May 6, 2021

Robinsue Frohboese
Acting Director, Office for Civil Rights
200 Independence Ave, SW
Washington, DC 20201

**Re: RIN 0945–AA00. Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement**

Dear Ms. Frohboese:

The College of Healthcare Information Management Executives (CHIME) appreciates the opportunity to comment on the Office for Civil Rights' (OCR), "Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement," published in the *Federal Register* on January 21, 2021.

The College of Healthcare Information Management Executives (CHIME) is an executive organization with a mission of advancing and serving healthcare leaders and the industry improving health and care globally through the utilization of knowledge and technology. Our members are chief information officers (CIOs), chief medical information officers (CMIOs), chief nursing information officers (CNIOs) and other senior healthcare IT leaders. Our members take seriously their charge to protect and secure patient records and are among the foremost experts on how this can best be achieved in a sector that has experienced an explosion in electronic data over the past few decades, CHIME strongly supports patients' rights to access their medical records and data in as facile a manner as possible.

Below we outline our top recommendations in response to the proposed rule. Our detailed feedback can be found following this.

## I. Key Recommendations

1. **HIPAA & Information Blocking -** One of our chief concerns with the proposed rule is that every effort should be made to align the Health Insurance Portability & Accountability Act (HIPAA), information blocking and other interoperability policies to the degree possible and permitted under existing statute;
2. **Individual Right of Access** – We are concerned with the reduction from 30 days to 15 days for meeting a Right of Acccess request will not always be feasible and could add costs to the healthcare system. If OCR adopts a 15 calendar day timeliness standard

starting with the receipt of the request, then there should be a way to document exceptions (i.e., legal dispute and custody cases) that exceed the one additional 15-day extension;

3. **Addressing Forms of Access** – We are concerned about the implications of proposals involving personal health applications (PHAs) calling for covered entities (CEs) to transmit electronic health information (EHI) to PHAs without requiring those PHAs to include privacy and security controls or sign Business Associate Agreements (BAAs);
4. **Strengthening the Access Right to Inspect and Obtain Copies of PHI –** "Readily available" should be designated to mean that the information is available in the patient room during the appointment, can be pulled up and reviewed within the time designated for the appointment and include the ability to temporarily delay release so that certain protected health information (PHI) can be suppressed where there are patient safety concerns;
5. **Addressing the Individual Access Right to Direct Copies of PHI to Third Parties** – CHIME opposes this provision because it places unreasonable responsibility on providers, assumes costs that cannot be reimbursed, and raises security issues associated with requiring a healthcare provider to submit a request for and obtain electronic copies of PHI on behalf of a patient under the Right of Access;
6. **Adjusting Permitted Fees for Access to PHI and ePHI** – We recommend OCR allow providers to charge for the costs of electronic media; and
   **Need for RFI** - OCR raised dozens of important questions in the form of requests for comment in this proposed rule. Given the number of outstanding questions, rather than issuing a final rule based on the responses, we urge OCR to: a) reissue the questions raised in the rule as a request for information (RFI) rather than retaining this as part of the current rule; and b) host listening session to gather more granular input that can be best contextualized through an iterative dialogue.

## II. Individual Right of Access

Our members have expressed several concerns with how the Information Blocking policies will interplay with HIPAA. These questions existed prior to this rulemaking and some of the additional changes, as proposed under this rule, have the potential to create even more confusion. We urge OCR to work closely with ONC to align as many policies as possible and to provide ample time for learning prior to any enforcement. We also strongly recommend that OCR provide significant education and training to providers and patients so that they understand how best to comply. Patients and consumers are an important stakeholder throughout this process.

### A. Proposed Additions of Definitions for EHR and Personal Health Application

OCR says they are proposing to incorporate definitions into the privacy rule that are needed to meet the Health Information Technology for Economic and Clinical Health (HITECH) Act (HITECH).

*EHR*

The Privacy rule does not define EHR. OCR proposes to define EHR as the following:

*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. For purposes of this paragraph, "health-related information on an individual" covers the same scope of information as the term "individually identifiable health information" as defined at § 160.103.*

As the HIPAA Privacy Rule does not currently contain a definition for "authorized health care clinicians and staff," OCR proposes that it include, at least, "covered health care providers who are able to access, modify, transmit, or otherwise use or disclose PHI in an EHR, and who have direct treatment relationships with individuals; and their workforce members (as workforce is defined at 45 CFR 160.103) who support the provision of such treatment by virtue of their qualifications or job role."

**Comment:** This definition is different from the definition in the ONC Information Blocking Rule. The varying definitions of "clinician" and "provider" among these intertwined rules will create confusion and ambiguity. **CHIME urges OCR to harmonize the definition of "clinician" and "provider" with that in the ONC Information Blocking Rule.**

Additionally, several of our members must comply with both HIPAA and the Family Educational Rights and Privacy Act (FERPA).[1] The intersection of FERPA allows for some variation of what OCR is proposing. Under OCR's proposal this means that student health systems ( which are often different than EHRs for hospitals and clinics) are designed with other needs in mind. We have questions about how the two laws align and how compliance will work. The limitations around release of information varies under both laws. How, for example, would an academic medical center who must meet both laws handle release of COVID-19 vaccination information? Does it make a difference if the provider is no longer billing for the vaccine? We seek clarification on these points.

OCR also proposes to define, for the purpose of information in an EHR, that "health-related information on an individual" mean all individually identifiable health information (IIHI) including not only clinical, but billing and other data. OCR notes that definition would be at least as broad as IIHI as defined in under the HIPAA Privacy Rule under Section 160.103[2].

**Comment:** IHII is a subset of data within the definition of PHI. This is different from the definition of (EHI contained in the ONC Information Blocking Rule, which is defined as ePHI contained in a designated record set as defined in Section 164.501[3].

Additionally, OCR proposes an earlier compliance timeline than what is finalized in the ONC Information Blocking Rule for electronic EHI transfer. **Creating conflicting regulations and**

[1] https://www.cdc.gov/phlp/docs/hipaa-ferpa-infographic-508.pdf

[2] Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:(1) Is created or received by a healthcare provider, health plan, employer or healthcare clearinghouse; and (2) Relates to the past, present or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual; and (i) That identifies the individual; or (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

[3] Designated record set means: (1) A group of records maintained by or for a covered entity that is:

(i) The medical records and billing records about individuals maintained by or for a covered healthcare provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals. (2) For purposes of this paragraph, the term record means any item, collection or grouping of information that includes protected health information and is maintained, collected, used or disseminated by or for a covered entity.

**requirements on the same topic is confusing, adds burden and will lead to uncertainty around compliance. CHIME urges OCR to work with ONC to harmonize the definitions and compliance timelines**.

Finally, we also request clarification from OCR on whether this includes release of practice notes – notes from a clinician or other staff member reminding the clinician to check something; we do not believe this should be included in the required information to be released. We are concerned that when a clinician has determined there is a patient safety issue (i.e., risk of suicide)

this policy will remove the clinical judgment concerning whether they should be released or not. And, if notes are to be released, will there be adequate time for clinicians to remove any items that present patient safety issues?

*Personal Health Application (PHA)*

OCR proposes to define for "Personal health application" (or "personal health app") as the following:

> *An electronic application used by an individual to access health information about that individual in an 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.*

OCR also states that PHAs are direct-to-consumer applications used for the individual's own purposes.

**Comment:** PHAs are not subject to HIPAA privacy and security obligations and, thus, can share patient PHI. While we support the definition of PHA, CHIME is concerned about the privacy implications of proposals in this proposed rule to require CEs to transmit EHI to PHAs without requiring those PHAs to include privacy controls. Furthermore, there are no controls in place like BAAs to help support privacy and security of patient information. How does OCR plan to ensure patient data is not used in ways not intended by patients? And, how will this work alongside more stringent state laws?

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

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

**Comment:** CHIME is generally in favor of this proposal, with some modifications. We appreciate the clarification that this proposal would not include allowing the individual to connect a personal device, such as a thumb drive, to the CE's information systems as this could pose a security risk.

CHIME is concerned with the following proposal to add: "When protected health information is readily available at the point of care in conjunction with a health care appointment, a covered health care provider is not permitted to delay the right to inspect." **We request clarification as we have several questions. First, would this include allowing patients to access PHI from previous visits/encounters? If so, CHIME urges OCR not to finalize this proposal as written as it could cause significant disruptions to workflow and increased wait times for all patients while such**

**in-appointment requests are fulfilled.** Second, presumably OCR does not envision a scenario in which patients could be peering at records that expose other patients' data (i.e., hovering over a computer screen or desk where other patient PHI could be seen. We seek clarification on how this would work. Last, does OCR envision that when clinicians need time to review previous cases and treatment pathways to help inform a treatment plan, they can do so prior to releasing a record? Again, presumably this would be permitted but we seek clarity on this point as well.

***OCR Requests Comment:*** On whether to require covered healthcare providers allow individuals to record PHI in this manner as part of the Privacy Rule access right; whether conditions or limitations should apply to ensure that a covered healthcare provider does not experience unreasonable workflow disruptions (e.g., limitations on time spent recording PHI in conjunction with a healthcare appointment); any potential unintended consequences of a new requirement to allow inspection of PHI that is readily available at the point of care in conjunction with a healthcare appointment; and how to determine when PHI is "readily available."

**Response:** CHIME strongly believes that there is not only a potential for disruption to provider workflow, but that this could also have a trickle-down effect in the sense that if more time is needed during the visit to accommodate these requests, then fewer patients can be seen. We ask OCR to ensure that such in-appointment requests are limited to the scheduled time of the appointment so as not to increase barriers to care for other patients who would then have to wait, and so as not to cut into the delivery of medical care to the current patient. We believe a more efficient use of the appointment – unless of course the information is easily accessible at the point of care – is not to require a provider to furnish records during a patient visit. **CHIME, therefore, recommends that "readily available," in this context, be designated to mean that the information is available in the patient room during the appointment and can be pulled up and reviewed within the time designated for the appointment.**

***OCR Requests Comment****:* On whether CEs should be permitted to provide copies of PHI in lieu of in-person inspection of PHI when necessary, to protect the health or safety of the individual or others, such as during a pandemic; and if so, whether the Department should establish additional rights for individuals in such circumstances, such as the right to receive such copies for free.

**Response:** CHIME requests that OCR permit reasonable delays in the instance that an in-person request has the potential to cause significant disruptions to workflow. We also strongly support permitting the provision of copies of PHI when necessary, to protect the health or safety of the individual or others. Fulfilling Individual Right of Access requests should not require anyone to be put in harm's way. CHIME suggests that the fee for such copies be dependent on the form and format requested, as other requests are under the Individual Right of Access request fee schedule.

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

*Requests for Access*

OCR proposes to modify the rule to expressly prohibit a CE from imposing "unreasonable measures" on an individual exercising the right of access that it creates a barrier to or unreasonably delays an individual from obtaining access.

**Comment:** CHIME agrees that providers should create unnecessary obstacles for patients seeking to access their medical records. We are concerned, however, that we are being asked to provide comment on this proposal prior a definition of "unreasonable" being established. OCR gives examples of what they believe to be unreasonable, but, OCR has not proposed a definition. There

are situations that providers routinely encounter that require additional effort on the part of the provider before the records can be released. For instance, while OCR cites as an example as a barrier "unreasonable identity verification," there are indeed situations like legal disputes, custody disputes and cases involving minors that can often take longer than a standard request. Additionally, in the case of clinical research, often times there is raw data that must go through review by an Institutional Review Board (IRB) for approval, peer review and others before being curated as accurate. As such, in addition to further clarification needed on what is "unreasonable," CHIME requests assurances that providers be given adequate time to resolve identity issues and other issues which may arise in more complex access request cases.

*OCR Requests Comment*: on whether a prohibition against "unreasonable measures" would result in adverse consequences for individuals or significant burdens on CEs (must include examples).

**Response:** CHIME believes that cases involving legal disputes, minors, conservatorship and unclear custody will require additional documentation and identity verification. We request exceptions be established for complicated cases.

*Timeliness*

Current OCR policy allows individuals to request access to or copies of their PHI in a designated record set and that individuals may be required to make this request in writing. It furthermore requires access be granted within 30 days allowing for one, 30-day extension be permitted. OCR proposes to require access be provided by a CE to an individual "as soon as practicable" but in no case later than 15 calendar days after receipt of request with the possibility of one 15 calendarday extension. OCR also states that requests for clarification from the CE to the individual would not extend the timeline or reset the clock on requests.

OCR further proposes to require CEs to establish written policies for prioritizing urgent or other high priority access requests (especially those related to health and safety) so as to limit the need to use the 15 calendar day extensions for such requests.

**Comment:** CHIME agrees that, in most standard cases, 15 calendar days is sufficient time to fulfill an individual request of access. However, we note that there are several instances in which this would be insufficient and thus may take longer than the proposed 15 calendar days plus one 15-day extension allows. Additionally, shortening the timeframe from 30 days to 15 days will continue to add costs to an already very strained process system and could lead to inadvertent, inappropriate releases of information due to foreshortening the due diligence processes. Situations that may necessitate more time include, but are not limited to, the following:

- Legal requests
- Requests involving minors, particularly in cases in which there is child abuse or a custody dispute, as these requests generally require additional documentation and identity verification
- Cases involving conservatorship proceedings
- Instances in which a small or under-resourced provider, one that cannot afford a separate medical records department, or is temporarily closed due to vacation or other extenuating circumstances
- Cybersecurity incidents which render access to medical records infeasible
- Natural disasters and pandemics which could create unforeseen delays

Therefore, CHIME requests that exceptions be allowed in exceptional cases, such as these.

CHIME is generally in favor of the proposal to require CEs to establish written policies for urgent and high priority requests. We also appreciate that OCR is not prohibiting using an extension for urgent / high-priority requests so long as they have a policy in place. We are concerned, however, that without a definition of urgent / high priority, and without a patient being asked the reason for the request, that everything can then be escalated under this rationale. We recommend the provider be allowed to ascertain what constitutes urgent or that OCR provide a concrete definition of what urgent and high-priority is.

**D. Addressing the Form of Access**

The Privacy Rule requires a CE to provide patients with access to their PHI in the form and format requested, if readily producible in that form and format. If this is not possible then the provider must provide the records in a hard copy form or any other form or format agreed to by the CE and patient. HHS is examining how best to address individuals' privacy and security interests when they use a PHA that receives PHI from a CE and has outlined several approaches. OCR has proposed that if a CE has a secure, standards-based API —such as one consistent with those required under Information Blocking policies, the agency has said they consider ePHI to be "readily producible." OCR has also said that a CE may require all applications to register before providing access via its secure API, and that doing so would not violate the form and format policy so long as the registration process did not exclude or prevent a PHA that was capable of securely connecting to the secure API from connecting.

**Comment:** CHIME agrees that regulations should be harmonized to minimize complexity of compliance. We do, however, have some questions and concerns with the proposal.

Concerning the term "readily producible," we have two comments. First, we are concerned that the term "readily producible" may be interpreted as being every possible data element is easily available and that is often not the case. As an example, we point to some of the APIs built to facilitate access to Medicare data via Blue Button. Medicare gives five years' worth of data, but Medicare does not provide every possible data element. As another example, some data is simply challenging to produce "on the spot," given how new the standards are. Examples of this type of data include but are not limited to radiology data, CAT scans and genomic data. Second, the term itself seems to suggest it's incautiously producible as if you are hitting the print button.

Separately, we also have questions around the app registration process. For instance, how does OCR envision this will work when providers find an app has been built by a nation state or actor that has been designated by the federal government as an entity we should not do business with? What will happen if citizens here download the app? Will providers still be required to share data with that app at the direction of the patient? Given the historic challenges faced by our sector with evergrowing cybersecurity threats, it's imperative that we do not jeopardize patient data or national security.

Finally, in that same vein, we question how is a provider to know which apps have standards-based and secure APIs? Will that responsibility fall to providers? And how will they know this about a vendor? Is OCR planning on maintaining a list of "good apps"?

*OCR Requests Comment*: on how best to address individuals' privacy and security interests when they use a personal health application (PHA) that receives PHI from a CE. The Department requests information about the costs and benefits of options for educating individuals in a manner that does not delay or create a barrier to access.

**Response:** PHAs – also referred to as third-party health apps – are not HIPAA-covered entities and, thus, can share patient protected health information without the requirement that they meet HIPAA privacy and security policies. CHIME has long expressed concerns about the treatment of health data by entities not governed by HIPAA. The regulatory oversight framework governing those covered by HIPAA and those who are not has created a separate and parallel but unequal universe which is at the heart of the privacy debate in healthcare. We have long contended that when a provider is mandated under information blocking policies to release a patient's data at their request, that there should be a requirement that the app disclose in plain English, up front:

1. Do you sell identifiable information?
2. If yes, is it used only for research?
3. Do you use the data for marketing?
4. What is your documented patient consent process?
5. Do you securely destroy data?

CHIME is concerned about the privacy implications of proposals in this proposed rule to require CEs to transmit EHI to PHAs without requiring those PHAs to include privacy and security controls. Most patients-turned-consumers are completely unaware of how an app intends to use their data and

---

many are under the false assumption that their data will continue to be safeguarded under HIPAA. Precious little attention, unfortunately, is being given to API security. According to a recent report of the 30 mobile health apps tested, 77% had hardcoded keys they don't expire and user-names and passwords that were also hard coded.

A study published in the *Journal of the American Medical Association (JAMA)*[4] found that many health apps created to track a user's progress in battling depression or quitting smoking are sharing the personal details they collect about an individual with third parties – like Google and Facebook – without the individual's knowledge or informed consent:

> *Transmission of data to third-party entities was prevalent, occurring in 33 of 36 top-ranked apps (92%) for depression and smoking cessation, but most apps failed to provide transparent disclosure of such practices. Commonly observed issues included the lack of a written privacy policy, the omission of policy text describing third-party transmission (or for such transmissions to be declared in a nonspecific manner), or a failure to describe the legal jurisdictions that would handle data. In a smaller number of cases, data transmissions were observed that were contrary to the stated privacy policies.*

If patients access their health data – some of which could contain family history and could be sensitive – through a smartphone, they must have a clear understanding of the potential uses of that data by app developers. **Most patients and clinicians will not be aware of who has access to the medical information, how and why they received it, and how it is being used.** For example, an app may collect or use information for its own purposes, such as an insurer using health information to limit/exclude coverage for certain services, or may sell information to clients such as to an employer or a landlord).

Finally, patients also must be able to easily use the app taking into consideration the Americans with Disabilities (ADA) Act and some providers are required to comply with the ADA for any app built or

---

[4] "Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation," April 19, 2019.

used. Providers must take care with presentation involving items such as color choices and multilanguage support.

The downstream consequences of data being used in this way may ultimately erode a patient's privacy and willingness to disclose information to his or her physician. OCR's proposal requires clinicians to transmit IIHI to PHAs without requiring that the PHAs include privacy or security controls. The technological capability to implement privacy and security controls exists, so by failing to require PHAs to implement them, the agency is making a deliberate policy decision to not

prioritize patient privacy. Additionally, we do not believe that the burden for educating patientsturnedconsumers on the risk of sharing their healthcare data should fall exclusively to providers.

*OCR Requests Comment*: On the following questions:

- Whether to require a healthcare provider that has EHR technology that incorporates a secure, standards-based API without extra cost, to implement the API?

**Response:** CHIME requests clarification from OCR on the anticipated timeline for this. In order to minimize conflicting regulations and simplify compliance, we request that, if any such requirement is imposed, it mirror the ONC Information Blocking timeline. In addition, we note that while OCR posits that an API may be free, the interfaces for each EHR system may not be free. As one member explains it, "there is no free lunch." Providers are still on the hook for monitoring the app and troubleshooting it. This burden is borne by providers. There are additional costs that may be

associated with API implementation and use that must be taken into account. If all costs amount to $0.00, CHIME would support such a requirement aligning with the ONC timeline.

- Whether to require a healthcare provider that could implement such an API at little cost to do so?

**Response:** As different practices have different abilities to absorb costs, this should be a practicelevel decision so as to avoid increasing barriers to care.

- How to measure the level of cost that would be considered a reasonable justification for not implementing an API?

**Response:** As stated above, different practices have different abilities to absorb additional costs. Because of this, this should be a practice-level decision. In addition, many practices took significant monetary losses during the COVID-19 public health emergency, making it even more difficult to absorb additional overhead and maintain practice solvency. It is also worth noting that the Information Blocking policies apply to providers who never qualified for EHR incentives under HITECH, which could create even great financial burdens for these other providers and impede care coordination across the care continuum.

*OCR Requests Comments:* Should a provider be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules.

**Response**: We do not believe that the burden for educating patients-turned-consumers on the risk of sharing their healthcare data should not fall exclusively to providers. This should be a shared

responsibility with the app developers. Additionally, other stakeholders like public health departments can also help with education.

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

The Right of Access policy allows an individual to transmit copy of their PHI to another person or entity when requested (a.k.a. third-party). This policy is totally separate from the one that allows a CE to send PHI to another entity under the Uses and Disclosures policy.

OCR proposes to create a separate set of provisions for the right to direct copies of PHI to a thirdparty. Specifically, OCR is proposing to expand an individual's right to:

- Direct only copies of PHI in an EHR to a third-party;
- Submit oral, electronic or written requests for a CE to transmit an electronic copy of PHI in an EHR to a designated third party; and
- Direct a healthcare provider or health plan to obtain electronic copies of their PHI in an EHR to a third party.

**Comment:** CHIME strongly urges OCR not to finalize this proposal. This proposal creates a second pathway, in addition to the permitted TPO disclosures, for a covered healthcare provider or health plan to obtain an electronic copy of PHI in an EHR from another covered healthcare provider through a required disclosure initiated by an individual in exercising their Right of Access.

CHIME is concerned that the provision requiring a healthcare provider to submit a request for and obtain electronic copies of PHI on behalf of a patient under the Right of Access pathway will significantly increase burden on and costs for providers by increasing the amount of paperwork and screen time per patient and creating no mechanism for reimbursement. This runs counter to HHS's *Patients Over Paperwork* initiative. Many of the provisions in this proposed rule will reduce the burdens on patients to have access to and to control their own health information. Healthcare providers, however, have hundreds of patients and the burden of this provision on providers will be substantial. If this provision is finalized, it would also require providers to furnish information without any extensions available.

In addition to creating burdens, there are some very serious concerns associated with the potential release to bad actors. This mandate will put providers in the untenable position of having to potentially release protected data to known and identified bad actors. For instance, if a hospital is attacked with ransomware at provider A and a patient visits provider B and requests their data be sent to provider A, who is liable for a data breach? Would provider B be charged with a breach if an unauthorized third party viewed the ePHI?

CHIME is in support of the remaining proposals regarding directing copies of PHI in an EHR to a third-party and allowing multiple methods for a patient to submit a request.

*OCR Seeks Comment:* on whether a Requester-Receiver should be permitted to refuse to submit a request for an individual in some cases (e.g., if it already has the requested information*)?*

**Response:** Yes. Healthcare providers should be permitted to refuse to submit a request for an individual if it already has the requested information or if the request, in combination with other requests and regulatory obligations, would be too burdensome for the provider to submit.

### F. Adjusting Permitted Fees for Access to PHI and ePHI

The current policy allows CEs to charge a reasonable, cost-based fee to fulfill access requests made by individuals for copies of their PHI. Current policy limits the allowable fees to the costs of: labor for copying (whether PHI in paper or electronic form); supplies for creating paper / electronic media; postage; and preparing an agreed upon summary of the PHI. HITECH expanded these rights to include individual directing access to PHI in an EHR to a 3rd party. The Department proposes to disallow covered entities from charging individuals for the costs of electronic media and postage when providing access by mailing copies of PHI in an EHR on electronic media.

OCR is proposing to change the permitted fees for access to PHI and ePHI to the following:

| Type of access | Recipient of PHI | Allowable fees |
|---|---|---|
| In-person inspection—including viewing and self-recording or -copying. | Individual (or personal representative). | Free. |
| Internet-based method of requesting and obtaining copies of PHI (*e.g.,* using View-Download-Transmit functionality (VDT), or a personal health application connection via a certified-API technology). | Individual ..... | Free. |
| Receiving a non-electronic copy of PHI in response to an access request. | Individual ..... | Reasonable cost-based fee, limited to labor for making copies, supplies for copying, actual postage & shipping, and costs of preparing a summary or explanation as agreed to by the individual. |
| Receiving an electronic copy of PHI through a non-internet-based method in response to an access request (*e.g.,* by sending PHI copied onto electronic media through the U.S. Mail or via certified export functionality) [129]. | Individual ..... | Reasonable cost-based fee, limited to labor for making copies and costs of preparing a summary or explanation as agreed to by the individual. |
| Electronic copies of PHI in an EHR received in response to an access request to direct such copies to a third party. | Third party as directed by the individual through the right of access. | Reasonable cost-based fee, limited to labor for making copies and for preparing a summary or explanation agreed to by the individual. |

**Comment:** CHIME opposes the proposal to eliminate the ability for CEs to charge for the costs of electronic media postage for providing electronic copies of PHI by any method. If an individual requires a paper copy, CEs are allowed to charge for supplies and postage because OCR recognizes that those costs, when summed over all requests, are non-trivial. Why then, when an individual requires PHI on a CD or memory stick, are the costs of supplies and postage considered trivial enough to prohibit charging a fee? CHIME strongly urges OCR to not finalize this proposal *Requests Comment:* on its view of the costs of providing access through an internet-based method, including any internet-based methods described in the ONC Cures Act Final Rule.

**Response:** Many her vendors charge fees for the use of APIs and for the volume of API transactions. These fees can be prohibitive, particularly to small practices.

## III. Reducing Identity Verification Burden for Individuals Exercising the Right of Access

Current OCR policy calls for CEs to take reasonable steps to verify the identity of a person requesting PHI before disclosure; however, the agency does not mandate a particular form of verification. Verification can be done orally, in writing, over the phone, by fax, email, portal, etc. using the CEs own form. Because OCR continues to get questions about verification, they are proposing to expressly prohibit a CE from imposing unreasonable identity verification measures on an individual (or his or her personal representative) when exercising their Right of Access under the Privacy Rule. OCR also proposes to clarify that unreasonable verification measures are those that require an individual to expend unnecessary effort or expense when a less burdensome verification measure is practicable for the particular CE.

**Comment:** CHIME generally supports these proposals except in special circumstances, including, but not limited to, the following:

- Legal requests;
- Requests involving minors, particularly in cases in which there is child abuse or a custody dispute, as these requests generally require additional documentation and identity verification; and
- Cases involving conservatorship proceedings.

In cases such as those above, additional information and identity verification would be required to ensure access is authorized and appropriate.

## IV. Amending the Definition of Health Care Operations to Clarify the Scope of Care Coordination and Case Management

OCR proposes to clarify the definition of healthcare operations to be "… population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment."

**Comment:** CHIME supports this proposal and appreciates the increased emphasis and value placed on case management and care coordination.

## V. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individuallevel Care Coordination and Case Management

OCR proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered healthcare provider for care coordination and case management. This would apply only for individual-level, not population-level requests.

**Comment:** CHIME supports this proposal and appreciates the increased emphasis and value placed on case management and care coordination.

## VI. Clarifying the Scope of CE's Abilities to Disclose PHI to Certain 3rd Parties for IndividualLevel Care Coordination and Case Management That Constitutes Treatment or Health Care Operations

OCR proposes to expressly permit CEs to disclose PHI to social services agencies, communitybased organizations, home and community-based services (HCBS) providers, and other similar third parties that provide health-related services to specific individuals for individual-level care coordination and case management, either as a treatment activity of a covered health care provider or as a healthcare operations activity of a covered healthcare provider or health plan. Under this provision a health plan or a covered healthcare provider could only disclose PHI without authorization to a third party that provides health-related services to individuals; however, the third party does not have to be a healthcare provider.

**Comment:** CHIME appreciates the need for care coordination, and acknowledges that HIPAA does not govern many entities with whom a patient interacts along their care journey. Increasingly, providers are addressing the social determinants of health (SDoH) aspects of population health, which means they coordinate care with entities such as those who oversee housing, legal aid and food banks. There is a tremendous challenge for providers in discerning who should and should not receive patient information. Under the OCR proposal, these judgment calls could be tested and inadvertently result in sharing in ways not intended or contemplated by the patient or situations where the downstream entity repurposes the patient's data, sells it or uses it for marketing purposes. We believe these uses would be contrary to OCR's intention. To quote one of our members, "It also shouldn't be a surprise that a local food bank is providing aid to a patient in a food desert as part of

managing diabetes and addressing health disparities." We, therefore, recommend that OCR clarify that information could be shared by CEs if the intended sharing is outlined in the patient's plan of care and or treatment plan process.

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

*Judgment Standards*

OCR makes the case that family members, friends and caregivers are a critical component to helping people who suffer from substance abuse disorder (SUD) and mental illness. There remains fear among providers that sharing information about these patients will violate HIPAA. In order to ameliorate these concerns and to best support patients, OCR proposes to amend five provisions of the Privacy Rule to replace "exercise of professional judgment" with "good faith belief" as the standard pursuant to which covered entities would be permitted to make certain uses and disclosures of PHI in the best interests of individuals. These five provisions include: 1) disclosures to personal representatives; 2) uses and disclosures requiring an opportunity for the individual to agree or object; 3) identity verification; 4) uses and disclosures to avert a serious threat to health or safety; and 5) relevant guidance encouraging disclosures of PHI to help individuals experiencing opioid use disorder or mental illness. Additionally, OCR also proposes a presumption that a CE has complied with the good faith requirement, absent evidence that the covered entity acted in bad faith.

**Comment:** CHIME appreciates the need for caregivers, family members and friends to be involved with the care of a loved one suffering from SUD. We are concerned, though, **that the change in the standard from "professional judgment" to "good faith below" could have unintended consequences in how the change could be implemented.** While good faith belief does rely on a set of circumstances and intuition, it may be difficult to maintain consistency across the care continuum, while relying on professional judgment centers on professional expertise. Professional expertise, in general, should carry across the nation and provider settings as all providers are held to a licensing-based set of standards and training. While we therefore appreciate that OCR will presume that a CE has complied with the good faith requirement, barring any evidence to the contrary, we nonetheless recommend that if the agency moves to adopt this new standard, that there is clear definition of what constitutes good faith.

*Threat Standards*

Within the proposed rule, OCR proposes an amendment to the Privacy Rule replacing the "serious and imminent threat" standard with a "serious and reasonably foreseeable threat" standard, allowing providers more flexibility in invoking the threat standard at the time of PHI disclosure and the reasonableness of the threat determination. Finally, OCR also proposes a non-substantive revision to change "preventing or lessening a threat" to "preventing a harm or lessening a threat."

**Comment:** CHIME agrees with the additional flexibility granted by OCR as it relates to altering the threat standard to serious and reasonably foreseeable threat. This change also brings the HIPAA Privacy Rule requirements more in line with the standards outlined in the Office of the National Coordinator for Health Information Technology's (ONC) information blocking rule preventing harm exception. While we appreciate the additional flexibility, CHIME requests OCR provide additional clarity on the definition for preventing a harm or lessening a threat. Clinical members of CHIME indicated – especially when it comes to substance use disorder – that threat and harm are often not considered the same and, thus, have different standards of concern for patient safety. Providing

additional clarity on these terms in this specific use will help providers better comply with requirements, use the granted flexibility and protect patients. Conversely, if OCR is unwilling to define the terms further, we recommend they defer to the judgment of providers.

*Requests for Information: Impact of Judgment and Threat Information Request Standards*

Within the proposed rule, OCR asks several questions related to how the changes in information request standards may impact patients and physicians in both how care is sought and received, and asked for comment on when the rules should be viewed more leniently or stringently.

**Comment:** CHIME believes many of these proposed changes within the Privacy Rule would be too nuanced for patients to fully grasp or even be cognizant of in practice. With that in mind, it is crucial for OCR to review and understand whether the proposed changes would potentially hurt or hinder the patient's ability to receive care, especially for SUD, since, in large part, patients may not even be aware they need to make a decision themselves. Many of the changes place the burden on providers to make what are, at times, highly nuanced decisions that will often fluctuate on a casebycase basis. This creates a scenario in which providers are vulnerable to malpractice and other legal challenges to their decision making. With this understanding, **CHIME urges OCR to ensure this and future policy changes move away from focusing on the risk to the provider and prioritizes patient care with clear and concise regulations all will be able to implement without question.** Furthermore, because providers are often faced with making decisions on the spot, it is imperative that OCR defer to the judgment of the provider barring any compelling evidence to the contrary.

As it relates specifically to SUD treatment, CHIME members believe these additional flexibilities will allow providers the ability to protect or trigger data releases to protect patients. This includes allowing providers to increase the use and strengthen the value of prescription drug monitoring programs to highlight instances of threat or harm such as adverse drug reactions and doctor shopping. While CHIME views these as positive changes that prioritize patient care and gives covered entities additional protections, the shift places additional subjectivity into the medical decision-making process and, thus, unintentionally increases risk to the provider. We recommend that OCR again defer to the clinician's judgment.

Finally, while OCR considers finalizing these changes, **CHIME recommends the agency focus its education and implementation on educating CEs on how these new changes interact with state laws.** Many states have similar or more stringent privacy protections for patients and these broad changes increase the likelihood both patients and CEs could struggle to understand their intersection. The same eye to clarity must be given to how these proposed changes interface with the ONC information blocking policies that took effect on April 5, 2021. Both this proposed regulation and ONC's final regulation center on the release of data and both feature sections on preventing patient harm and threat; thus, it is crucial for ONC and OCR to work together to clarify what is and is not allowable under both pieces of rulemaking. CHIME also requests OCR utilize the ongoing revision to 42 CFR Part 2 to provide additional clarity on how these Privacy Rule changes specifically impact the treatment and care of substance use disorder.

## VIII. Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgement of Receipt, Establishing an Individual Right to Discuss the NPP with a Designated Person, Modifying the NPP Content Requirements, and Adding an Optional Element

Current OCR policy requires providers to make a good faith effort to obtain a written acknowledgment of receipt of the provider's Notice of Privacy Practices (NPP). OCR proposes to

eliminate the requirements for a CE to obtain a written acknowledgment of receipt of the NPP and to remove the current requirement to retain copies of such documentation for six years. OCR proposes to replace the written acknowledgment requirements with an individual right to discuss the NPP with a person designated by the CE.

**Comment:**

CHIME supports these changes. We agree that removing the requirement to furnish a paper copy of the NPP will reduce the administrative burden significantly on providers and will reduce healthcare spending. In a survey of our members, we asked about the burden of obtaining written acknowledgment of NPP by patients and our members responses indicate that the NPP is of little value and is a costly mandate.

In addition, our members indicated that, other than for legal purposes, they had no use for these signed paper NPPs.

*OCR Requests Comment:* for how best to impart to individuals how health information can be used and disclosed under the healthcare operations permission in the model NPP.

**Comment:**

We believe this information can be conveyed a number of different ways, including but not limited to patient portals, websites and posting this inside the walls of the provider (i.e., clinical room), and during the intake process. ***Conclusion***

CHIME appreciates the opportunity to offer our feedback on this Proposed Rule and stand ready to have a longer dialogue on any of the topics discussed in our letter. Should you have any questions, please contact Mari Savickis, vice president of public policy, at mari.savickis@chimecentral.org.
Sincerely,

Russell P. Branzell, CHCIO, LCHIME
President and CEO
CHIME

John Kravitz, CHCIO, MHA
Chair, CHIME Board of Trustees
Chief Information Officer
Geisinger Health System