AMA AMERICAN MEDICAL ASSOCIATION

James L. Madara, MD
CEO, EXECUTIVE VICE PRESIDENT

james.madara@ama-assn.org

May 5, 2021

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

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

Dear Acting Director Frohboese:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the Notice of Proposed Rulemaking (NPRM) from the Office for Civil Rights (OCR) on the Health Insurance Portability and Accountability Act (HIPAA) regulations and how these regulations can be revised to support coordinated care and individual engagement.

OCR has created a proposal full of well-intentioned policies that are poised to ease how patients access their data, increase the amount of information payers can receive from health care providers, expand the scope of entities to which physicians may disclose patient data, and reduce patient and physician burden. However, we question the need for these changes, particularly at this time. Physician practices are already making significant, paradigm-changing adjustments to their information management, patient engagement, and exchange processes to comply with information blocking regulations promulgated by the Office of the National Coordinator for Health Information Technology (ONC). These changes went into effect in early April 2021 and will continue for many months and years as the full suite of policies required by the 21st Century Cures Act (Cures Act) are implemented. Small practices will likely lag behind large health systems implementing Cures Act changes due to the technical and human resources needed to implement these policies. Moreover, many physician practices are still dealing with the impacts of the public health emergency (PHE) caused by the novel coronavirus, COVID-19. **We urge OCR to reconsider implementing a massive change to patient privacy laws in the midst of this transition.** At the very least, we recommend that OCR prioritize what changes can be implemented in tandem with the technology and policy changes already slated for the next 18 months.

The first step of any ultimately successful privacy framework, legislative or regulatory, places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private—something that technology can help physicians accomplish in a minimally burdensome way. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose. These are the ground rules of AMA policy and they should be the ground rules for federal privacy policy. AMA policy and ethical opinions on patient privacy and confidentiality provide that a patient's privacy should be honored unless waived by the patient in a meaningful way, de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient privacy or breaches of confidentiality.

The AMA is very concerned that significant changes to HIPAA, which is permissive, will result in required information sharing when combined with information blocking regulations. While we understand that may be the intent of policy makers, we continue to caution that most patients will not be aware of or understand the impact of these changes—changes that could have enormous impact on patient privacy and autonomy and could create or exacerbate inequities. OCR's intent to reduce administrative burden and expand ways in which covered entities may share protected health information (PHI) is understandable, but it also whittles away at the mechanisms clinicians have to keep health data private and secure in ways that patients have come to expect from their health care providers. For each action taken to expand access to information, OCR must consider ways in which physicians can honor patient requests to keep data private. For example, OCR's intent to reduce barriers to exchanging information by allowing oral requests is completely understandable given the hoops that patients often must jump through to receive access to their information. We agree with OCR's proposal that covered entities should be prohibited from imposing onerous, burdensome requirements on their patients requesting that PHI be sent to a third party. However, some safeguards exist for a reason: written instruction to covered entities outlining where to send PHI should be maintained to ensure that PHI is sent to the correct facility or person. Both the patient and physician would suffer the consequences of sending information to an unintended recipient. The AMA is concerned about a loss of balance between access and privacy: the NPRM does not include any proposals giving patients greater control over who their information is shared with and for what purpose. In fact, the NPRM even includes questions about overriding a patient's expressed privacy wishes. **The AMA strongly opposes the finalization of any policies expanding the current ability of covered entities—or any other type of entity, including smartphone apps and third parties—to override an individual's privacy preferences.**

Relatedly, should OCR finalize the proposals in its NPRM, we encourage OCR to consider and publicize how it plans to educate covered entities about the vast scope of changes that will be required to implement the new regulations, particularly in light of their intersection with ONC regulations. Despite efforts by OCR, the AMA, and others, understanding of HIPAA has historically been challenging for covered entities and other stakeholders—likely in part due to the nuances and complexities added by state law and varying interpretations by lawyers, compliance offices, and risk management teams. As such, health care providers frequently report that privacy laws inhibit their ability to exchange information even when such laws, in fact, do permit information sharing. Indeed, we encounter many industry stakeholders beyond health care providers who misunderstand privacy laws and thus perpetuate confusion about how such laws permit information sharing. Physicians need and want guidance that helps them navigate the "grey areas" of privacy law, rather than revision of laws that protect patient privacy interests. As such, we urge OCR to strategize around ways to ensure physicians, patients, and other health care industry stakeholders are alerted to new and existing guidance that contains answers to common, real-world clinical scenarios. The AMA would like to work with OCR to amplify its educational efforts.

In closing, thank you for this opportunity to share the views of the AMA regarding the proposals, issues, and questions that OCR has raised in its NPRM. Our comprehensive comments are found in the enclosed chart. If you have any questions, please contact Laura Hoffman, Assistant Director, Federal Affairs, at laura.hoffman@ama-assn.org.

Sincerely,

James L. Madara, MD

Attachment

Proposal	AMA Comments
A. Individual Right of Access (45 CFR 164.524)	
1. New Definitions: EHR and PHA (45 CFR 164.501)	
OCR proposes to add definitions for the terms electronic health record (EHR) and personal health application.	
Response to Proposals on EHR/PHA proposals	
a. Whether the Department's proposed definition of EHR is too broad, given the context of the HITECH Act, such that the definition should be limited to clinical and demographic information concerning the individual. b. Whether the Department should instead define EHRs to align with the scope of paragraphs (1)(i) and (2) of the definition of designated record set. c. h. Whether EHR should be defined more broadly to include all ePHI in a designated record set, and benefits or drawbacks of doing so. d. Should the definition of EHR for Privacy Rule purposes be aligned with other Department authorities or programs related to electronic health information? If so, which ones and for what purposes? e. j. Any other effects, burdens, or unintended consequences of the proposed definition of EHR or of including a definition for EHR in the Privacy Rule.	The AMA appreciates OCR's desire to expand on the HITECH Act definition of EHR. However, it is unclear how the proposed definition aligns, complements, or supports similar electronic health information (EHI) definitions. For example, the Office of the National Coordinator for Health Information Technology (ONC) includes the concept of electronic protected health information (ePHI) in its definition of EHI. ONC describes this linkage as intentional with "the focus of the EHI definition on terms that are used in the HIPAA Rules and that are widely understood in the health care industry as well as on a set of health information that is currently collected, maintained, and made available for access, exchange, and use." EHI is a term established by Congress with the intention to better facilitate information exchange and patient access. ONC's linkage between ePHI and EHI helps facilitate that intent. Furthermore, OCR is not proposing to modify the definition of ePHI and uses the term through its proposed rule—further solidifying its importance. By creating yet another definition that encapsulates electronic health information (i.e., OCR's proposed EHR definition), OCR is negating ONC's effort to create a widely understood set of health information. **The AMA recommends that OCR merge EHI into its EHR definition—ensuring a more cohesive language for the health care community to communicate patients' electronic health information.** Moreover, the lack of alignment between EHI and EHR will significantly contribute to physician confusion with HIPAA regulations and information blocking compliance (e.g., the access, exchange, and use of EHI) and may lead to conflicting regulatory interpretations across HIPAA covered entities and information blocking Actors. Physicians should not have to separate and distinguish EHR from EHI to comply with both the HIPAA and information blocking rules. It is unreasonable to think that the nuance of overlapping and complex regulations will consistently be appreciated by busy physicians taking care of patients. Furthermore, OCR's use of the term "EHR" is confusing. Physicians commonly refer to their electronic health record systems as EHRs. EHR software products are distinct from

	the electronic medical records retained in them. Physicians and patients will understand "EHR" to mean different things. For instance, a patient may request access to their EHR. However, a physician or a member of the practice's staff may interpret that to mean the patient is requesting access to the EHR software product itself. This would likely result in the physician or practice staff denying access believing the patient wanted to log into the practice's EHR system—gaining access to all patients' medical records. While this concern may seem simplistic or unrealistic, it illustrates the types of confusing scenarios that could arise based on creating a new meaning for the term "EHR." It is important for physicians and their staff to clearly understand the terminology being used and what health information should be available for access, exchange, and use—particularly when patients exercise their right of access under HIPAA. The AMA disagrees with OCR's proposal to explicitly include electronic billing records in the term EHR. In its final information blocking rule, ONC identified reasons why billing information should not be a defined component of EHI. These include issues with a lack of billing record standardization and concerns with information clearly and understandability. The AMA agrees with ONC's alternative approach that, to the extent ePHI includes billing information and is included in a designated record set, billing information would be considered EHI. It should follow that OCR adopts this same logic as to not add confusion or increase the friction patents experience requesting EHI via their right of access. **AMA recommends OCR include billing records in the term EHR only to the extent that such records are included in a designated record set. Additionally, we recommend OCR coordinate with ONC to ensure cross-agency agreement and alignment on what comprises the designated record set.** This approach is intended to assure that the current scope of EHI for purposes of information blocking is aligned with the definitions of ePHI and designated record set under the HIPAA Rules.
b. Whether an electronic record can only be an EHR if it is created or maintained by a health care provider, or whether there are circumstances in which a health plan would create or maintain an EHR.	Providing electronic records to patients is an important part of patient engagement and a fundamental aspect to the patient right of access under the HIPAA Rules. Several recent regulations have further enabled patients to better access, exchange, and use their electronic records. These include regulations from ONC and CMS.

	These regulations have also positioned CEs—including health plans—to access and store a broad range of patients' medical information. Health plans' collection of electronic records increasingly comprise the entirety of an individual's longitudinal care. By removing the "minimum necessary" limitations on the data set sent from physicians to payers for care coordination or case management, OCR is proposing to enable even greater access and collection of information by health plans. The AMA is also aware of health plans tapping directly into physicians' EHRs and extracting entire sets of electronic medical records. The AMA has identified several concerns with health plans having unfettered access into a physician's EHR. One consideration is the lack of bi-directional exchange between physicians and health plans. The flow of information goes from the physician to the health plan with little provided back to the physician in return. This puts physicians and patients in a disadvantage. Health plans may wind up knowing more about an individual's medical history than either the physician or patient themselves. Accordingly, regardless of what the repository of such information is called, health plans are in fact already creating and maintaining EHRs for their members. **OCR should designate any health plan that requests, access, or maintains patients' medical records to facilitate "care coordination" or "case management" as creating and maintaining an EHR.**
d. Whether the proposed definition of EHR includes PHI outside of an electronic designated record set, whether it should, and examples of such PHI.	The AMA disagrees with OCR's proposal to explicitly include electronic billing records in the term EHR. There are instances where billing records would not be part of a physician's designated record set. Billing records may not be maintained by a physician (e.g., billing information between an individual and a health plan), or may not be consulted by a physician since health plans often do not provide complete information on actual charges, costs, and prices for medications. OCR must do more to ensure health plans provide this information to both physicians and patients. **The AMA urges OCR to consider expanding the designation of EHR to health plans to support this goal.** Furthermore, unless and until health plans are required to meet the same EHR requirements as physicians, AMA recommends OCR include billing records in the term EHR only to the extent that such records are included in a designated record set.

e. Whether the proposed interpretation of "health care clinicians and staff" as it relates to the proposed EHR definition is appropriate, too broad, or too narrow, and in what respects. f. Should "health care clinicians and staff" be interpreted to mean all workforce members of a covered health care provider? What are the benefits or adverse consequences of such an interpretation? Does the same interpretation apply regardless of whether the provider has a direct treatment relationship with individuals, and why or why not?	OCR's inclusion of health care staff as an entity that may generate electronic health records will cause complications, confusion, and misinterpretation. The AMA is concerned that physicians' staff may capture or document information about a patient outside the normal workflow of a patient encounter—without physicians' or other authorized health care clinicians' knowledge. Staff may lack the necessary expertise to understand the reliability or completeness of such information. For instance, under OCR's proposal, back-office administrative staff who scan in (i.e., convert a document from paper to an electronic medium like a PDF) information faxed from an outside laboratory may not realize the information is preliminary or may not have the ability to determine if the information is accurate. However, this action would nevertheless transform inaccurate or incomplete information into EHRs which could then be accessed by the patient through their right of access—potentially without their physician's knowledge. Inaccurate or incomplete information could pose a serious physical and mental harm to patients or their non-clinical caregivers. OCR's proposal to include non-clinical staff as it relates to the creation of EHRs lacks sufficient guardrails. **The AMA recommends OCR limit EHR creation to authorized health care clinicians.**
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.	Personal health applications (apps) can provide individuals increased access and use to their electronic health records and facilitate the exchange of those records between and among the individual's care team. However, the AMA is aware that apps are not regulated by HIPAA and there are few if any meaningful federal laws that protect individuals from apps managing, sharing, or controlling their electronic health records without their knowledge. OCR can and should provide additional protections for individuals. The AMA recognizes OCR does not have the authority to regulate apps themselves. However, OCR's proposal to define personal health applications and subsequently provide those apps increased access to electronic health records should be balanced with the need for increased transparency. This can be accomplished by modifying the proposed definition by including the following in italics: "[…] provided that such information is *securely* managed, shared, and controlled by or primarily for the individual *and that the individual is informed by the personal*

	health application developer what information will be managed, shared, or controlled by the application developer, including the intended use by the developer." This definition will increase the transparency around an app's collection and use of an individual's information while strengthening individuals' trust in personal health applications. **App developers seeking to be considered personal health applications under OCR's definition will be strongly motivated by the addition of this qualifying language to improve their data use practices.** This definition does not require OCR to regulate apps, rather it extends OCR's stated desire to promote individuals' data privacy and meaningful knowledge of electronic health record use. **Furthermore, the AMA recommends OCR interpret the term "securely" as an app meeting the applicable data security requirements found in the HIPAA Security Rule.**
o. Whether a covered health care 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? For example: Accepting the individual's judgment without requiring covered entities to provide education, notice, or warning; requiring a covered entity to provide a warning verbally and/or electronically at the time the individual requests transmission of PHI to a personal health application; providing education about the application developer's privacy and security policies and practices through an automated attestation and warning process; or adding information about risks to PHI disclosed to a personal health application in the covered entity's NPP.	The AMA is a strong advocate for individuals to have meaningful information about an app's management, control, or use of their PHI.[1] We applaud OCR for recognizing the need to ensuring transparency for individuals and to strengthen data privacy. Patients place considerable trust in their health care team—sharing personal health information and confiding in their physicians. The loss of trust between a patient and physician can severely impact their health and wellness. Research has shown that patients trust their physicians when seeking recommendations about the choice in personal health applications. However, physicians are often limited in their knowledge of app privacy and security risks. Sharing incomplete information or misinformation with patients can harm these trusted relationships. App developers are not required to share privacy and security information with individuals nor are developers required to be truthful about what information is shared. **The AMA does not support any requirements on health care providers to inform individual about privacy and security risks; health care providers are not provided all the necessary information by app developers to be a learned intermediary between patients and app developers.**

[1] https://www.ama-assn.org/delivering-care/patient-support-advocacy/ama-health-data-privacy-framework

	The AMA urges OCR to consider those entities best situated to know and communicate information about the management, sharing, or control of a patient's PHI and to explore methods to increase transparency. For instance, the AMA supports app attestations and warning process and has urged CMS and ONC to include these processes within their regulatory frameworks. Recognizing OCR does not have the authority to regulate apps themselves, **the AMA urges OCR modify its proposed definition of personal health applications to promote transparency.** Specific recommendations can be found in our previous comments.[2] This would allow patients to select apps that have privacy values most like theirs, make more informed decisions while shopping for apps with which they are comfortable sharing personal health information (i.e., better ability to "comparison shop"), and bolster trust in the use of emerging technologies. **OCR should also consider additional incentives to motivate health IT developers to collect and share app attestations.**
p. The Department also invites comment on whether to apply any potential education, notice, or warning requirement to only health care providers or also to health plans. Whether the Department should consider requiring a covered health care provider or health plan to provide any specific educational or advisory language to individuals who may choose to share their PHI with other individuals through applications that are not regulated by the Privacy Rule.	The AMA does not support applying any education, notice, or warning requirements on health care providers. Health care providers are themselves do not receive the necessary information by app developers to educate patients or other individuals about privacy and security risks. The AMA urges OCR to consider those entities best situated to know and communicate information about the management, sharing, or control of a patient's PHI and to explore methods to increase transparency. For instance, the AMA supports app attestations and warning processes and has urged CMS and ONC to include these processes within their regulatory frameworks. Recognizing OCR does not have the authority to regulate apps themselves, **the AMA urges OCR modify its proposed definition of personal health applications to promote transparency.** Specific recommendations can be found in our previous comments. This would allow patients to select apps that have privacy values most like theirs, make more informed decisions while shopping for apps with which they are comfortable sharing personal

[2] See, e.g., https://searchlf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-5-31-Letter-to-Dr-Rucker-re-ONC-NPRM-Comments.pdf; and https://searchlf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-5-31-Letter-to-Verma-re-CMS-Comments.pdf.

	health information (i.e., better ability to "comparison shop"), and bolster trust in the use of emerging technologies.
2. Inspecting PHI in Person	
OCR proposes to: • Allow individuals to take notes, videos, and photographs, and use other personal resources to view and capture PHI in designated record set (DRS). • Extend the right to inspect to situations where mutually convenient times and places include points of care where PHI in a DRS is readily available for inspection by the patient, for example, by viewing x-rays, ultrasounds, or lab results in conjunction with a health care appointment with a treating provider.	
Response to Proposals on Inspecting PHI in Person	
OCR seeks comment on whether to require covered health care providers to allow individuals to record PHI [via notes, photographs, and recordings] as part of the Privacy Rule access right.	The AMA generally supports the right individuals to take notes and photographs while reviewing his or her PHI, though we recommend OCR direct covered entities to develop policies and procedures to facilitate this right, rather than imposing a blanket requirement on covered entities to allow recordings. For example, it will be essential for covered health care providers to develop policies and procedures for how patients may take photos without risk to other patients' privacy. These processes could vary based on the type of facility, the number of staff able to assist with requests, and the physical space in the facility to accommodate such requests. We oppose any policy that would allow patients to record conversations with their physicians absent express consent from the physician prior to the recording. This would include conversations between a physician and patient during which a physician explains the patient's PHI.
OCR seeks comment on whether conditions or limitations should apply to ensure that a covered health care provider does not experience unreasonable workflow disruptions (*e.g.,* limitations on time spent recording PHI in conjunction with a health care appointment).	OCR should consider that covered entities may not have the space to facilitate a patient's desire to review their records while at the office. It should also consider that many practices do not have personnel devoted to accommodating patients' requests to inspect their records in person, which could be perceived as blocking access. Again, we urge OCR to require consent from a physician before a patient may record PHI during a health care appointment in which the physician is present. We further recommend OCR make clear to covered entities and patients that the option to photograph PHI may only be available if the practice is able to offer a segregated

	space in which no other identifiable patient information (including actual pictures of other patients) may be captured.
OCR seeks comment on 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 health care appointment	As mentioned above, physician practices may not have dedicated space within their offices to provide patients with a private place to review their PHI and ensure any photographs or recordings do not capture other identifiable patient information. If OCR fails to include limitations on a requirement allowing for inspection of PHI in conjunction with a health care appointment, practices may find themselves able to see fewer patients because rooms will be taken for record review rather than patient encounters. Additionally, physicians may be asked to spend additional time with their patients to review PHI with them—time for which they are not financially compensated. While physicians are generally willing to review PHI with patients, a requirement that they take time from their clinic or that they spend additional time outside of working hours to do so could prove problematic.
OCR seeks comment on how to determine when PHI is "readily available."	We recommend to OCR that PHI is "readily available" for inspection when it is mutually convenient for both the patient and the physician. "Readily available" must not be interpreted to mean "on demand." OCR is likely aware that covered entities often do not store all PHI onsite at any given time. Moreover, even PHI that has not been placed into off-site storage could be difficult to access at a moment's notice. For example, multi-site clinics often use one administrative address. A patient may show up for an appointment with his or her clinician at one site and ask about labs they had done the week prior. Those lab results may have been sent to the practice's central location, where they will be reviewed by the clinician and input into the EHR. In circumstances like these, the patient may be aware that the *practice* has received the patient's lab results, but the actual clinician with whom they are meeting literally may not be able to access the results.
l. State laws or other known legal restrictions that might affect the ability of individuals to take photos of or otherwise capture copies of their PHI in a designated record set.	We are not aware of state laws that would restrict an individual from taking photos of his or her PHI in a designated record set. However, there may be physician practice or hospital policies in place to prevent pictures of PHI or other patient data, presumably as a risk management tool. We reiterate our comment from above, supporting the ability of patients to take photographs of their records, but not

	recordings without the consent of all parties involved. State wiretapping laws may apply to questions around recording conversations with clinicians, as well.
3. Modifications to Requests for Access and Timeliness	
OCR proposes to: • Expressly prohibit a covered entity from imposing unreasonable measures on an individual exercising the right of access that create a barrier to or unreasonably delay the individual from obtaining access—specifically, clarification that, while an entity may require individuals to make requests for access in writing, it would not be permitted to do so in a way that impedes access. • Shorten covered entities' required response time to no later than 15 calendar days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension). • Require covered entities to establish written policies for prioritizing urgent or other high priority access requests (especially those related to health and safety) to help limit the need to use 15 calendar-day extensions for such requests. • Apply the same timeline to access requests regardless of whether the information sought is stored on paper or electronically.	
Response to Proposals on Requests for Access and Timeliness	
OCR requests comment on burdens that covered entities believe may result from this proposed change.	**The AMA agrees with other commenters in the 2018 RFI citing numerous factors that may negatively affect a covered entity's ability to timely fulfill access requests and urges the OCR to reconsider its evaluation of these factors** (this list is not exhaustive): the nature of the requested information, whether the records are stored off-site, the need for professional or legal review based on state law or 42 CFR Part 2 requirements to segregate information that cannot be released at all or without authorization, and the size and complexity of the covered entity. We further believe that there are a number of factors that can affect access times for the production of electronic records and urge the OCR to re-evaluate their analysis of these factors (this list is not exhaustive): including PHI residing in multiple IT systems in varying formats and requests covering long periods of time, or covering a high volume of records related to complex and intensive medical treatment that must be collated and put into the requested electronic format or medium.
n. Whether a time limit shorter than 15 calendar days for a covered entity to submit, or respond to, an individual's access request would be appropriate. OCR seeks comment on time limits for covered entities to respond	The length of time needed to respond to an individual's request for a copy of their PHI will vary with each practice and health care system. Some practices may be able to provide records more quickly if, for example, the practice has relatively few patients, has an established and well-functioning health information management

to access requests, requests to direct electronic copies of PHI in an EHR to a third party, and requests to submit a request to another provider on behalf of the individual. OCR welcomes data on the burdens and benefits such a time limit would impose.	department or employs a full-time privacy officer, or the patient is only asking for a small portion of his or her records. Alternatively, practices with a large number of patients, practices without records management procedures, practices that receive a large number of access requests, and practices lacking employees dedicated to health records management may struggle to expeditiously respond to patient requests (though often still do so within the time required under HIPAA). Additionally, a practice may take longer to respond to established patients with large records as opposed to a patient with relatively small records. Furthermore, a practice may store records of patients who have not recently been seen by the practice in an offsite long-term storage facility, which may take longer to access than the records of current patients. **The AMA opposes any effort to establish a time limit shorter than 15 calendar days for a covered entity to submit, or respond to, an individual's access request.** A patient should always be able to receive his or her records in a timely manner. However, OCR should also recognize that specific practice response times to access requests will vary depending on the individual practice, the size of the patient's record and what portion of the record the patient is requesting, where the patient's records are located, and, presumably, the number of requests received by the practice. Shortening the timeframe in which a practice must respond to access requests would almost certainly increase the practice's administrative burden, particularly in practices without personnel dedicated to records management. Decreasing the time limit by half, as proposed, would necessitate practices increasing expenditures on staff and thus diverting resources from treating patients. This is especially true with regards to smaller practices. Administrative staff in small practices often "wear multiple hats" and have multiple disparate responsibilities, so staff can become spread thin when additional responsibilities are added through regulation. Further, all physicians and their staff must prioritize the numerous requests they receive each day, and regularly spend an average of two business days (16 hours) each week completing prior authorization requests to ensure their patients do not have a delay in necessary care and/or a serious adverse event.[3]

[3] https://www.ama-assn.org/system/files/2021-04/prior-authorization-survey.pdf

	Additionally, a shortened response timeframe may become incredibly burdensome if a patient requests his or her entire record and/or has been a patient for many years, or if a practice stores old records offsite to provide rapid patient access to those records. The many nuances of this process—not physician unwillingness to share information—make it unrealistic to always expect a quick response to a request for PHI. In sum, federal regulation and policy must balance the goal of prompt patient data access with the limitations placed on physicians by the characteristics of a physician's practice and the logistics associated with obtaining a patient's record.
r. Whether any federal or state law time limit shorter than 15 calendar days that applies to disclosures of PHI to a third party (e.g., public health agency) should be deemed a "practicable" time limit under the Privacy Rule right of access.	Although the AMA agrees with the goal of providing timely access to requested PHI, the variability of time standards would add complication and confusion to covered entities, particularly those who practice in multiple states where standards are not consistent. Varying standards are not practicable to uphold under the Privacy Rule right of access.
s. Whether and how a covered entity should be required to implement a policy for prioritizing urgent or otherwise high priority access requests, so as to minimize the use of the 15-calendar-day extension. Would there be unintended adverse consequences of such a requirement—e.g., would covered entities begin to require individuals to state the purposes for their access requests even though the Privacy Rule does not make the right of access contingent on the purpose for the request? If a covered entity did impose such a requirement, would this constitute an unreasonable measure that impedes the individual from obtaining access?	Although the AMA agrees with the goal of this specific proposal and has been vocal about urging covered entities to implement a system allowing patients to flag emergency requests versus those that are more routine,[4] the AMA does not believe that covered entities should be mandated or required to implement a specific policy for prioritizing urgent or otherwise high priority access requests to utilize a 15-day extension. While we appreciate the positive incentive approach to this proposal, we would suggest a different mechanism to accomplish the goal, as there are potential unintended consequences associated with requiring an urgent/high priority access policy. For example, because OCR does not propose to define what constitutes an urgent or high priority request, administrative staff would be tasked with determining which requests for records are truly urgent or high priority versus other high priority requests (e.g., prior authorization requests that if delayed could directly hinder immediate patient care). Additionally, such a policy would likely require individuals to state the purposes for their access requests, even though the Privacy Rule does not make the right of access contingent on the purpose for the request. This could infringe upon a patient's right to privacy even while requesting records in a timely

[4] https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf (PDF page 32)

	manner. **We recommend that OCR create and publish a model urgent request policy for voluntary use. We also recommend that OCR take a covered entity's written urgent request policy into account as a mitigating factor when conducing an audit or investigation into patient access complaints.**
4. Addressing the Form of Access	
OCR proposes to: • Clarify the form and format required for responding to individuals' requests for their PHI. • Require covered entities to inform individuals that they retain their right to obtain or direct copies of PHI to a third party when a summary of PHI is offered in lieu of a copy.	
Response to Proposals on the Form of Access	
OCR requests information about the costs and benefits of options for educating individuals about privacy and security interests when they use an app to get their PHI from a covered entity in a manner that does not delay or create a barrier to access.	As described earlier, the AMA is a strong advocate for individuals to have meaningful information about an app's management, control, or use of their PHI.[5] We applaud OCR for recognizing the need to ensuring transparency for individuals and to strengthen data privacy. Patients place considerable trust in their health care team—sharing personal health information and confiding in their physicians. The loss of trust between a patient and physician can severely impact their health and wellness. Research has shown that patients trust their physicians when seeking recommendations about the choice in personal health applications. However, physicians are often limited in their knowledge of app privacy and security risks. Sharing incomplete information or misinformation with patients can harm these trusted relationships. App developers are not required to share privacy and security information with individuals nor are developers required to be truthful about what information is shared. Just as such information is not consistently or reliably shared with app users, health care providers are not provided with all the information needed from app developers to provide patients with appropriate guidance on the privacy and security

[5] https://www.ama-assn.org/delivering-care/patient-support-advocacy/ama-health-data-privacy-framework

	of a given app. **Accordingly, the AMA does not support any requirements on health care providers to inform individual about privacy and security risks**. The AMA urges OCR to consider those entities best situated to know and communicate information about the management, sharing, or control of a patient's PHI and to explore methods to increase transparency. For instance, the AMA supports app attestations and has urged CMS and ONC to include these processes within their regulatory frameworks.[6] Recognizing that OCR does not have the authority to regulate apps themselves, **the AMA urges OCR modify its proposed definition of personal health applications to promote transparency as described earlier in this table.** Doing so would allow patients to select apps that have privacy values most like theirs, make more informed decisions while shopping for apps with which they are comfortable sharing personal health information (i.e., better ability to "comparison shop"), and bolster trust in the use of emerging technologies. **OCR should also consider additional incentives to motivate health IT developers to collect and share app attestations.**
OCR seeks comments on related situations: Whether to require a health care provider that has EHR technology that incorporates a secure, standards-based API without extra cost, to implement the API; whether to require a health care provider that could implement such an API at little cost to do so; and how to measure the level of cost that would be considered a reasonable justification for not implementing an API.	The AMA opposes requirements for physicians to implement API technology that would unreasonably increase costs to the physician or their practice, particularly considering the many alternative ways patients can access their health information. While the AMA strongly supports the use of APIs to promote information exchange, it will be difficult for the federal government to determine what an acceptable "little cost" is for practices of all specialties, sizes, and locations. Relatedly, "extra cost" is subjective; costs can be hidden by EHR vendors in monthly or yearly service fees, training, customizations, or other unnecessary line items. API usage fees may also far exceed what a small physician's practice can afford. Moreover, many practices will already be required to use EHR technology that incorporates a secure, standards-based API; OCR should not further constrain physicians' choices on how to do so in a way that the practice can afford.

[6] See, e.g., https://searchlf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-5-31-Letter-to-Dr-Rucker-re-ONC-NPRM-Comments.pdf; and https://searchlf.ama-assn.org/undefined/documentDownload?uri=%2Funstructured%2Fbinary%2Fletter%2FLETTERS%2F2019-5-31-Letter-to-Verma-re-CMS-Comments.pdf.

5. Addressing the Individual Access Right to Direct Copies of PHI to Third Parties	
Copies of PHI to Third Party is Limited to EHR Information Only: • OCR proposes to clarify that requests to direct copies of PHI to a third party will be limited to only electronic copies of PHI in an EHR. This will only apply to health care providers as OCR assumes only health care providers have EHRs. (No payers, no HIEs, etc.) Clear, Conspicuous, and Specific Requests: • OCR proposes that covered health care providers would be required to respond to an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual when the request is ''clear, conspicuous, and specific''—which may be orally or in writing (including electronically executed requests). The proposed requirement would replace the current requirement that a request to direct an electronic copy of PHI in an EHR be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI. Requestor-Recipient Pathway: • OCR proposes to create a pathway for individuals to direct the sharing of PHI in an EHR among covered health care providers and health plans by requiring covered health care providers and health plans to submit an individual's access request to another health care provider and to receive back the requested electronic copies of the individual's PHI in an EHR. • The Requester-Recipient would be required to submit such access requests to Discloser on behalf of the individual as soon as practicable, but no later than 15 calendar days after receiving the individual's direction and any information the Requester-Recipient needs to submit the access request to Discloser. One 15 calendar day extension would be permitted under the same conditions described above with respect to the Discloser fulfilling other access requests.	
Response to Proposals on Individual Access Right to Direct Copies of PHI to Third Parties	
mm. What are commonly available electronic forms and formats that covered entities and business associates generally provide to individuals or third parties? How many requests per month for electronic copies of PHI on electronic media do covered entities and business associates receive from individuals? How many requests per month are received for electronic copies provided through internet-based methods? How long does it take to fulfill each type of request?	The electronic forms and formats commonly available for electronic copies of PHI are directly influenced by the health IT vendors (e.g., EHRs) physicians use to manage, export, or communicate PHI. Physicians are only able to support forms and formants provided by their EHR vendors. Most EHRs provide physicians the ability to export or save PHI from the EHR's database using portable document format (PDF) documents, plain text format documents, comma-separated values (CSV) documents, or imaging format (e.g., .gif, .jpg, and .png) files. While ubiquitous, these formats may not meet the needs of all individuals or third parties requesting PHI. Furthermore, individuals or third parties may encounter difficulty using records storied in proprietary medical record standards. For instance, some EHR vendors will

nn. Do individuals or third parties ever receive requested PHI in unreadable electronic forms and formats? What are those forms and formats, and do covered entities or business associates provide another form and format if they are told the first copy of PHI they provided is unreadable or unusable?	retain imaging studies (e.g., digital x-ray) in their original digital imaging and communications in medicine (DICOM) format. Providing DICOM images to patients without DICOM viewing software may restrict patients or other physicians from using the images. Physicians exporting or coping PHI for an individual may encounter significant costs or delays when requesting their EHR vendor change formats or formatting or provide additional "reading" or "viewing" software to support a proprietary standard. **OCR should not enact policies that unduly penalize physicians for costs or temporal limitations caused by their health IT vendors.**
q. Whether OCR should specify in regulatory text that if a Requestor-Recipient discusses the request with the individual (e.g., to clarify the request or explain how the request could be changed to be more useful in meeting the individual's health needs), such discussion does not extend the time limit for submitting the request, and the benefits or drawbacks of such a provision.	Yes, OCR's inclusion of this clarification in regulatory text would be helpful to physician practices.
t. Any benefits or drawbacks of the proposal to require a covered entity to act on an oral access request to either direct an electronic copy of PHI in an EHR to a third party or direct a covered entity to submit such a request, provided the oral communication is clear, conspicuous, and specific.	The AMA appreciates the intent of OCR's proposal to make it easier for patients to orally request that a covered entity provide records access to another covered entity or a third party. However, we anticipate that the use of oral communication to direct information to a third party will result in significant unintended consequences. For example, a patient may inadvertently misspeak when describing who information should be disclosed to, or a covered entity could mishear or inadvertently misrecord the destination/recipient of the patient's PHI. In such situations, the practice may be exposed to increased likelihood of breach despite best intentions from all involved parties. In this case, both the patient and covered entity are harmed—the patient's PHI will be disclosed to an unintended recipient, and the covered entity may be liable for a breach. If information is inadvertently disclosed to the wrong covered entity, at least the receiving covered entity would be bound to protect the privacy and security of such information; however, this is not necessarily true for other third party recipients.

u. Whether there would be unintended consequences for the covered entity that has received PHI as a result of a request that was made to another covered entity by an individual.	We note that this type of record exchange is already both permitted by HIPAA and frequently utilized by patients. That said, it is possible that covered entities will receive an increased number of requests from patients to request PHI from other covered entities, which could result in additional administrative burden. It is also possible that more information will be disclosed in response to a covered entity's request for access than the patient fully intended. For example, a patient may simply want one covered entity to share a medication or diagnosis list with another covered entity, but the sending covered entity will send the patient's entire medical record. OCR should consider ways to ensure that the patient is able to specify, on a granular level, which information it wants transmitted under the right of access.
v. "Clear, conspicuous, and specific" is a statutory standard that OCR proposes to use in place of the existing regulatory requirement that the request be signed and in writing and clearly identify the designated third party. OCR requests comment on how to interpret the phrase "clear, conspicuous, and specific," including when the request is verbal.	We support the "clear, conspicuous, and specific" statutory standard. However, absent very clear guidelines, we disagree with OCR's interpretation that this phrase can include oral communications. For example, we can foresee circumstances in which a patient would make an oral request for records to be directed to "Family Medical Group" – but without knowing the medical group's address or phone number, there is no way to ensure the covered entity sends records to the correct "Family Medical Group." The current requirement that the request for access directed for a third party be "in writing…[clearly identifying] where to send the copy"[7] of PHI is important and should be retained. We recommend requiring at least one additional identifying element beyond the name of the recipient organization. Additionally, OCR should develop a list of practices that are not permitted to ensure that the process is not overly burdensome to patients. Practices such as requiring notarization, an inked signature, or delivering the request in person should each be prohibited.
w. Whether the Department should specify any bases for a Requester-Recipient to deny an individual's request to submit an access request to a Discloser, for example, if the requested disclosure is prohibited by state or other law or if the Requester-Recipient already has the information.	Request-Recipients should be permitted to deny requests lacking "clear, conspicuous, and specific" elements, such as name of the organization, address of the organization, or phone number of the organization. They should also be permitted—in fact, obligated—to adhere to state or other privacy laws and to any previously expressed wishes by the patient with respect to privacy of their PHI.

[7] 45 CFR 164.524(c)(3)(ii).

x. Whether there are certain types of individual requests to submit an access request to a Discloser that would place an undue burden on the Requester-Recipient, such as submitting large numbers of requests to multiple Disclosers, or other factors affecting the potential burden on or benefit to a Requester-Recipient.	OCR is proposing to require covered health care providers and health plans to submit an individual's access request to one or more health care provider(s) and to receive back the requested electronic copies of the individual's PHI in an EHR. Request-Recipient physicians would be required to submit the request as soon as practicable, but no later than 15 days after receiving the individual's request. Additionally, an individual may use an internet-based method (e.g., personal health app) to submit the initiating request to the Request-Recipient. While the AMA recognizes the burden patients face coordinating the collection of their disparate health records and believes more should be done to reduce friction, we have concerns with the potential for physician burden, gaps in closing the request loop, and abuse of internet-based request methods by third parties. OCR's proposal would make it the responsibility of a physician to mediate the data collection between a patient and a multitude of Disclosers. While large health systems, hospitals, and health plans may have the resources, technical expertise, and staff to coordinate multiple Discloser requests and the corresponding collection of the requested PHI, many small, solo, or rural practices lack the capability to support such a requirement. Physician practices should not be expected to operate as request clearinghouses for complex and potentially costly data exchange scenarios. For example, a solo medical practice acting as an individual's Requester-Recipient could be required to coordinate Disclosers from three local hospitals, two primary care physicians, three specialists, and two sub-specialists. In addition, the patient may not be sure where else their PHI is located and request that their Requester-Recipient physician "ask" a few other medical providers just to be sure. Additional Disclosers could be located across several states. In this example, each Discloser may use a different health IT vendor, use a mix of vendors, use non-certified EHRs, not support electronic exchange, and could be subjected to various state laws impacting the disclosure of PHI. Several of the Disclosers may not provide or make electronic endpoints available, further complicating the request and collection of PHI. Furthermore, the Requester-Recipient would need to task at least one staff member to act as the project manager for this single discloser request—potentially removing staff from direct patient care. Logistically, this example would be challenging for

	sophisticated health systems, let alone a solo medical practice. Health IT fees—both direct and indirect—could quickly suffocate the Requester-Recipient's IT budget. Using this same example, the AMA is concerned individuals will falsely assume their Request-Recipient will receive requested PHI from each Discloser, that the PHI will be complete and accurate, and that the PHI will be disclosed in a timely manner. We believe that OCR is expecting ONC's information blocking regulations will pressure Disclosers to accommodate all Request-Recipient requests. However, as ONC has rightfully noted in its information blocking interim final rule, the COVID-19 pandemic has complicated the implementation of its rules by health care providers and EHR vendors. For example, many of the information blocking technical requirements needed to support OCR's proposal will not be widely available until early 2023. Relatedly, neither ONC nor HHS' Office of Inspector General (OIG) have released sufficient compliance guidance for physicians leaving many confused on how to respond to requests. OCR's proposal would make it possible for third party personal health apps to submit access requests. Personal health apps are not bound by HIPAA Rules—releasing them from any responsibility to act as good stewards of patients' PHI. These apps are not required to meet privacy or security requirements, nor are they required to be transparent or truthful about the intended use of PHI. Individuals may *expect* improved PHI coordination using apps but *experience* actual threats to their privacy. Lastly, Request-Recipients may receive access requests from multiple individuals at the same time—further exacerbating the concerns noted above. **The AMA urges OCR to reconsider its proposal for physicians shoulder the responsibility of Requester-Recipient until costs, technical capabilities, data governance, state laws, and access request management logistics are fully considered.**
y. Whether a covered health care provider or health plan that uses an HIE to make a broadcast query to identify other HIE participants that have PHI about that individual, and that requests the PHI on behalf of an individual, should be considered to be making a	We urge OCR to maintain and reiterate the importance of minimum necessary. There are very few controls within HIPAA related to broadcast queries to covered entities and HIEs. We encourage OCR to ensure there is balance between broad access capabilities and controls around information exchange.

permissible disclosure of PHI for customer service or other administrative or management activities that are part of the covered health care provider or health plan's health care operations. Are there unintended consequences for covered entities or individuals of such an interpretation of health care operations?	
6. Adjusting Permitted Fees for Access to PHI and ePHI	
OCR proposes to: • Specify when electronic PHI (ePHI) must be provided to the individual at no charge. • Amend the permissible fee structure for responding to requests to direct records to a third party.	
Response to Proposals on Fee Proposals	
General Comment bb. Should the Privacy Rule prohibit covered entities from charging fees for copies of PHI when requested by certain categories of individuals (e.g., Medicaid beneficiaries or applicants for or recipients of Social Security Disability Insurance (SSDI)), or when the copies are directed to particular types of entities (e.g., entities conducting clinical research)? cc. Whether the Privacy Rule should prohibit covered entities from denying requests to exercise the right of access to copies of PHI when the individual is unable to pay the access fee. If so, how should a covered entity determine when an individual is unable to pay? ff. How covered entities currently treat access requests that involve converting non-electronic PHI into an electronic format, the fees that are charged for such requests, and how that compares to fees charged for	**The AMA opposes any changes in the Privacy Rule to mandate or require covered entities to charge specific fees for copies of PHI in specific scenarios, or conversely, any prohibition from charging fees.** The AMA agrees with OCR's policy goal and believes that providing individuals with access to their health information is an important component of delivering health care. However, the AMA also believes that physicians individually and collectively should promote access to care for individual patients, in part through being prudent stewards of resources. Thus, physicians have a responsibility to balance patients' needs and expectations with responsible business practices. There is also a distinction between providing access to one's own records and providing copies of records to a third party when considering fees. The Privacy Rule permits covered entities to impose reasonable, cost-based fees when patients request copies of their medical records. Because the Privacy Rule does not include a fee schedule, the fees typically vary by State. As stated before, physicians must continue to balance the right of every patient to access their medical records in a timely fashion with the administrative burden and cost associated with fulfilling those patient requests. One can imagine that as the U.S. population ages, there will be an increase in requests for sizeable medical records—not all of which will be available electronically. According to the U.S. Census Bureau, by "2030, all

similar requests for copies of PHI made by a third party with an individual's valid authorization. gg. How the proposals to narrow the access right to direct PHI to third parties to electronic copies of PHI in an EHR will affect fees for copies of PHI.	baby boomers will be older than age 65. This will expand the size of the older population so that 1 in every 5 residents will be retirement age."[8] Moreover, "[t]he aging of baby boomers means that within just a couple decades, older people are projected to outnumber children for the first time in U.S. history[.]"[9]Additionally, more than 77 million individuals were enrolled in Medicaid and CHIP according to reported enrollment data for September 2020.[10] The cost required to respond to an individual's request for a copy of their PHI will vary with each request, and within each practice and health care system. Older Americans with chronic health conditions may have records that take much more time to assemble than those of someone younger with no chronic health conditions. The Department should take note of the changing demographics and balance it with the burden placed on physicians, their staff, and their practices. The AMA believes that encouraging covered entities to waive access fees in certain cases, is not only a key driver of delivering health care to all patients, but by waiving access fees in certain situations covered entities can take a proactive role in fostering an environment that allows for equity. We believe cultivating an environment where all patients, including those from historically minoritized and marginalized groups, have access to their PHI is an important first step in combatting the health inequities that exist in our country. However, mandating or prohibiting access fees is not the answer. The proposal could have the unintended consequence of forcing practices, particularly smaller practices or those in urban areas, to reduce the time they spend caring for patients in order to fulfill these requests for medical records at no cost. The AMA, like OCR, will continue to encourage covered entities that charge fees for copies of PHI to waive fees or provide flexibility in payment (such as delaying charges or accepting payment in installments, without delaying the provision of copies) for individuals who are unable to pay upfront due to an emergency or a lack

[8] https://www.census.gov/newsroom/press-releases/2018/cb18-41-population-projections.html
[9] *Id.*
[10] https://www.medicaid.gov/medicaid/program-information/medicaid-and-chip-enrollment-data/report-highlights/index.html

	of resources. The AMA has repeatedly and proactively communicated to members that records access should not be viewed as an opportunity to generate revenue.[11]
aa. Whether the term "internet-based method" or alternative terms adequately describe online patient portals, mobile applications, APIs, and other related technologies. If there are unintended consequences associated with using such broad terminology, are there ways in which any unintended adverse effects could be minimized? (p. 6469)	The AMA agrees with the notion that fees should not be charged to patients for accessing their information through a patient portal or other internet-based method. The AMA is concerned, however, that OCR's proposal would prohibit health care providers from charging reasonable fees for internet-based access by business and commercial third parties. OCR's rationale for the prohibition on fees (that the information is electronically available) fails to account for the frequency with which the required information resides on multiple systems and compiling the information must be done manually. OCR's fee structure should recognize, as ONC's does, a difference when manual efforts are required.
jj. Whether the Department should establish in regulation a separate required timeframe for covered entities to respond to individuals' requests for access fee estimates or an itemized list of charges, and what timeframe(s) would be appropriate, and whether the time to respond to a request for access should be tolled pending an individual's confirmation that it desires the requested information given the fee estimate.	While this policy may be helpful to some patients, requiring covered entities to respond to individuals' requests for access fee estimates or an itemized list of charges would add to the amount of work practice staff must undertake to fulfill an access request. Most importantly, time spent responding to requests about fee estimates is time taken away from fulfilling actual record requests. We encourage OCR to not pursue this approach through regulation but rather focus efforts on ensuring that covered entities and patients understand what covered entities may charge for records requests under federal law. This educational approach would help to promote consistency and transparency around fees.
7. Notice of Access and Authorization Fees	
OCR proposes to require covered entities to post estimated fee schedules on their websites for access and for disclosures with an individual's valid authorization and, upon request, provide individualized estimates of fees for an individual's request for copies of PHI, and itemized bills for completed requests.	
Response to Proposals on Notice of Access and Authorization Fees	

[11] https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf; https://www.ama-assn.org/practice-management/digital/patient-access-playbook-faqs; https://www.ama-assn.org/system/files/2021-03/Patient-access-playbook-Key-points-to-remember.pdf

kk. Whether there should be a legal consequence to covered entities for the bad faith provision of an incorrect estimate of fees for access and authorization requests, and if so, what actions should be considered evidence of bad faith sufficient to subject a covered entity to potential penalties.	Because a notice of access and authorization fees would already impose a new requirement of covered entities, and because it is often difficult to know in advance what fulfilling a request for records may entail, the AMA believes it would be premature to create a legal consequence associated with fee estimates. We encourage OCR to consider possible alternatives. For example, a physician practice can (and should) communicate with a requestor if it appears as though their records request will result in higher fees than originally anticipated or communicated. At that point—as long as the practice is within the bounds of what they are allowed to charge the requestor under law—the requestor may agree to pay the fees or may decide to narrow the request to reduce the associated fees. The AMA has repeatedly and proactively communicated to members that records access should not be viewed as an opportunity to generate revenue and therefore think this specific proposal is unnecessary.[12] Should the Department finalize this proposal, the AMA would like to collaborate with OCR on ways to ensure covered entities receive the education they need.

8. Technical Change to General Rules for Required Business Associate Disclosures of PHI

OCR proposes to clarify 45 CFR 164.502(a)(4)(ii), which currently requires business associates to provide copies of PHI to covered entities, individuals, or individuals' designees, to satisfy the covered entity's obligations under the right of access. To clarify when a business associate must disclose PHI and to whom, the proposal would specify that a business associate is required to disclose PHI to the covered entity so the covered entity can meet its access obligations. However, if the business associate agreement provides that the business associate will provide access to PHI in an EHR directly to the individual or the individual's designee, the business associate must then provide such direct access.

Response to Technical Change

The AMA supports this proposal.

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

OCR proposes to:

- Expressly prohibit a covered entity from imposing unreasonable identity verification measures on an individual (or his or her personal representative) exercising a right under the Privacy Rule.

[12] https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf

- Clarify within the regulatory text 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 covered entity.

Response to Proposals on Identity Verification

The AMA supports this proposal. We agree with OCR that it is important to verify the identity of each patient, and that verification measures should not become an unreasonable obstacle to the patient accessing medical records. The AMA has been vocal about educating its members that imposing burdensome verification requirements on individuals seeking to obtain their PHI pursuant to the individual right of access is unacceptable. We agree that the Privacy Rule should not mandate any particular form of verification (such as viewing an individual's driver's license at the point of service), but instead generally leave the type and manner of the verification to the discretion and professional judgment of the covered entity, provided the verification processes and measures do not create barriers to, or unreasonably delay, the individual from obtaining access to their PHI. Moreover, the AMA has repeatedly and proactively communicated to members that covered entities may not require an in-person verification upon receiving a patient's request for records or any other verification mechanism that creates an unreasonable obstacle. Instead, the AMA encourages physicians to seek to verify the patient's identity, by obtaining information that is not publicly known (such as the last four digits of the patient's Social Security number) or having the patient transmit a copy of a government ID.[13] Should the Department finalize this proposal, the AMA would like to collaborate with OCR on ways to ensure covered entities receive the education they need.

C. Amending the Definition of Health Care Operations To Clarify the Scope of Care Coordination and Case Management (45 CFR 160.163)

OCR proposes to amend the definition of health care operations to clarify the scope of permitted uses and disclosures for individual-level care coordination and case management that constitute health care operations.

Response to Proposals on Amended Definition of Health Care Operations

The Department requests comments on the benefits and costs of clarifying the definition of health care operations, including information on how, if at all, this clarification would affect covered entities' decision-making regarding uses and disclosures of PHI for these purposes, and on any potential unintended adverse consequences.	We appreciate OCR's desire for clarity in its regulatory definitions. We caution OCR against finalizing this proposal along with the proposal to create an exception to the minimum necessary standard for such disclosures. As explained in the next section, OCR appears to consider care coordination and case management to be both treatment activities and health care operations, which is somewhat confusing. The AMA defines "health care operations" narrowly to include only those activities and functions that are routine and critical for general business operations and that cannot reasonably be undertaken with de-identified information. Policy crafted by our House of Delegates dictates that payers should have access to medical records and

[13] https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf

	individually identifiable health information solely for billing and payment purposes, and routine and critical health care operations that cannot reasonably be undertaken with de-identified health information. We urge OCR to take a cautious approach to expanding access to individual level PHI without accompanying safeguards and controls for patient privacy.
D. Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management (45 CFR 164.502(b))	
OCR proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management.	
Response to Proposals on Exception to Minimum Necessary	
General feedback on the proposal.	The AMA strongly opposes the addition of an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management. AMA policy states that "any information disclosed should be limited to that information, portion of the medical record, or abstract necessary to fulfill the immediate and specific purpose of disclosure."[14] Our policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship. This is particularly important in scenarios involving sensitive health information. For example, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders (SUD) to seek treatment. Consumers are also increasingly concerned with privacy in today's environment. In fact, many industries, states, and countries are moving towards increasing privacy rights and protections, not expanding ways in which information can be shared without an individual's consent. Additionally, PHI accessed by health plans can lead to selective, discriminatory reimbursement models and intrusion on physician medical decision-making power (e.g., paying less for certain types of care that a physician deems necessary or in the best interest of the patient). Furthermore, physician practices could be priced out of

[14] Patient Privacy and Confidentiality H-315.983

	markets if a health plan uses the requested PHI to determine they are a "second or third-tier" option. **The AMA strongly opposes any policies that remove limits on health plan access and use of PHI.** OCR has not proposed the necessary security or privacy guardrails to protect patients or physicians from PHI data abuse. Moreover, physicians must not be forced to turn over PHI to a health plan simply to facilitate information blocking and HIPAA compliance. Additionally, we note that OCR states that "covered entities would continue to be able to agree to and honor an individual's request not to use or disclose information for these purposes, as provided in the Privacy Rule and the ONC Cures Act Final Rule information blocking exception for respecting an individual's request."[15] Unfortunately, the Privacy Rule only *requires* covered entities to agree to such requests from individuals if the disclosure is (1) for the purpose of payment or health care operations and not otherwise required by law, and (2) pertains solely to health care for which the individual has paid in full out of pocket.[16] This serves an example of how OCR is proposing to broaden information exchange without ensuring that appropriate counterbalances are in place to protect patient privacy when the patient desires it.
a. Would the proposed exceptions improve the ability of covered entities to conduct care coordination and case management activities? Why or why not? Please provide any cost or savings estimates that may apply both on the entity level and across the health care system.	We urge OCR to prioritize patient privacy over costs/savings to the health care system.
c. Please describe any unintended negative consequences of the proposed changes for the privacy of PHI or the health information rights and interests of individuals. Would there be any negative impact, in particular, on certain populations (e.g., people with disabilities, older adults, rural dwellers, persons experiencing mental health	Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as "sensitive"—and policymakers must be very cautious in discussions of how to relax regulation around privacy. We must always ask whether relaxing privacy controls will encourage patients to seek care or potentially deter them. Privacy risks include re-identification of patients through de-identified (or partially de-identified) data,

[15] 86 Fed. Reg. 6446 (Jan. 21, 2021) at 6474.
[16] 45 CFR 164.522(a)(vi)

conditions and/or substance use disorders or other illnesses, or others)?	misunderstanding or disregard of the scope of a patient's consent, patient perception of loss of their privacy leading to a change in their behavior, embarrassment or stigma resulting from an unwanted disclosure of information or from fear of a potential unwanted disclosure, perceived and real risks of discrimination including employment and access to or costs of insurance, and law enforcement accessing data repositories beyond their intended scope. Inequitable data governance disproportionately harms historically minoritized and marginalized communities. This harm occurs even as such communities "are most in need of privacy in order to avoid downstream discrimination and other negative consequences that often results when their sensitive information, including but not exclusively information directly [related] to their minority status, is disclosed."[17] We urge OCR not to finalize any proposals that could result in the broad or unexpected use of personal information.
f. A health care provider that refused to disclose PHI would not be considered to be information blocking when a state or federal law requires one or more preconditions for providing access, exchange, or use of electronic health information and the precondition has not been satisfied. This proposed modification would remove one of the minimum necessary policy "preconditions" for refusing to respond to a request for an individual's PHI without violating the information blocking prohibition. How would the information blocking provisions in the ONC rule interact with these modifications, and are there any adverse unintended consequences that might result, such as covered entities requesting and receiving far more than the minimum amount of PHI necessary for individual-level care coordination and case management and using PHI for other unrelated purposes?	ONC correctly includes an "minimum necessary condition" within its information blocking Privacy Exception, allowing physicians to withhold access, exchange, or use of EHI if requests exceed the necessary amount of information needed to meet the purpose of use. Health plans are not required to ensure PHI is used exclusively for care coordination or case management and are not required to specify the purpose of use for the requested PHI. **Until controls and policies are made available to limit a health plan's secondary, tertiary, or downstream uses of PHI, OCR should not remove the minimum necessary requirement.** The minimum necessary precondition avails physicians with an opportunity to review requests and limit unnecessary or inappropriate uses or disclosures. ONC's information blocking regulations convert *permitted* disclosures into disclosure *requirements*. That is, physicians must send all requested PHI to a requesting health plan without delay or unless an exception can be identified. Congress recognized the need for reasonable and appropriate information blocking exceptions—particularly for patient privacy and safety. Without an appropriate level of review or evaluation, physicians will not be able to act in their patient's best interest, nor will they be able to counter health plan requests for PHI that can be used to discriminate against patients or interfere with a physician's autonomy.

[17] Skinner-Thompson, Scott (2020-11-04T22:58:59). Privacy at the Margins. Cambridge University Press. Kindle Edition.

	The AMA agrees that reducing the difficulties inherent in accessing medical information at the individual level is an important goal; however, we have concerns with the potential pitfalls of health plans having unprecedented access to wide swaths of information across the health care system. This is particularly concerning given the highly automated nature of PHI requests by health plan information systems. Current data request processes, while limiting, are narrowly scoped for specific use cases and involve some level of "gating" that helps prevent improper use and disclosure and helps enforce compliance on both ends of the transaction (collection (query) and disclosure). **The AMA maintains that an expressed "need" for information—including for care coordination or case management purposes—does not confer a right to such information, particularly when it conflicts with a patient's wishes.** Patients currently have no assurances that requests to not disclose information will be honored, other than self-pay patients seeking to limit disclosures to health care plans for payment purposes. Removing the minimum necessary standard without accompanying—and increasingly necessary—controls on PHI requests and use, individual privacy rights will be diminished as a consequence. Exploiting the link between minimum necessary and information blocking requirements may also lead to "bullying." For example, physicians already have established processes to determine what constitutes the minimally necessary amount of information to process claims. This balances adjudication needs with clinical judgment and patient privacy. As proposed, OCR's removal of minimum necessary protections, along with ONC's information blocking regulations, will empower payers to demand more information than is needed without providing any assurances on its use. Patients trust physicians to safeguard access to their most personal information, only sharing it for appropriate purposes and with their consent. OCR seems to conflate health plans' assertion of need with actual patient care. **The AMA again stresses that removing minimum necessary for care coordination and case management empowers health plans to make unilateral decisions as to what information is needed, overriding physician discretion and patient choice.**

	Lastly, payers are not subject to information blocking requirements and are therefore emboldened to use (and withhold) information as they see fit. Unfortunately, under ONC's regulations, a physician who denies a payer's request for EHI—regardless of whether the request is fully warranted—may implicate the physician in information blocking. The minimum necessary precondition exception is currently the only mechanism to protect patient privacy and limit abuse by health plans. **OCR must evaluate methods to limit PHI use to that of a health plan's stated purpose, including creating compliance enforcement and monitoring capabilities.**
g. Some disclosures for payment purposes with respect to an individual's health care are related to care coordination and case management (e.g., review of health care services for appropriateness of care). Disclosures for payment purposes are subject to the minimum necessary standards. Should all or certain individual-level payment activities be included in the proposed exception?	No, individual-level payment activities should not be included in the proposed exception. The AMA strongly supports and advocates for a minimum necessary standard of disclosure for individually identifiable health information requested by payers. The information necessary to accomplish the intended purpose of the request should be determined by physicians and other health care providers.
h. Please provide additional examples of circumstances in which it should be considered reasonable, or unreasonable, to rely on the representations of another entity that it is requesting the minimum necessary PHI.	It should be reasonable for covered entities to rely on the representations of public health authorities requesting PHI that the public health authority is requesting the minimum necessary PHI.
E. Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations (45 CFR 164.506)	
OCR proposes to create a new section of HIPAA that would expressly permit covered entities to disclose PHI to social services 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 health care provider or as a health care operations activity of a covered health care provider or health plan. Under this provision a health plan or a covered health care 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 health care provider. Instead, the third party may be providing health-related social services or other supportive services—e.g., food or sheltered housing needed to address health risks.	

Responses to Proposals on Disclosing PHI to Third Parties	
a. Whether the proposal to create an express permission to disclose PHI to certain third parties for individual level treatment and health care operations would help improve care coordination and case management for individuals, and any potential unintended adverse consequences. b. Whether the proposal poses any particular risks for individuals related to permitting disclosures without authorization for individual-level care coordination and case management activities that are health care operations (i.e., those that are conducted by health plans) in addition to individual-level care coordination and case management activities that constitute treatment (i.e., those that are conducted by health care providers). f. Should OCR specify the types of organizational entities to be included as recipients of PHI in this express permission in regulation text, as well as limitations or exclusions, if any, that should be placed on the types of entities included? If yes, what types of organizational entities should be included or excluded? h. To what extent are social services agencies, community-based organizations, and HCBS providers covered health care providers under HIPAA? How many are non-covered health care providers? Are any such entities covered under HIPAA as health plans?	The AMA agrees with OCR that certain individuals can benefit from social service agencies and community-based support programs (collectively, community-based organizations, or CBOs). Such programs often provide needed assistance to individuals who may not otherwise receive it. We also understand why access to a patient's PHI can be beneficial to an individual particularly in the case of homelessness, limited access to health care services, or patients receiving multiple supports across a spectrum of services. Physicians often struggle with how to best care for these patients without violating HIPAA. However, permitting covered entities to disclose PHI to a non-health care provider without a patient's authorization presents challenges, as outlined in this section of our comments. Just as it is difficult to truly define "health data", it is difficult to define "health-related social services or other supportive services." This is an incredibly broad description that could a wide range of organizations, including community-run food pantries, halfway houses, crisis pregnancy centers, churches, schools, and day cares run out of an individual's home. **While covered entities should not be restricted from providing PHI to any of these entities at a patient's request, we have significant concerns about how OCR's current proposal would be implemented, particularly in light of ONC's information blocking requirements, which will require covered entities to supply such information.** In fact, the patient may not always even be aware of what information the CBOs are requesting from their physician. Since the information blocking regulations will compel a physician to disclose such information upon request, a patient may not have the opportunity to ask their physician not to share certain pieces of information—physicians will also be unable to utilize the "precondition not satisfied" exception of the information blocking regulations that would have allowed the physician to check with a patient before release of PHI. So, for example, a church might request information about an individual's medical appointments with the intent of assisting the patient with transportation to those appointments. But if the church receives information revealing the patient's homosexual sexual orientation or HIV-positive status, the patient may experience repercussions within his or her church community. Additionally, there are no restrictions around how the CBO may further use or disclose the information to

	other third parties, which is a significant risk to patient privacy of which patients may be unaware. They may think that if their physician is sending information to a CBO for "health related" services, that the information will remain confidential—something for which there is no guarantee under the current proposal. At a minimum, OCR should ensure that covered entities inform the patient in a timely manner of (1) who the information shared with; (2) what information was shared; and (3) the intended purpose of the disclosure. This requirement should be separate and apart from the accounting of disclosures policy that has yet to be implemented via regulation. OCR should also consider that CBOs may not have EHRs or any other type of digital data system with privacy/security safeguards to ensure the confidentiality and integrity of the individual's PHI. We raise this simply as a potential unintended consequence—we understand that this proposal would not require physicians to verify that the recipient has any particular controls. But this potential unintended consequence is significant, particularly in small communities where word travels fast. CBOs may not have access controls or really any way of ensuring that information about a patient is not accessible to anyone within the organization who does not need to know it. The vast majority of CBOs are under no legal obligation to ensure the privacy and security of PHI. Such assurances are very important for both physicians and patients and will be necessary to truly assist with improved health outcomes. It is inappropriate to open the door to *required* PHI disclosure to entities that do not have the resources and infrastructure to protect the information. This does not mean that we should not work towards facilitating such information exchange. Rather, **prior to implementing regulatory changes, OCR and other federal agencies should prioritize additional financial, technical, and human resources to CBOs to help them manage the confidentiality of PHI.**
e. Would this permission to disclose PHI for case management and care coordination to the entities described above interact with the ONC information blocking requirement to create any unintended adverse consequences for individuals' privacy? Please explain.	**The AMA recognizes the potential benefit of community-based organizations having access to a patient's PHI. However, OCR has not established appropriate counterbalances to mitigate oversharing of information. We recommend OCR postpone changing the PHI disclosure to certain third parties process until technical and legal frameworks are in place to protect patient privacy.** ONC's

	information blocking regulations convert HIPAA-permitted disclosures and rights of access into a requirement and obligation for physicians to disclose PHI if requested. For example, OCR's proposal would allow a community food pantry (providing supportive services) to request PHI from a patient's oncologist. As an Actor under information blocking regulations, the oncologist would be required to disclose the requested food and medication allergy PHI stored in the physician's EHR. However, the oncologist's EHR cannot send just the allergy information so it instead sends a consolidated clinical document containing office notes, diagnostic results (including genetic tests), and problem list along with the patient's allergies. This lack of granular data management is common across EHR products. While ONC's regulations provide for exceptions allowing the physician to withhold information in some instances (e.g., when an EHR cannot segment data in compliance with state or federal law), identifying and documenting exceptions is complex and arduous, possibly resulting in an oversharing of information. Additionally, physicians are receiving inconsistent education and support from their EHR vendors on information blocking compliance. Clearly, a community food pantry should not have access to sensitive medical information. Yet, fear of not being HIPAA and information blocking compliant—coupled with limited EHR functionality and support—may promote risky data sharing practices impacting patient privacy. We urge OCR to consider ways in which it can support the development and use of technology to manage patient privacy. For example, an organization could implement a security labeling service to tag data with special privacy considerations. Essentially, information is "tagged" to identify where the information originated, for what purposes it can be disclosed, and to whom. The need for such technology is increasingly critical as data continues to be generated outside of the clinical setting and would help to solve burden associated with using and disclosing multiple types of sensitive data such as SUD, HIV-status, genetic information, minors' health information, and reproductive health information. While we recognize that segmentation efforts do not seem to have been prioritized by developers, such technology currently exists, as recognized by ONC's Draft Report to Congress (Draft Report) on reducing regulatory and administrative burden relating to the use of health IT and EHRs:

	"[With respect to difficulty implementing Part 2 and integrating such information into EHRs,] HHS has recognized these implementation challenges and encourages the use of health IT to help clinicians appropriately share sensitive information while complying with legal requirements and respecting patient privacy preferences. For example, technical standards exist for electronically tagging health information to indicate privacy considerations, including legal requirements, within a patient record or summary of care document within the EHR, and SAMHSA supports ONC's Data Segmentation for Privacy initiative [DS4P] to support clinicians sharing of health information in accordance with patient choices. These tags on data elements, segments, or whole documents can then be used by automated access control solutions to prevent unauthorized access to patient data."[18] ONC recommended in its Draft Report that HHS monitor, test, and support development of technical standards for data segmentation. We wholeheartedly agree with this recommendation, and strongly urge the administration to demonstrate its commitment to greater interoperability and privacy protections by prioritizing data segmentation in development, testing, and policy-making. We note that while technology exists to segregate data and software can help to electronically manage patient consent (e.g., Consent2Share), we have heard from physicians and health systems that such segregation functionality is costly to implement, and that open-source consent management software can be prohibitively expensive to incorporate into a customized EHR. We urge the administration to recognize the pressing need for data segmentation to be made accessible and affordable to physicians. Such capabilities will enhance interoperability, strengthen the patient-physician relationship through a patient's increased confidence that a physician will not share data in a way that violates the patient's trust, and improve care coordination and patient outcomes resulting from a physician's ability to access sensitive information. Furthermore, such data segmentation capabilities would help to ease the burden stemming from physicians' compliance with state privacy laws. Congress and HHS

[18] *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs*, available at https://www.healthit.gov/sites/default/files/page/2018-11/Draft%20Strategy%20on%20Reducing%20Regulatory%20and%20Administrative%20Burden%20Relating.pdf, p. 44.

	should reject the approach of legislating and regulating around these problems and instead focus on developing data segmentation standards and software, while ensuring that such technology is widely available and affordable. **OCR should support the efforts of organizations who adopt such technology to promote both access and privacy by creating safe harbors from breach enforcement for organizations that adopt security labeling services.**
g. Should OCR limit the proposed permission to disclose PHI to circumstances in which a particular service provided by a social services agency, community-based organization, or HCBS provider is specifically identified in an individual's care plan and/or for which a social need has been identified via a screening assessment? Should OCR require, as a condition of the disclosure, that the parties put in place an agreement that describes and/or limits the uses and further disclosures allowed by the third party recipients?	We appreciate these questions. We support the concept of limiting disclosures to CBOs that the physician and patient discuss together, in advance of releasing the information. The information released should be limited to that which the patient is comfortable releasing to a particular CBO. We also support the concept of the parties creating an agreement describing the permitted uses and disclosures by the recipient, including to third parties. **OCR should explore options for data sharing agreements between covered entities and CBOs in their patients' communities that aim to reduce friction while still maintaining patient privacy.** Information sharing concepts are explored in an issue brief by the National Center for Medical-Legal Partnership, housed within the Milken Institute School of Public Health at the George Washington University.[19]
F. Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder, Serious Mental Illness, and in Emergency Circumstances (45 CFR 164.502 and 164.510-514)	

• Replacing the privacy standard that permits covered entities to make certain uses and disclosures of PHI based on their "professional judgment" with a standard permitting such uses or disclosures based on a covered entity's good faith belief that the use or disclosure is in the best interests of the individual. The replacements would be made in the following sections: 45 CFR 164.502(g)(3)(ii)(C), 164.510(a)(3), 164.510(b)(2)(iii), 164.510(b)(3), 164.514(h)(2)(iv).
  • The professional judgment standard presupposes that a decision is made by a health care professional, such as a licensed practitioner, whereas good faith may be exercised by other workforce members who are trained on the covered entity's HIPAA policies and procedures and who are acting within the scope of their authority.
  • The proposed standard is more permissive in that it would presume a covered entity's good faith, but this presumption could be overcome with evidence of bad faith.	

[19] *Information Sharing in Medical-Legal Partnerships: Foundational Concepts and Resources*, available at https://medical-legalpartnership.org/wp-content/uploads/2017/07/Information-Sharing-in-MLPs.pdf.

• Expanding the ability of covered entities to disclose PHI to avert a threat to health or safety when a harm is "serious and reasonably foreseeable," instead of the current, stricter standard, which requires a "serious and imminent" threat to health or safety.	
Response to Proposals on Disclosures of PHI Related to Substance Use Disorder, Serious Mental Illness, and Emergencies	
General feedback	A widespread perception exists that HIPAA prevents physicians from sharing information—especially related to behavioral health and substance use disorder (SUD)—with families and caretakers. This is not true. The HIPAA Privacy Rule does not prohibit communication with a patient's family members (not only parents), friends, or others involved in the patient's care. The HIPAA Privacy Rule does not prohibit physicians from listening to family members or other caregivers who may have concerns about the health and well-being of the patient, so the physician can factor that information into the patient's care. In fact, there is no record of OCR or the Department of Justice ever pursuing civil or criminal HIPAA enforcement against covered entities sharing information with family or caregivers to facilitate treatment or payment. Yet, this Proposed Rule states it seeks to "ensure that HIPAA is not a barrier in instances when entities believe a disclosure of PHI is necessary to prevent harm to the individual and to others."[20] To be clear, in recognition of the integral role that family and friends play in a patient's health care, the HIPAA Privacy Rule already allows often routine—and sometimes critical—communications between health care providers and these persons.[21, 22] Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient's family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. The provider may ask the patient's permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment,

[20] 86 Fed. Reg. 6446, 6483 (Jan. 21, 2021).
[21] 45 CFR § 164.510(b). *See also HIPAA Privacy Rule and Sharing Information Related to Mental Health*, available at https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf.
[22] *Information Related to Mental and Behavioral Health, including Opioid Overdose*, available at https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html.

	that the patient does not object. Where a patient is not present or is incapacitated, a health care provider may share the patient's information with family, friends, or others involved in the patient's care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interest of the patient. The proposed changes to 45 CFR 164.502 and 164.510-514 are not necessary and risk ushering in a host of unintended consequences. As the Legal Action Center points out, the proposals could disproportionately impact historically marginalized and minoritized populations: "Due to stigma and the criminalization of substance use, it is easy to foresee ways that this would end up harming patients, who may end up losing their housing, employment, child custody, or other rights if the covered entity shares information against their wishes…It is also easy to foresee ways that this could disproportionately harm certain patients more than others – patients who are Black, indigenous, other people of color, undocumented patients, patients with concurrent mental health diagnoses, or patients with more highly stigmatized substance use histories (e.g., injection drug use)."[23] OCR should not finalize policies that run the risk of further endangering these populations. Additionally, while not formally proposed, OCR questions whether to expand the circumstances under which a covered entity may disclose PHI in a manner inconsistent with a patient's privacy preferences. **The AMA strongly opposes changes that would expand the ability of covered entities to disclose PHI against a patient's wishes.** Instead, OCR should promote policies that center the patient's desires around how his or her information is disclosed to third parties, including friends and family. For example, **we urge OCR to expand the definition of "harm" to include situations in which, according to professional judgement, such access may cause mental and emotional harm to patients whose most personal information—that which relates to their health—is disclosed against their wishes.** Such disclosures can be incredibly destabilizing and upsetting to patients, which could potentially lead to complications with or setbacks in recovery and treatment, or even deter patients from seeking treatment in the first place.

[23] *Will Biden's HHS Protect OD Survivors' Medical Privacy Rights?*, available at https://filtermag.org/hhs-overdose-privacy/ (Jan. 25, 2021)

	Specifically, adolescents must be permitted to avail themselves of this right to ensure their records will not be disclosed to personal representatives in a way that would result in mental and emotional harm. **Additionally, we encourage OCR to follow the lead of many states and establish a federal mature minor policy.** Mature minors, defined by AMA policy as "certain older minors who have the capacity to give informed consent to do so for care that is within the mainstream of medical practice, not high risk, and provided in a nonnegligent manner," should have a federal right to access confidential medical, psychiatric, and surgical care without parental consent and notification—and the access rights that are granted to parents as the minor's personal representative. Federal law should support physicians and other health care professionals in their role in providing confidential health care to their adolescent patients while permitting physicians to inform parents about a minor's treatment if allowed by state law and if the minor (with decision-making capability) does not object. OCR should work with ONC to ensure that both the mature minor and the emotional and mental harm exceptions described above are available as exceptions to information blocking.
a. Would the proposed change in standard from "professional judgment" to "good faith belief" discourage individuals from seeking care?	**We urge OCR to maintain the current "professional judgement" standard and not to finalize its proposal to permit disclosures under a "good faith belief" standard.** Professional judgement develops over years of training and experience, whereas a "good faith" belief can be rendered by anyone. Additionally, one develops insight into the totality of a patient's circumstances within the context of a clinical relationship. For these reasons—training, experience, and relational context—clinicians are better equipped, for example, than front desk staff to make determinations about when information should be shared. Indeed, confidentiality is a core tenet of the medical profession. The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship. This is particularly important in scenarios involving sensitive health information. For

	example, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders (SUD) to seek treatment. Consumers are also increasingly concerned with privacy in today's environment (e.g., the Facebook–Cambridge Analytica data scandal). In fact, many industries, states, and countries are moving towards increasing privacy rights and protections, not expanding ways in which information can be shared without an individual's consent. **Any change in policy that decreases the level of privacy a patient may receive during or after seeking care threatens to discourage individuals from seeking care.**
b. Should the Department apply the good faith standard to any or all of the other nine provisions in the Privacy Rule that call for the exercise of professional judgment? Are there circumstances in which it would be inappropriate to apply a presumption of compliance across the other nine provisions?	OCR should not apply the good faith standard to any of the other nine provisions in the Privacy Rule that call for the exercise of professional judgement for the reasons described above.
c. Should 45 CFR 164.510(b)(3) be revised to permit a covered entity to disclose the PHI of an individual who has decision making capacity to the individual's family member, friend, or other person involved in care, in a manner inconsistent with the individual's known privacy preferences (including oral and written expressions), based on the covered entity's good faith belief that the use or disclosure is in the individual's best interests, in any situations outside of an emergency circumstance? Put another way, are there examples in which the totality of the facts and circumstances should or would outweigh an individual's preferences, but do not rise to the level of posing a serious and reasonably foreseeable threat	**The AMA generally opposes proposals to expand authorities for disclosing PHI against an individual's known privacy preferences (including oral and written expressions), particularly if such disclosures are based merely on a covered entity's good faith belief. Expanding these authorities would drastically undermine the trust inherent in and critical to the patient-physician relationship, while violating legal and societal norms around privacy, autonomy, and free will.** The AMA's Code of Medical Ethics states that patients generally are entitled to decide whether and to whom their PHI is disclosed. Patients need to be able to trust that physicians will protect information they have shared in confidence. They should feel free to fully disclose sensitive personal information to enable their physician to most effectively provide needed services. Physicians in turn have an ethical obligation to preserve the confidentiality of information gathered in association with the care of the patient.[24]

[24] *AMA Code of Medical Ethics, 3.2.1 Confidentiality*, available at https://policysearch.ama-assn.org/policyfinder/detail/3.2.1%20Confidentiality?uri=%2FAMADoc%2FEthics.xml-E-3.2.1.xml

under 45 CFR 164.512(j)? Are there examples related to individuals who have regained capacity after having been formerly incapacitated, such as where an individual recovering from an opioid overdose leaves the hospital against medical advice or leaves a residential treatment program?	Patient consent continues to be a critical consideration in the use and disclosure of PHI. The AMA has continuously maintained that an expressed "need" for information—including for individuals with SUD or serious mental illness—does not confer a right to such information, particularly when it conflicts with a patient's wishes. Some parties may reject this principle as too deferential to patients' rights at the expense of administrative feasibility. However, the AMA believes that this approach properly balances the interests at stake. We encourage OCR to embed these tenets of confidentiality into federal policy.
d. When should overriding an individual's prior expressed preferences constitute bad faith on the part of the covered entity, which would rebut the presumption of compliance? Are there instances in which overriding an individual's prior expressed preferences would not constitute bad faith on the part of the covered entity?	Proposals contemplating overriding an individual's prior expressed preferences set the stage for an incredibly slippery slope. The AMA strongly urges OCR to resist expanding the current ability of covered entities—or any other type of entity, including smartphone apps and third parties—to override an individual's privacy preferences.
e. Would the proposed "serious and reasonably foreseeable threat" standard discourage individuals from seeking care?	**The proposed standard of "serious and reasonably foreseeable threat" could discourage some individuals—particularly those from historically marginalized and minoritized populations—from seeking care. OCR should not finalize this proposal.** Patients experiencing serious mental illness or SUD often find trusted, confidential refuge in their clinicians. Additionally, word spreads quickly among patient communities about how PHI related to SUD or serious mental illness may be shared. A decrease in privacy protections will absolutely have a chilling effect on individuals seeking care.[25] While important work is being done to remove stigma and regard SUD as a medical issue like any other medical issue, the fact remains that "disclosure of SUD-related

[25] *As 42 CFR Part 2 faces possible demise, methadone patients panic, taper*, available at https://onlinelibrary.wiley.com/doi/10.1002/adaw.32018 (July 2, 2018). While this article is focused on 42 CFR Part 2, it demonstrates the importance of privacy to patients seeking treatment for SUD. *See also* Knopf, A., *42 CFR Part 2 Faces Tough Going in Congress*, available at https://atforum.com/2018/09/42-cfr-part-2-faces-tough-going-congress/ (Sept. 4, 2018)

	information can have serious consequences" and SUDs are "widely stigmatized."[26] Furthermore, most substance use is illegal, creating a complex privacy dynamic that patients with other medical conditions do not experience. In fact, before enacting a law requiring that police and prosecutors obtain warrants before searching in sensitive patient information in the state's prescription monitoring database, Massachusetts allowed police and prosecutors to view patient medical records without warrants nearly 11,000 times—or about 20 times per day—between August 2016 and March 2018.[27] Massachusetts changed that policy because it realized it harmed patient outcomes. **Patients should not never to worry about their health care needs potentially exposing them to law enforcement suspicion or investigation.** Additionally, as mentioned in the general comment on this section, a changed standard may disproportionately impact historically marginalized and minoritized populations, many of which are already disproportionate targets of law enforcement and face discrimination rooted in systemic racism and white supremacy. Indeed, Black and Hispanic/Latinx individuals experience higher rates of incarceration than white individuals relative to the population.[28] Health care professionals are not immune from conscious and unconscious bias; such bias may result in patients of color disproportionately being identified as posing a "serious and reasonably foreseeable threat" simply based on the color of their skin. A change to the harm standard could result in historically minoritized and marginalized patient populations being subjected to additional encounters with law enforcement, suffering additional losses of medical privacy compared to their peers, and becoming increasingly wary of seeking out needed care—all of which will increase our nation's existing health inequities.

[26] *Medicaid and CHIP Payment and Access Commission's (MACPAC) statement in its June 2018 Report to Congress on Substance Use Disorder Confidentiality in Regulation and Care Integration in Medicaid and Chip (MACPAC Report)*, available at https://www.macpac.gov/wp-content/uploads/2018/06/Substance-Use-Disorder-Confidentiality-Regulations-and-Care-Integration-in-Medicaid-and-CHIP.pdf

[27] *Police in Massachusetts Must Get a Warrant to Access Patient Data*; American Civil Liberties Union Massachusetts; Kate Crockford; available at https://www.aclum.org/en/publications/victory-police-massachusetts-must-now-get-warrant-access-sensitive-patient-data

[28] *The Color of Justice: Racial and Ethnic Disparity in State Prisons*, available at https://www.sentencingproject.org/publications/color-of-justice-racial-and-ethnic-disparity-in-state-prisons/ (June 14, 2006)

f. Would the proposed standard improve a covered entity's ability to prevent potential harm, such that the benefits of the change would outweigh potential risks? Please provide examples.	**We do not believe the proposed standard would improve a covered entity's ability to prevent potential harm and, in fact, harm may result from the change.** As OCR's own guidance notes, "HIPAA regulations allow health professionals to share health information with a patient's loved ones in emergency or dangerous situations – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose."[29] The guidance further states, "health care providers have broad ability to share health information with patients' family members during certain crisis situations without violating HIPAA privacy regulations."[30] The answer to a covered entity's failure to understand the HIPAA privacy rules is not stripping patients their privacy rights. In sum, **changing this standard is not necessary to accomplish OCR's policy goals and would not achieve benefits that outweigh the potential risks and harms.**
h. Are there potential unintended consequences related to granting extra deference to a covered health care provider based on specialized risk assessment training, expertise, or experience when determining that a serious threat exists or that serious harm is reasonably foreseeable? Are there unintended consequences related to specifying mental and behavioral health professionals as examples of such providers?	Specialized risk assessment training, expertise, and experience are all desirable qualifications when determining whether a serious threat exists or that serious harm is reasonably foreseeable. However, these same qualifications enable an individual to determine the existence of a serious and imminent threat—the current standard. **There is no evidence that a more stringent standard is necessary and would result in saved lives; in fact, the only certain outcome of this proposal is that the federal government would essentially codify the idea that patients with certain health conditions must accept a lower level of privacy than all other individuals.** This "othering" is unnecessary, harmful, and unjust. OCR's proposal should not be finalized for these reasons and the other potential unintended consequences included above.
i. As an alternative to the existing proposal, should the Department establish a specific permission for mental and behavioral health professionals to disclose PHI when in the view of the professional, the disclosure could prevent serious and reasonably foreseeable harm or	While this alternative is preferable to the existing proposal in that it limits the scope of health care professionals who would have the authority to make such a determination, the AMA opposes the overall concept of changing the standard to "serious and reasonably foreseeable harm" from "serious and imminent" threats for all of the reasons included above.

[29] *How HIPAA Allows Doctors to Respond to the Opioid Crisis*, available at https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf.
[30] *How HIPAA Allows Doctors to Respond to the Opioid Crisis*, available at https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf.

lessen a serious and reasonably foreseeable threat to the health or safety of a person or the public? What would be potential unintended consequences of such an alternative?	
G. 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 (45 CFR 164.520)	
OCR proposes to: • Eliminate the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP) and to retain copies of such documentation for six years. • Modify the content requirements of the NPP to clarify for individuals their rights with respect to their PHI and how to exercise those rights.	
Response to Proposals on NPPs	
General Comments	**The AMA supports eliminating the requirement to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP) as well as the retention requirement.** While AMA policy requires that confidentiality be protected and only allows the disclosure of information with a patient's authorization or when an objective analysis concludes that the benefits of disclosure outweigh risks to patients' privacy, removing the written acknowledgement requirement and the six-year retention requirement would reduce administrative burden by decreasing the amount of paperwork to print and store; it would also limit unneeded compliance monitoring. However, we urge OCR to ensure that patients can access the information contained within an NPP as easily and clearly as possible. For example, OCR should continue to require that covered entities make NPPs easily and readily available to patients upon demand. Particularly as information sharing increases and expands, patients must always be aware of how their information will be used and disclosed by the covered entity.
a. Would the proposed changes to the NPP requirements have any unintended adverse consequences for individuals or regulated entities?	Covered entities may be unable to demonstrate that patients understand an organization's privacy practices. Patients may not understand how HIPAA permits an organization to share information without the patient's authorization, particularly if many of this NPRM's proposals are finalized. Covered entities may experience the

	consequences of such misunderstanding in ways including, but not limited to, complaints to OCR. For example, patients may post complaints on social media about a covered entity for any number of reasons, including misunderstandings around privacy practices. We receive many complaints from our members who feel that they are unable to respond to such complaints without compromising their confidentiality obligations. We encourage OCR to develop a mechanism for physicians to respond to such complaints without violating HIPAA. The frequency of these scenarios only stands to increase—particularly if OCR expands the ways in which information is exchanged without a patient's direct knowledge.
b. Would the revised NPP content requirements improve individuals' understanding of, and ability to exercise, their rights under the Privacy Rule?	We do not support the revised NPP content. Rather, we encourage OCR to develop model NPPs that are more specific as to how a patient's information may be used within the health care system and among business associates.
c. Are there ways that OCR can improve the model NPPs to be more informative and easier to understand? d. Should the model NPP's description of health care operations be modified? If so, please provide suggested language for modifying the description in the model NPP to reflect how your organization uses PHI for health care operations purposes.	OCR should require more specificity in what is disclosed in an NPP. For example, the level of detail included in describing uses and disclosures for health care operations should be adequate to alert the patient to the multiple categories for which their information is being used. Patients generally enter a physician's office or a hospital believing that the information they provide is going to their individual care and benefit. Activities that use patients' information for marketing and other non-routine categories or for the benefit of a population or group should be explained with more specificity.
e. Are there specific examples that should be included in a model NPP to explain to individuals how PHI can be used or disclosed for health care operations?	NPPs should include examples of how health plans may access and use PHI for health care operations purposes. For example, patients may want to know that health plans can request and receive an individual's PHI under information blocking regulations. Patients should know that health care operations encompass a wide range of activities—the examples should include a sampling of such activities. If OCR's proposals are finalized, this information may not be limited to the minimum amount necessary, so patients should be aware that a significant part of their medical record may be shared upon request. Additionally, third parties acting on behalf of the patient—including non-covered entities—may receive large amounts of information held in a patient's record. Patients should be informed that such information will no

	longer be protected by HIPAA and may be used and redisclosed at will by the third party. Patients should also be informed about the scope of information released under such requests (e.g., the USCDI, EHI, etc.).