



233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

March 22, 2021

Acting Director Robinsue Frohboese
US Department of Health and Human Services
Office for Civil Rights
Hubert H. Humphrey Building
Room 509F
200 Independence Avenue, 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 NPRM

Submitted electronically via www.regulations.gov

Dear Acting Director Frohboese:

Thank you for the opportunity to provide comments on the *Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement Notice of Proposed Rulemaking (NPRM)*.

AHIMA is a global nonprofit association of health information (HI) professionals. AHIMA represents professionals who work with health data for more than one billion patient visits each year. AHIMA's mission of empowering people to impact health drives our members and credentialed HI professionals to ensure that health information is accurate, complete, and available to patients and clinicians. Our leaders work at the intersection of healthcare, technology, and business, and are found in data integrity and information privacy job functions worldwide.

AHIMA commends the Office for Civil Rights' (OCR) intention to address current barriers to care coordination and case management, as well as other regulatory burdens that do not necessarily lead to greater protection of patient privacy. In particular, we appreciate OCR's intent as part of this rule to enhance individuals' access to their health information. AHIMA supports the right of individuals to access their accurate and complete health information in a timely manner. The ability of individuals and their caregivers to access, exchange, and use their health information is essential to managing their care. Today, nearly all hospitals provide patients with the ability to electronically view and download their health information.¹ However, despite these technological advances and the right of individuals to access their health information under the Health Insurance Portability and Accountability Act (HIPAA), individuals continue to struggle with accessing their health information in a manner that is seamless, timely, and electronic.

AHIMA offers comments on the following high-level issues, in addition to more detailed comments regarding certain aspects of the proposed rule.

¹ Available at: <https://www.healthit.gov/sites/default/files/page/2019-04/AHApatientengagement.pdf>.

Alignment with ONC Cures Act Final Rule

In general, AHIMA is concerned that while certain aspects of this proposed rule align with the requirements of the ONC Cures Act Final Rule, other provisions could benefit from greater harmonization. We are concerned that in the current state, lack of further harmonization could lead to additional confusion among stakeholders between the requirements of the two rules, leading to many thinking that they must violate one rule to comply with the other, which is clearly not the intent of either of these rules. We encourage OCR to continue to work with ONC to harmonize these rules further. Additionally, we recommend OCR and ONC consider developing a crosswalk from the HIPAA Privacy Rule to the ONC Cures Act Final Rule to provide assistance to stakeholders seeking to comply with both rules.

More specifically, we are concerned about the unintended consequences of the designated record set being a key component of the definition of electronic health information (EHI). What was originally intended as a means to clarify the scope of an individual's right to access, amend, restrict and acquire an accounting of disclosures, has become, under the ONC Cures Act Final Rule, what an actor must be able to access, exchange and use for purposes of information blocking. However, despite being defined in regulation and [guidance](#), the definition of the designated record set is expansive, and covered entities are generally left to define for themselves which records are part of their designated record set. As a result, there is variation and discrepancy in how healthcare organizations interpret their designated record set, which has led to longstanding inconsistencies and confusion for covered entities and business associates over how to comply with the HIPAA Privacy Rule. Furthermore, there are aspects of the definition, such as 45 CFR 164.501(1)(iii), which includes records that are used, in whole or in part, by or for a covered entity to make decisions about individuals. This raises the question of whether a wide variety of information may be considered part of the designated record set, (as well as EHI), including unverified external records that may be used in clinical decision support algorithms. We encourage OCR to work with ONC and review the definition of the designated record set in light of this new definition of EHI, as well as new use cases. We also encourage OCR to consider providing additional guidance as to how the designated record set may be further understood through the lens of the ONC Cures Act Final Rule.

For the last several months, AHIMA, the Electronic Health Records Association (EHRA) and the American Medical Informatics Association (AMIA) have been working together to develop consensus recommendations/guidance among HI, health informatics, and health IT professionals on how best to translate policy concepts related to the designated record set and the definition of EHI into technical guidance for operationalization in an electronic environment. While this work is ongoing, we agree that it could be beneficial to develop a set of rules that could guide actors as to when ePHI would not be considered part of the designated record set. Examples of when ePHI may not be considered part of the designated record set could include when: (1) ePHI is considered unvalidated, (2) ePHI is a "work in-progress," "in draft form," or "not yet final," such as an audio file of a transcription, (3) state and federal record retention requirements have expired on the ePHI or (4) the ePHI was not used in medical decision-making. Some of these rules will likely require further clarification from both OCR and ONC based on existing guidance; however, we believe the development of such rules/guidance could assist actors under the ONC Cures Act Final Rule. We welcome the opportunity to meet with OCR and ONC to discuss this work further.

Enforcement Discretion During Public Health Emergency

As the COVID-19 pandemic continues, health information professionals continue to be stretched in terms of time and resources, limiting our members' ability to adequately prepare for the compliance date of this rule once it has been finalized. This challenge is compounded by the fact that in addition to the pandemic, many health information professionals are currently focused on preparing for the compliance date of the ONC Cures Act Final Rule. At the same time, we recognize that a number of recommendations made in this proposed rule could not only enhance care coordination and case management but enhance the ability of patients to gain access to their health information—two goals that are incredibly important during this pandemic. For that reason, should OCR finalize this proposed rule during the public health emergency, we recommend that the agency consider a period of enforcement discretion until the public health emergency ends. This would allow health information professionals to begin to revise existing policies and procedures as well as institute education and training on the final rule without fear of incurring penalties for noncompliance.

III. Need for the Proposed Rule and Proposed Modifications

A. Individual Right of Access (45 CFR 164.524)

1. Adding Definitions for “Electronic Health Record” or EHR and “Personal Health Application” (45 CFR 501)

OCR proposes to clarify the definition of “electronic health record” (EHR) in the HITECH Act. OCR proposes the definition of EHR to mean, “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 by §164.501, such as physicians, nurses, pharmacists, and other allied health professionals.”

AHIMA is concerned that the definition of EHR as currently proposed is too narrow. For example, while the preamble states that electronic healthcare billing information would be included as part of the proposed definition of EHR because it is health-related information, it is not entirely clear based on a plain-reading of the definition itself. Furthermore, we are concerned that the proposed definition of EHR could cause confusion given other definitions of EHR currently in existence, including the term “certified EHR technology” as used by CMS. Adding another definition of EHR may not only lead to misinterpretation of the rule but also create additional complexity as health information professionals are currently trying to navigate compliance with the ONC Cures Act Final Rule, CMS Promoting Interoperability Program, the HIPAA Privacy Rule, as well as state law. Furthermore, in some instances today there is both clinical and administrative data in the EHR that would not be considered part of the designated record set – these include subpoenas and other communications not used for medical decision-making. However, under this proposed definition, covered healthcare providers would be required to provide such information to a third party. We are also concerned and seek clarification as to whether certain types of information, including social determinants, would be included under this narrow definition even though they might be used to help make medical decisions about the individual. For consistency and administrative clarity, AHIMA recommends that OCR align the definition of EHR to the scope of paragraphs (1)(i) and (2) of the definition of the designated record set.

AHIMA is also concerned about the unintended consequences of narrowing the scope of “authorized health care clinicians and staff” to covered healthcare providers that have a direct treatment relationship with individuals. We seek clarification as to whether PHI from covered healthcare providers that have an indirect treatment relationship with an individual, such as radiologists, would be considered part of the proposed definition of the EHR. Often times, information or reports from an indirect covered healthcare provider will flow immediately into the EHR without the covered healthcare provider with the direct treatment relationship having to document such information in the EHR. For that reason, we ask that OCR offer additional illustrative examples of covered healthcare providers that have an indirect treatment relationship with individuals where information flowing from such providers would not necessarily be considered part of the EHR.

OCR proposes a new definition, “personal health application.” OCR proposes to define a personal health application (PHA) as an “electronic application used by an individual to access health information about that individual in electronic form, which can be drawn from multiple sources, provided that such information is managed, shared, and controlled by or primarily for the individual, and not by or primarily for a covered entity or another party such as the application developer.” OCR requests comments the types of activities encompassed in the terms, “managed,” “shared” and “controlled.”

AHIMA supports the definition of a PHA as we believe it will create additional clarity for health information professionals in distinguishing services that truly stand in the shoes of the individual versus a request from a third party that requires an individual’s authorization to obtain copies of PHI. That said, AHIMA is concerned about the ongoing challenge of distinguishing a “true” individual access request versus a request made by a third party under the right of access that should require an individual’s authorization. The inability to distinguish between these two types of requests continues to challenge HIM departments and often requires additional follow-up with the individual to confirm whether they have directed the third party to request their PHI.

We also seek clarity as to whether a PHA would include an electronic application that is managed, shared, and controlled by an employer on behalf of the individual. We also ask that OCR shed further light on whether the definition of PHA is intended to contemplate online tools, platforms, and services that meet the functional capabilities of a PHA but are not necessarily considered an “application.”

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

OCR proposes to require covered entities to allow individuals to take notes, videos, and photographs using personal resources after arranging a mutually convenient time and place for the individual to inspect their PHI including points of care where PHI in a designated record set is readily available for inspection by the patient.

AHIMA supports the right of individuals to inspect their PHI, however, we have concerns regarding how this provision might be operationalized in a manner that minimizes provider burden and maintains patient privacy. For example, this proposed requirement will require additional training and education of all staff to ensure that a patient is only recording their own PHI. For requests made during the point of care, we are concerned that such a requirement could lead to workflow disruptions, taking providers away from their operational purpose because responding to access requests are not always in the clinical workflow. We are also concerned about the potential for liability to a covered entity when certain elements of PHI have not been incorporated into the record yet (e.g.—lab values, imaging, etc.) and an individual takes a photo and/or video of their PHI which in turn, is relied upon for care by

another provider. Additionally, we seek clarity on whether covered healthcare providers would be allowed under this provision to object if an individual's recording and/or photograph includes the provider.

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

b. Proposals

i. Requests for Access

OCR proposes to expressly prohibit a covered entity from imposing unreasonable measures on an individual exercising their right of access that creates a barrier to or unreasonably delays the individual from obtaining access.

AHIMA supports OCR's proposal to prohibit the imposition of unreasonable measures on an individual exercising their right of access that creates a barrier or unreasonably delays the individual from obtaining access, and we believe this is consistent with OCR's 2016 Access Guidance. We appreciate that OCR includes in regulatory text a non-exhaustive list of examples of reasonable and unreasonable measures that covered entities have used to delay access. We encourage OCR to list as many unreasonable measures as possible to assist stakeholders in making sure their policies do not conflict with the proposed requirements. Additionally, we suggest that OCR identify in regulation reasonable measures including the use of electronic signatures which we have seen as a frequent barrier to access used by covered entities that prohibit its use despite its permissive use under the HIPAA Privacy Rule.

ii. Timeliness

OCR proposes to require that an individual must be provided access to their PHI no later than 15 calendar days. If state law requires a covered entity to provide access in less than 15 calendar days, the shorter timeline applies. OCR also proposes that if a covered entity is not able to provide the individual with access to their PHI within the 15 days, the covered entity may use one 15-calendar-day extension if it has done the following: (1) notified the individual via written statement of the reasons for the delay and the date by which it will complete the request and (2) that it has established a policy to address urgent or high-priority requests.

AHIMA supports OCR's intent to require a uniform standard for PHI that is maintained by covered entities in electronic and non-electronic format. However, some of our members who still operate in a hybrid electronic/non-electronic environment are concerned that 15 days would a difficult target to meet when processing certain requests, including those that may require travelling to off-site storage to retrieve an individual's PHI. We are also concerned about the varying timeliness requirements under the HIPAA Privacy Rule, the ONC Cures Act Final Rule, the CMS Promoting Interoperability Program, and state law. Such variability creates an additional layer of complexity that could lead to confusion and unnecessary delays when individuals are seeking access to their PHI. We ask that OCR work with ONC and CMS to further harmonize these timelines as much as possible to limit confusion and complexity.

AHIMA supports the proposed requirements associated with a covered entity being able to take advantage of a 15-calendar-day extension. However, we encourage OCR to offer additional examples of

what may constitute an urgent or high-priority request to assist covered entities in the development of their policy around such requests.

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

b. Proposals

OCR proposes that a covered healthcare provider would be required to respond to an individual's request to direct an electronic copy of PHI in an EHR to a third party when the request is "clear, conspicuous, and specific," which may be orally or in writing.

AHIMA recognizes and appreciates that a request that is "clear, conspicuous, and specific" is consistent with the original intent of section 13405(e) of the HITECH Act. However, we ask that OCR consider providing illustrative examples or additional guidance as to what types of requests might or might not be considered "clear, conspicuous, and specific." Such examples would be helpful to ensure that covered entities are not putting up roadblocks to prevent individuals from accessing their PHI.

AHIMA is also concerned about how an oral request by an individual to direct an electronic copy of PHI in an EHR to a third party may be operationalized. In other words, if a request by a third-party designee is made verbally, how might a health information professional validate that the request was handled correctly? We are concerned that not only could such requests get lost and go unfulfilled, but should such an event occur, how health information professionals will be able to identify where compliance broke down in the process to avoid such an occurrence in the future. Furthermore, we are concerned that requiring covered entities to process verbal requests from third party designees raises the potential for abuse by third parties. In the past, this concern was minimized by requiring an authorization when a third party requested an individual's PHI because it could be clearly documented that the covered entity received the individual's authorization. Should a covered entity be required to rely on a verbal request from a third party, it is unclear how the covered entity will be able to know whether the request truly came from the individual. HIM departments already struggle with deciphering whether a third-party request is at the individual's direction when such requests are made in writing —how will such validation occur when such requests are made verbally? We will also note that these concerns are not lessened with OCR's proposal to require a provider or plan to facilitate a request for an individual's PHI when that request is submitted by another covered entity.

AHIMA also seeks clarification on whether, proposed 45 CFR 164.524(d)(1), is consistent with section 13405(e) of the HITECH Act which includes all covered entities, including health plans.

OCR proposes a requirement within the right of access that if an individual makes a clear, conspicuous, and specific request that his or her covered healthcare provider or health plan ("Requester-Recipient") obtain an electronic copy of PHI in an EHR from one or more covered healthcare providers ("Discloser"), the Requestor-Recipient would be required to submit the individual's request to the Discloser as identified by the individual.

AHIMA recognizes this proposed requirement offers a second mechanism (in addition to the permitted disclosure for TPO) for a covered healthcare provider or health plan to obtain an electronic copy of PHI in an EHR from another healthcare provider through a required disclosure initiated by an individual's exercise of the right of access. However, we are concerned about the benefit of this proposed provision vis a vis the administrative burden for a covered entity.

We also seek clarification as to whether the individual or the Requester-Recipient would be responsible for reporting to OCR the Discloser's failure to provide an electronic copy of the individual's PHI.

6. Adjusting Permitted Fees for Access to PHI and ePHI

b. Proposal

OCR proposes that a covered entity may not impose a fee when: (1) an individual inspects their PHI by taking notes, photographs or uses other personal resources to record the information or (2) an individual accesses ePHI maintained by or on behalf of the covered entity using an internet-based method. (e.g.--using the covered entity's certified health IT or a personal health application.)

AHIMA agrees with OCR's proposal to not permit a covered entity to impose a fee when an individual inspects their PHI or uses an "internet-based method" to view, capture, or obtain an electronic copy of their PHI. However, we would like to offer perspective on OCR's assumption that "access through an internet-based method likely occurs without involvement of a covered entity's workforce members." In today's production environment, human intervention is still very much required, especially when using patient portals. Such intervention might include pushing a patient's PHI into the portal or undertaking data integrity processes to ensure that an individual is matched correctly to their health information when creating a portal account. We are not suggesting that patients should bear the burden of these costs. Rather, we want to share our perspective that there still exists workforce involvement when facilitating an individual's access to their electronic PHI. Indeed, our hope is that these complex workflow processes will continue to be streamlined and automated with the advancement of modern technical standards, including the use of application programming interfaces (APIs). We will continue to support policies that intend to leverage such modern technical standards in ways that maintain the privacy, confidentiality, and security of an individual's PHI.

7. Notice of Access and Authorization Fees

OCR proposes how different types of access and recipients of PHI would affect the proposed allowable access fees. The chart on page 6465 of the proposed rule outlines the proposed fees.

It is our understanding that the proposed rule divides the right of access into different "sub-rights," including the right to inspect, the right to access PHI regardless of format and source (which includes the right to direct PHI to a PHA), and the right to direct PHI in an EHR to a third party. AHIMA is concerned that with the creation of these distinctions, it may be more challenging for health information professionals to identify which fee provisions apply to which types of access. We encourage OCR to develop additional educational materials to help individuals and covered entities navigate this environment to ensure that individuals do not experience undue delays in accessing to their PHI. A chart AHIMA developed with Ciitizen can be found in **Appendix 1**.

9. Request for Comments

b. Whether an electronic record can only be an EHR if it is created or maintained by a healthcare provider, or whether there are circumstances in which a health plan would create or maintain an EHR?

As healthcare continues to move towards value-based care models and enhanced care coordination, we see the traditional lines of providers and payers becoming increasingly blurry. Increasingly, payers are

exploring new opportunities to integrate value-based care with personalized approaches that take on more of a provider role than previously contemplated.² As such, some plans appear to be exploring the development of platforms that would allow multidisciplinary care teams to access a member's entire medical history as well as integrated clinical workflows. Such developments raise the question of how such platforms really differ from a covered healthcare provider's EHR and whether plans should be included in the proposed definition of the EHR. We recommend that OCR review these new types of platforms and consider whether plans should be included in the definition of EHR.

k. What types of activities should be encompassed in the terms, “managed,” “shared” and “controlled” in the proposed definition of personal health application, and whether other terms would improve the clarity of the definition?

AHIMA recommends that OCR provide further guidance as to what types of activities might be encompassed in the term, “managed,” “shared,” and “controlled.” Such guidance will assist health information professionals in identifying and processing requests from a personal health application. Activities that might typify whether the information is managed, shared, or controlled by or primarily for the individual might include: (1) whether the PHA can be used by the individual to make decisions about the individual’s health, wellness or health care and includes functionalities to facilitate those purposes, (2) whether an individual determines the rights of access and consents to whether the information is shared, (3) whether an individual opens a PHA account on their own or by their personal representative, and (4) whether an individual has the ability to shut down the account and take their information with them.

o. Whether a covered healthcare provider should 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. What are the benefits or burdens of different approaches?

In general, AHIMA believes that federal privacy and security baseline standards should be developed for the protection of health information held by data holders [outside of the scope of HIPAA](#). We recognize that adoption of such standards may require congressional action which is outside the scope of this rulemaking. However, the fact that an increasing number of consumer-facing technologies, applications, products, and services that access, produce, and manage health information are not bound by or required to abide by the rules established under HIPAA raises serious concerns about the extent to which an individual’s electronic health information is kept private and secure. That said, requiring covered healthcare providers to inform individuals of the privacy and security risks when requesting their PHI be transmitted to the individual’s PHA (which may not be covered by HIPAA) may be overly burdensome. Several operational considerations must be taken into account when considering such an obligation, including whether a covered healthcare provider would be required to prove the individual was informed of the risks, as well as how they may prove such a warning took place. Other questions that arise include whether a covered

² Available at: https://www.fiercehealthcare.com/payer/humana-to-pilot-new-tech-enabled-chronic-care-management-platform?utm_medium=nl&utm_source=internal&mrid=111895214&mkt_tok=eyJpljoiTnpneVl6YzFOakI5WldWaCIsInQiOjXQkxBcm1laFdRWGFTDZNRTRwZjNza1FwUExGT280aVB6QTk5am1rbDRFR1gydmFxeEplMzE0bDlxUVKZIFlaBMeUpkTWNhcGh5VW9WUUUpLTEVYbDBaUVNTZ3J0UW5ZWGQ4TVB2a1FONkppQVJtXC9oZFwvc2pRXC80c0s2ZzdkYUtKTlpvRHBoazRMSU5iNIRreG1Ecmc9PSJ9

healthcare provider would be required to wait to transmit an individual's PHI to a PHA until the patient agrees to accept such privacy and security risks.

In our [comments](#) to CMS regarding the Provider Burden and Prior Authorization proposed rule, we supported CMS' proposal to require plans under CMS' authority to implement and maintain a process for requesting a privacy policy attestation from a third-party application developer that is requesting to retrieve a patient's health information via the Patient Access API. Such an attestation process may not only provide individuals with a better understanding of how their health information may be used by a third party application developer, but also offer an informed choice to individuals as to whether they want their health information to be shared with a third party application depending upon the application developer's attestation. However, we noted that CMS should not be overly prescriptive in terms of how plans could implement such a process. Should OCR decide to adopt a similar attestation process, we reiterate that such a process should not be overly prescriptive as to become unduly burdensome on covered healthcare providers. Rather, we believe nonprofits and industry third parties could play an important role in assessing and helping application developers attest that they have established a minimum set of privacy and security provisions to be compliant with this requirement.

p. Should any potential education, notice, or warning requirement apply only to healthcare providers or also to health plans?

Any potential education, notice, or warning requirement should apply to all covered entities that are contemplated under 45 CFR 164.524. We believe it makes sense to require plans to institute such a requirement given the API requirements under the CMS Patient Access and Interoperability Final Rule. Additionally, if OCR were to adopt an attestation approach, such a requirement would also be consistent with what certain plans under CMS' authority may be required to adhere to under the CMS Provider Burden and Prior Authorization rule.

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

2. Proposals

OCR proposes to expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual or their personal representative exercising a right under the Privacy Rule. 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 covered entity.

AHIMA supports the prohibition of unreasonable identity verification measures on an individual or their personal representative when exercising a right under the Privacy Rule. We also encourage OCR to provide additional examples of unreasonable verification measures.

3. Request for Comments

a. Please describe any circumstances in which individuals may have faced verification barriers in exercising their Privacy Rule rights, as well as examples of verification measures that should be encouraged as convenient and practicable, in comparison to those that should be prohibited as per se unreasonable.

AHIMA encourages OCR to work with ONC to encourage the use of multi-factor authentication (MFA) as a means to authenticate an individual's or their personal representative's identity. We believe that greater adoption of MFA for identity management will also help to streamline existing complex release of information processes to further facilitate individuals' access to their PHI.

b. What verification standard should apply when a covered healthcare provider or health plan submits an individual's access request to another covered healthcare provider or health plan? Specifically, should the covered entity that holds the requested PHI be required to verify the identity and authority of the covered entity that submitted the request, but be permitted to rely on the requesting entity's verification of the identity of the individual (or personal representative?)

AHIMA believes that a covered entity that holds the requested PHI should be required to verify the identity and authority of the covered entity that submits the request, but should be permitted to rely on the requesting entity's verification of the identity of the individual or their personal representative. To require a covered entity holding the requested PHI to verify the identity of the individual or personal representative would be burdensome and incredibly difficult to manage from a release of information perspective.

e. Whether a different identity verification standard should apply when an individual requests access, as compared to when a personal representative requests access on the individual's behalf.

AHIMA does not believe a different standard for a personal representative requesting access on the individual's behalf is necessary given that typically the personal representative has already provided proof that they are authorized under State or other applicable law that they may act on behalf of the individual in making healthcare related decisions. To require a different identity standard for a personal representative when making an access request would be duplicative. Furthermore, should a different identity verification standard apply when a personal representative requests access on the individual's behalf, we recommend that OCR not prescribe the identity verification standard requirements but rather leave it to the discretion and professional judgment of the covered entity.

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

2. Proposal

OCR proposes to clarify the definition of healthcare operations to encompass all care coordination and case management by health plans, whether individual-level or population based.

AHIMA supports the clarification of the definition of healthcare operations, we believe that this clarifies for covered entities and individuals which Privacy Rule standards apply to which care coordination and case management activities. We also believe this clarification is necessary to further enhance care coordination and case management at the individual and population-based level.

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))

2. Proposal

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 activities at the individual level.

AHIMA supports the 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 activities at the individual level. We believe that this express exception is a logical extension to allow covered healthcare providers and health plans to better coordinate and manage patient care across different care delivery models. However, with this proposed provision, we are concerned about the operational feasibility of a covered entity being able to agree to a request by an individual to restrict disclosure of PHI to a health plan under 45 CFR 164.522(a)(vi) when the PHI pertains to a healthcare item or service that the individual has paid the covered entity in full. In other words, given how the data is currently structured, it would be difficult to parse the PHI the individual does not want shared with a health plan. The ability of individuals to opt-out of the sharing of certain pieces of PHI is difficult as such granularity is not necessarily possible with all health IT systems.

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 Healthcare Operations (45 CFR 164.506)

2. Proposals

OCR proposes to expressly permit covered entities to disclose PHI to social service agencies, community-based organizations, home and community-based service (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 healthcare provider or as a healthcare operations activity of a covered healthcare provider or health plan.

A growing body of evidence suggests that upstream factors, such as social determinants of health, impact the health of individuals and communities. The recent shift in healthcare towards value-based care models that incentivize prevention and promote improved outcomes for individuals and populations offers an opportunity to consider approaches and partnerships across clinical and non-clinical organizations that address health-related factors upstream from the clinical encounter.

For that reason, AHIMA supports the disclosure of PHI to social service agencies, HCBS providers, and similar third parties that provide health-related services to individuals for individual level care coordination and case management. However, we seek clarification as to whether minimum necessary will still apply under this proposed permission, consistent with existing guidance. Because such organizations generally do not fall under the scope of HIPAA, we are concerned that should minimum necessary not apply, allowing the sharing of such information without limiting the scope of PHI to carry out a specific purpose or function could jeopardize an individual's privacy and confidentiality.

Furthermore, the disclosure of an individual's PHI without adequate safeguards could also lead to potential discrimination, stigmatization, and implicit bias further exacerbating poor outcomes and existing health inequities. Should OCR finalize the proposed provision without the continued application

of minimum necessary, we believe the agency should require, at a minimum, notification to individuals in the Notice of Privacy Practices requirements that their PHI may be shared with social service agencies, community-based organizations, HCBS providers, and other similar third parties that provide health-related services.

3. Request for Comments

f. Should the Department specify the types of organizational entities to be included as recipients of PHI in this express permission in regulation text, as well as limitation of exclusions, if any, that should be placed on the types of entities included?

AHIMA does not believe it would be appropriate to specify the types of organizational entities that would be recipients of PHI in this express permission. Such a specification would be too limiting and runs the risk of excluding entities that perform such critical health related services. However, OCR may want to consider specifying the purpose or service provided by a social service agency, community-based organization or HCBS provider in this express permission to offer additional guidance to covered entities who may be asked to share PHI with such entities.

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)

2. Proposals

OCR proposes to amend five provisions of the Privacy Rule to replace the “exercise of professional judgment” with “good faith belief” as the standard to which covered entities would be permitted to make certain uses and disclosures in the best interests of the individual.

Generally, AHIMA supports the “good faith belief” standard to which a covered entity would be permitted to make certain uses and disclosures in the best interests of the individual. We believe that the modification of this standard from “exercise of professional judgment” makes sense with respect to these five particular circumstances.

OCR also proposes to amend the Privacy Rule at 45 CFR 164.512(j)(1)(i)(A) to replace the “serious and imminent threat” standard with a “serious and reasonably foreseeable threat” standard.

AHIMA supports the proposed modification as we believe that it will reduce the uncertainty of whether a threatened harm is imminent and provide other persons, whether it be family members, caregivers, and others with sufficient time to act to prevent harm to the individual or others.

G. Eliminating Notice of Privacy Practices 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)

2. Proposals

OCR proposes to eliminate the requirements for a covered healthcare provider with a direct treatment relationship to an individual to obtain a written acknowledgment of receipt of the Notice of Privacy

Practices (NPP) and, if unable to do so, to document their good faith efforts and the reason for not obtaining the acknowledgement. OCR also proposes to remove the current requirement to retain copies of such documentation for six years.

AHIMA supports OCR's intention to eliminate the above requirements. Removal of these requirements would alleviate administrative burden of health information professionals tasked with obtaining, documenting, and retaining this documentation.

OCR also proposes to replace the written acknowledgment with an individual right to discuss the NPP with a person designated by the covered entity.

AHIMA supports replacement of the written acknowledgment with the right to discuss the NPP with a person designated by the covered entity. We believe such a requirement not only creates additional accountability by holding a specific individual out to the patient to discuss their rights but empowers an individual to know who they may speak to should they have questions about their rights under HIPAA.

OCR also proposes to modify the required header of the NPP to specify to individuals that the notice provides information about: (1) how to access their health information, (2) how to file a HIPAA complaint, and (3) individuals' right to receive a copy of the notice and to discuss its contents with a designated person.

AHIMA supports the modification of the required header of the NPP. We believe this modification to include this information at the beginning of the NPP will improve individuals' awareness of their HIPAA Privacy Rule rights including what they can do if they suspect a violation of the HIPAA Privacy Rule and who to contact if they have questions concerning their rights.

OCR also proposes to modify the required element of an NPP that addresses the access right to describe how an individual can exercise the right of access to obtain a copy of their records at limited cost or, in some cases, free of charge, and the right to direct a covered healthcare provider to transmit an electronic copy of PHI in an EHR to a third party. Additionally, OCR proposes an optional element to the NPP to include information to address instances in which individuals seek to direct their PHI to a third party, when their PHI is not in an EHR or is in non-electronic format.

AHIMA supports both of these proposed modifications as they will help to improve individuals' awareness of their rights under the HIPAA Privacy Rule.

We thank you for the opportunity to comment on this proposed rule. AHIMA looks forward to having the opportunity to work with OCR to ensure the finalization of this rule and subsequent implementation. Should you or your staff have any additional questions or comments, please contact Lauren Riplinger, Vice President, Policy & Government Affairs, at lauren.riplinger@ahima.org and (202) 839-1218.

Sincerely,



Dr. Wylecia Wiggs Harris, PhD, CAE
Chief Executive Officer
AHIMA



233 N. Michigan Ave., 21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

Appendix 1: AHIMA and Ciitizen Fee Chart

Scenario	Documentation Required for Request?	Can Choose form/format for data?	Fees?	Other
Patient requests to inspect PHI	Written request is permissible but not required. Written request may not impose unreasonable measures		None when in person or via “internet-based” method (no fee to person or to app developer)	
Patient requests PHI (paper or electronic) to be sent to “personal health application”	Written request is permissible but not required. Can also be oral.	Yes – to personal health app	Reasonable, cost-based fees for labor costs of making copy, and cost of preparing summary/explanation (plus any supplies, or postage if applicable) – free if by “internet-based” method	
Patient requests PHI to be sent to self	Entity can ask for request in writing	Yes	Reasonable, cost-based fees for labor costs of making copy, and cost of preparing summary/explanation (plus any supplies, or postage if applicable) – free if by “internet-based” method	

Scenario	Documentation Required for Request?	Can Choose form/format for data?	Fees?	Other
Patient requests PHI to be sent to third party (not from EHR)	Requires HIPAA-compliant authorization – not part of HIPAA right of access	No	Not subject to access fee limitation but sale of data provisions apply (must be a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI (search & retrieval fees can be included)), “or fee otherwise expressly permitted by other law” (state law fees).	Permissive disclosure – unless third party is patient’s health care provider
Patient requests ePHI to be sent from EHR to third party	Written request not required (can be oral)	No	Reasonable cost-based fee limited to labor for making the copies (no supplies) (and cost of preparing a summary/explanation), (free if use internet based-method)	
Patient requests ePHI from an EHR to be sent directly to a health care provider or health plan	Written request not required (can be oral)	No	Reasonable cost-based fee limited to labor for making the copies (no supplies) (and cost of preparing a summary/explanation), (free if use internet based-method)	
Third party requests (with patient)	Requires HIPAA compliant authorization	No	No limits on fees but sale of data provisions	Permissive disclosure

Scenario	Documentation Required for Request?	Can Choose form/format for data?	Fees?	Other
authorization) not from EHR			apply (must be a reasonable, cost-based fee to cover the cost to prepare and transmit the PHI (so search & retrieval fees can be included)), “or fee otherwise expressly permitted by other law” (state law fees).	