclosure to those qualifying organizations whose primary purpose is the provision of the services in question, as evidenced by an appropriate license or certification. Finally, for those that provide health services, we recommend that permitted disclosures be limited to such organizations that hold themselves out to be, and are, health care providers, as evidenced by an appropriate state license. This will ensure that the express permission granted by this provision is appropriately focused and targeted in a manner that protects individual privacy while facilitating the sharing of PHI to enable the delivery of these important services.

Recommendation*: *We generally support efforts by HHS to clarify the circumstances under which covered entities may disclose PHI to social service, community-based organizations and HCBS providers for individual-level care coordination and case management, but recommend that the HHS provide a more focused and targeted exceptions that better captures the intended organizations and services so that this express permission does not become a loophole that puts vulnerable patients' health information at risk.

F. Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder (Including Opioid Use Disorder), Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510–514)

The Confidentiality Coalition supports the proposal 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. We agree that this new standard will facilitate sharing of PHI with family and caregivers by covered entities in emergency and crisis situations and recommend that HHS make this change consistently in the other nine places in the Privacy Rule where this standard is used. We also support the proposal to replace the "serious and imminent threat" standard with a "serious and reasonably foreseeable threat" standard, with the goal of reducing situations in which covered entities decline to make appropriate uses and disclosures due to concerns about their ability to determine whether a threat of harm is imminent. Given the inherent subjectivity in terms such as "serious and reasonably foreseeable" and "good faith," (and even with the new definition of "reasonably foreseeable"), we recommend that HHS provide further clarity on the practical meaning and application of such terms in context, such as through guidance, including guidance

on the factors a covered entity may consider in making a determination, and real-world (i.e., not the most extreme or obvious) examples of what HHS believes would and would not qualify.

We caution, however, that these changes, while positive, will have only incremental value. The primary barriers to sharing PHI of those experiencing a substance use disorder (SUD) or serious mental illness remain the regulations at 42 CFR Part 2 (Part 2 regulations) and more stringent state laws. We understand that HHS is required to issue new Part 2 regulations by March 27, 2021 to implement certain provisions in the Coronavirus Aid, Relief, and Economic Safety Act (CARES Act) that will more closely align the Part 2 regulations with HIPAA. We urge HHS to do so in a manner that removes unnecessary barriers to the appropriate sharing of Part 2 records, such as the current detailed and complex consent requirement in Part 2. Even though the CARES Act eliminates the requirement to obtain a new consent for each disclosure, if the Part 2 consent process and content requirements, as well as other Part 2 record disclosure requirements, remain unduly complex and burdensome, this will frustrate the intent of the CARES Act and Part 2 will remain a significant impediment to the delivery of care to those experiencing SUDs and serious mental health illness.

We also urge HHS to consider ways in which, consistent with its regulatory authority, it can modify the Privacy Rule requirements to mitigate the negative effect of stricter state laws governing SUD, mental health, other sensitive health records, and the records of minors. We do not advocate lessening appropriate privacy protections but rather, eliminating or reducing the impact of state law differences that inhibit the appropriate and beneficial sharing of such data among entities involved in the delivery or coordination of care, or payment for such care. These differences may come in the form of additional consent requirements, which often add paperwork without necessarily improving privacy protections, but also in the form of a myriad of different, often inconsistent, state law requirements that, simply as a result of their differences, pose a major stumbling block to the beneficial sharing of PHI. In some cases, covered entities may not even know what these various requirements are, given the numerous regulatory agencies and types of laws in which they may be found. As a result, they often default to the most stringent state law of which they are aware. This gives the strictest, and sometimes the least well-founded, laws undue weight and influence, contrary to the intent of Congress, HHS and the legislators of other states. We would welcome the opportunity to present suggestions to HHS regarding modifications to the Privacy Rule to address these issues.

<u>Recommendation</u>: We support the proposed changes to encourage the disclosure of PHI in emergency and crisis situations but note that these changes alone will not be sufficient to achieve HHS's stated goals. We urge HHS, pursuant to its authority under the CARES Act, to modify the Part 2 regulations to not only align better with HIPAA, but to do so in a manner that removes barriers to the appropriate exchange of SUD records. We also ask that HHS consider ways in which it may modify the HIPAA regulations to reduce the negative impact of inconsistent state laws on the proper sharing of patient information.

G. Eliminating Notice of Privacy Practices (NPP) Requirements Related to Obtaining Written Acknowledgment of Receipt, Establishing an Individual Right to Discuss the NPP With a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element (45 CFR 164.520)

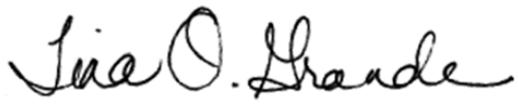
The Confidentiality Coalition strongly supports the proposed elimination of the requirements for a covered health care provider with a direct treatment relationship to an individual to obtain a

written acknowledgment of receipt of the NPP. We agree that the current requirement has not contributed to a greater understanding of a covered entity's privacy practices and that, in some cases, it has even created confusion and misunderstanding. We commend HHS for recognizing the lack of patient benefit and the paperwork burden on covered entities of the NPP acknowledgement requirement. We agree that the proposed changes to the NPP and requirement to designate a person with whom individuals may discuss the NPP would better achieve the intended objective of enhancing patients' understanding of their privacy rights.

***Recommendation*: The Confidentiality Coalition commends HHS for eliminating the NPP acknowledgement requirement for direct treatment providers and supports the other proposed changes to the NPP as better calculated to enhance a patient's understanding of their privacy rights and a covered entity's privacy practices.**

The Confidentiality Coalition appreciates this opportunity to provide comments to ONC on the Proposed Rule. Please do not hesitate to contact Tina Grande at tgrande@hlc.org or at (202) 449-3433 if you have any questions or seek more information about the comments in this letter.

Sincerely,



Tina O. Grande
Chair, Confidentiality Coalition and
Executive VP, Policy, Healthcare Leadership Council