February 12, 2019

Mr. Roger Severino
Director, Office for Civil Rights
U.S. Department of Health & Human Services
200 Independence Avenue, Humphry Building
Washington, DC 20021

Re: Request for Information on Modifying HIPAA Rules To Improve Coordinated Care (HHS-OCR-0945-AA00)

Submitted electronically at: https://www.Regulations.gov

Mr. Severino:

The American Medical Informatics Association (AMIA) appreciates the opportunity to comment on the Request for Information (RFI) on Modifying HIPAA Rules to Improve Coordinated Care.

Access to information and the ability to integrate and use information has changed how individuals book travel, find information about prices and products, and compare and review products and services. Information can empower individuals, but healthcare has lagged behind other service sectors in reflecting this customer-centric approach. In 1996, HIPAA gave patients a right to a copy of their health information maintained by hospitals, physician offices, and (later) laboratories. But more than twenty years later, patients still struggle to leverage this right guaranteed by law.

From HIPAA to the HITECH Act to the 21st Century Cures Act, Congress has prioritized improved patient data access as a key lever to improve care, enable research, and empower patients to live healthy lifestyles. Enacting these policies into regulations that achieve improved patient data access and clinical interoperability for care coordination has proven more difficult in practice than Congress imagined.

HIPAA's contribution to the protection of patient privacy is essential and it has been a serviceable policy for more than 20 years. However, the digitization of healthcare delivery, the continued integration of traditional and non-traditional healthcare encounters, and long-standing challenges related to access and sharing of PHI necessitate a review of HIPAA. We applaud OCR for issuing this RFI. Given the rapid digitization of healthcare delivery across the U.S. in the last ten years, a public dialogue on the attributes of HIPAA is long overdue.

In reviewing questions in the section related to "Promoting information sharing for treatment and care coordination," we identified three core problems: (1) it takes too long for PHI to be shared for permitted purposes, including with patients under the right of individual access; (2) HIPAA has been misused to restrict sharing of PHI; and (3) HIPAA has been a barrier to sharing mental health data

and information. To these general concerns, AMIA adds that HIPAA has been a barrier to data-driven observational research and population health management.

We understand that HIPAA already permits sharing of PHI in the case of treatment and that patients already have a right to a copy of their information. The reality is that despite this permission and despite this right, HIPAA has instilled a pervasive concern over the legality of sharing patient data improperly – especially related to requests for PHI based on treatment and for individual access.[1,2]

For these reasons, OCR must (1) require timely sharing of information when both the patient consents to it and a treating clinician has requested it; (2) clarify that HIPAA permits the sharing of PHI when the patient requests or instructs that their PHI be shared – regardless of whether the target of this sharing is bound by HIPAA; and (3) elevate the failure to deliver an individual "right of access" to an enforcement and penalty priority on par with data breaches.

Specifically, AMIA recommends:

- **OCR work with ONC to ensure that Certified Health IT can provide individuals a complete, electronic copy of their data as part of the HIPAA right of access;**
- **OCR issue guidance or take more binding steps to ensure that lawful requests for PHI under "treatment" be recategorized as obligatory, not simply permissible;**
- **OCR coordinate with the HHS OIG to develop an information blocking rule that will compel sharing of PHI for purposes of "treatment" and require Covered Entities (CEs), Business Associates (BAs), and other non-covered entities (NCEs) that manage PHI, to establish a uniform individual "right of access" policy;**
- **OCR provide formal guidance permitting the sharing of PHI to entities outside the traditional bounds of HIPAA when directed by the individual;**
- **OCR consider classifying genetic data at the genome scale as PHI, not simply health information, regardless of other identifying information; and**
- **OCR revise or clarify that the use of PHI by a CE for observational, data-driven research purposes is permissible as part of HIPAA "operations."**

To provide accountability and oversight in a paradigm that compels sharing, **AMIA recommends that OCR work closely with CEs and BAs to develop IT-enabled audit trails and accounting of disclosures.** If the desired outcome of the public policy is to make more complete access, exchange, and use of patient data available for improved care coordination, then we must have

[1] The second and third most frequent forms of information blocking, according to a survey by Adler-Milstein and Pfeifer, occurs when hospitals and health systems selectively share patient information by using HIPAA as a reason not to share, making it less likely that patients will seek care elsewhere. Adler-Milstein J, Pfeifer E. Milbank Q. 2017 Mar; 95(1): 117–135. Published online 2017 Mar 7. doi: 10.1111/1468-0009.12247

[2] Lye CT, Forman HP, Gao R, et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. JAMA Netw Open. 2018;1(6):e183014. doi:10.1001/jamanetworkopen.2018.3014

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

robust means for understanding who was granted access and for which purpose. This is the crux of the trade-off between removing providers from legal uncertainty in sharing data (e.g., force sharing through an information blocking rule or through a revised interpretation of HIPAA), while providing more accountability and oversight for those data that are shared.

We also acknowledge that HHS is working to develop rules related to "information blocking." We understand that this rule will identify instances where information blocking is acceptable, thus leaving broad swaths of activities subject to information blocking penalties. Whether these activities will include specific requirements under HIPAA, such as the requirement to provide patients with a copy of their PHI upon request, is unknown at this time. **OCR should coordinate any updates to HIPAA with the information blocking rule to ensure that the policies are mutually reinforcing** to compel sharing of PHI for purposes of "treatment" and require CEs, Bas, and NCEs who handle PHI to deliver data pursuant to an individual's "right of access."

Finally, **AMIA recommends that a concerted effort be made at the policy level to enable individuals to access all their information maintained in a CE's "designated record set," as a "readily producible" function of certified EHR technology (CEHRT) capability.** There has been a long-standing discordance between what federal policy requires and what technology and/or organizational policies have delivered as part of HIPAA's individual right of access. HIPAA established broad definitions and these concepts were developed long before use of EHRs, mobile apps, and other kinds of health technology became commonplace. In a document-centered, paper-based world, defining information in terms of "records" makes sense, but as more than 96 percent of all US hospitals possess EHRs,[3] we must rethink how to better ensure individuals' right of access in a data-centric world through CEHRT.

As recently outlined in a joint statement with AHIMA,[4] AMIA recommends that policymakers modernize HIPAA by either establishing a new term, "Health Data Set," which includes all clinical, biomedical, and claims data maintained by a CE or BA, or by revising the existing HIPAA "Designated Record Set" definition and requiring Certified Health IT to provide the amended DRS to patients electronically in a way that enables them to use and reuse their data.[5] The goal of this recommendation would establish an operational definition – either as part of a newly conceptualized "Health Data Set" or a revised definition of the DRS – to support individuals' right of access and guide future development of ONC's Certification Program so individuals could view, download, or transmit to a third party this information electronically and access this information via application programming interface (API) of their choice. OCR's policy should dictate CEHRT functionality, not the other way around.

[3] https://dashboard.healthit.gov/quickstats/pages/certified-electronic-health-record-technology-in-hospitals.php
[4] AMIA, AHIMA Joint Statement: HIPAA Modernization Needed, Experts Say. December 5, 2018. http://bit.ly/2WQm1Eh
[5] AMIA, AHIMA Recommendations to Improve Individuals' Health Data Access. December 5, 2018. http://bit.ly/2WWqt4r

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

February 12, 2019

Below, in Table 1, we outline our recommendations to select questions in the RFI. Should you have any questions or require additional information, please contact AMIA Vice President for Public Policy Jeffery Smith at jsmith@amia.org or (301) 657-1291 ext. 113. We thank OCR for the opportunity to comment and look forward to continued dialogue.

Sincerely,

Douglas B. Fridsma, MD, PhD, FACP, FACMI
President and CEO AMIA

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

February 12, 2019

Table 1.

Question #	OCR Questions	AMIA Comments
	Promoting information sharing for treatment and care coordination.	
1	How long does it take for covered entities to provide an individual with a copy of their PHI when requested pursuant to the individual's right of access at 45 CFR 164.524? How long does it take for covered entities to provide other covered entities copies of records that are not requested pursuant to the individual's right of access? Does the length of time vary based on whether records are maintained electronically or in another form (e.g., paper)? Does the length of time vary based on the type of covered entity? For instance, do some types of health care providers or plans take longer to respond to requests than others?	We are unaware of aggregate data indicating how long it takes a covered entity to provide individuals with copies of their PHI when requested via 45 CFR 164.524. However, a recent study from JAMA found that discrepancies exist in the information provided to patients regarding the medical records release process and confusion over how to comply with federal and state regulations and recommendations among some of the nation's most highly ranked hospitals.[6] To the difference in length of time, members note that records maintained electronically are more quickly provided than those records and information that are not. Yet, we reiterate our position that even for records maintained electronically, the length of time is too great. Anecdotally, CEs that are under-resourced or do not possess CEHRT tend to have more difficulty in fulfilling such requests. Efforts should be made to ensure that all parties along the care continuum use EHRs.
2	How feasible is it for covered entities to provide PHI when requested by the individual pursuant to the right of access more rapidly than currently required under the rules? (The	Current requirements established by CMS dictate that data included as part of the Common Clinical Data Set (CCDS) and 2015 Edition CEHRT be made available within 36 hours of the patient visit, consistent with current

[6] Lye CT, Forman HP, Gao R, et al. Assessment of US Hospital Compliance With Regulations for Patients' Requests for Medical Records. JAMA Netw Open. 2018;1(6):e183014. doi:10.1001/jamanetworkopen.2018.3014

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	Privacy Rule requires covered entities to respond to a request in no more than 30 days, with a possible one-time extension of an additional 30 days.). What is the most appropriate general timeframe for responses? Should any specific purposes or types of access requests by patients be required to have shorter response times?	CMS requirements.[7] This timeframe should become the standard general timeframe for data generated using CEHRT and considered part of the CCDS, and these data should be easily accessible to individuals through their patient portal or an API. When and if the US Core Data for Interoperability (USCDI) is finalized, this should succeed the CCDS as the minimum-level expectation for data availability within the timeframe established by CMS's Promoting Interoperability Program. Operationally, we note there may be circumstances when individual / family need information more quickly than other situations. Diagnosis and prognosis would be examples of specific purposes.
3	Should covered entities be required to provide copies of PHI maintained in an electronic record more rapidly than records maintained in other media when responding to an individual's request for access? (The Privacy Rule does not currently distinguish, for timeliness requirements, between providing PHI maintained in electronic media and PHI maintained in other media). If so, what timeframes would be appropriate?	Yes – HHS policy should encourage near real-time access to PHI when responding to an individual's request for access, especially if the requested data is generated using CEHRT and part of CCDS. Timeliness requirements should encourage electronic access of all data maintained by CEs and BAs. We reiterate our recommendation to make current CMS requirements to make available data to the patient within 36 hours of its availability to the eligible hospital or CAH.
4	What burdens would a shortened timeframe for responding to access requests place on covered entities? OCR requests specific examples and cost estimates, where available.	If CEHRT is leveraged to provide individuals access, costs will be minimized. This question of cost should also consider costs of not making data / information available in shortened timeframe.

[7] https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/MedicareEHStage3_Obj3.pdf#page=3

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

5	Health care clearinghouses typically receive PHI in their role as business associates of other covered entities, and may provide an individual access to that PHI only insofar as required or permitted by their business associate agreement with the other covered entity, just as other covered entities, when performing business associate functions, may also provide access to PHI only as required or permitted by the business associate agreement(s) with the covered entity(ies) for whom they perform business associate functions. Nevertheless, the PHI that clearinghouses possess could provide useful information to individuals. For example, clearinghouses may maintain PHI from a variety of health care providers, which may help individuals obtain their full treatment histories without having to separately request PHI from each health care provider. a) How commonly do business associate agreements prevent clearinghouses from providing PHI directly to individuals? b) Should health care clearinghouses be subject to the individual access requirements, thereby requiring health care clearinghouses to provide individuals with access to their PHI in	We do not support changes to clearinghouses' current status or their current expectations / responsibilities under HIPAA.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	a designated record set upon request? Should any limitations apply to this requirement? For example, should health care clearinghouses remain bound by business associate agreements with covered entities that do not permit disclosures of PHI directly to an individual who is the subject of the PHI? c) Alternatively, should health care clearinghouses be treated only as covered entities—i.e., be subject to all requirements and prohibitions in the HIPAA Rules concerning the use and disclosure of PHI and the rights of individuals in the same way as other covered entities—and not be considered business associates, or need a business associate agreement with a covered entity, even when performing activities for, or on behalf of, other covered entities? Would this change raise concerns for other covered entities about their inability to limit uses and disclosures of PHI by health care clearinghouses? For example, would this change prevent covered entities from providing assurances to individuals about how their PHI will	

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	be used and disclosed? Or would covered entities be able to adequately fulfill individuals' expectations about uses and disclosures through normal contract negotiations with health care clearinghouses, without the need for a HIPAA business associate agreement? Would covered entities be able to impose other contractual limitations on the uses and disclosures of PHI by the health care clearinghouse? d) If health care clearinghouses are not required to enter into business associate agreements with the other covered entities for whom they perform business associate functions, should such requirement also be eliminated for other covered entities when they perform business associate functions for other covered entities?	
6	Do health care providers currently face barriers or delays when attempting to obtain PHI from covered entities for treatment purposes? For example, do covered entities ever affirmatively refuse or otherwise fail to share PHI for treatment purposes, require the requesting provider to fill out paperwork not required by the HIPAA Rules to complete the disclosure (e.g., a form representing that the	According to member feedback, it is common for CEs to refuse to send records to other CEs until/unless there is a written request from the patient and/or request is made using requestor's letterhead. As stated previously, HIPAA has instilled a perverse incentive to hoard data, rather than compel sharing under permitted circumstances. This commonly occurs in mental health and substance use disorder treatment settings, either because of stricter state laws on information release, stricter requirements of 42 CFR or misunderstandings of HIPAA

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	requester is a covered health care provider and is treating the individual about whom the request is made, etc.), or unreasonably delay sharing PHI for treatment purposes? Please provide examples of any common scenarios that may illustrate the problem.	requirements. Mental health providers are often told information can't be released without a signed authorization from the patient. On some occasions, we are told that information won't be released at all due to the need for confidentiality of mental health services. This frequently leads to unreasonable delays in decision making or, more often, a need to make decisions about treatment or hospitalization without having all of the necessary information.
7	Should covered entities be required to disclose PHI when requested by another covered entity for treatment purposes? Should the requirement extend to disclosures made for payment and/or health care operations purposes generally, or, alternatively, only for specific payment or health care operations purposes? a) Would this requirement improve care coordination and/or case management? Would it create unintended burdens for covered entities or individuals? For example, would such a provision require covered entities to establish new procedures to ensure that such requests were managed and fulfilled pursuant to the new regulatory provision and, thus, impose new administrative costs on covered entities? Or would the only new	Yes – covered entities should be required to disclose PHI when requested by another CE for treatment purposes. Developing policy to compel sharing of PHI for purposes of treatment, rather than simply permit the sharing of PHI, will help assuage concerns over the legality of sharing and it will help identify instances of flagrant violation. While we anticipate that new systems and controls will be needed to verify a treating relationship this change could remove pervasive barriers to better care coordination. AMIA also recommends that OCR provide formal guidance permitting the sharing of PHI to non-covered entities and non-business associates when directed by the individual. For example, patients may want to direct their health data to businesses outside of medicine, such as with an architect who is going to modify a home to make it less prone to induce falls, or to a personal trainer who will help a child with cerebral palsy practice her walking. This HIPAA guidance would clarify that sharing of this data is permitted because the patient wants it shared. If increased sharing is the desired outcome, we need better visibility into who accessed and acquired patient data through such pathways. Better

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	administrative costs arise because covered entities would have to manage and fulfill requests for PHI that previously would not have been fulfilled? b) Should any limitation be placed on this requirement? For instance, should disclosures for healthcare operations be treated differently than disclosures for treatment or payment? Or should this requirement only apply to certain limited payment or health care operations purposes? If so, why? c) Should business associates be subject to the disclosure requirement? Why or why not?	audit trails and accounting of disclosures are necessary to ensure accountability and oversight.
8	Should any of the above proposed requirements to disclose PHI apply to all covered entities (i.e., covered health care providers, health plans, and health care clearinghouses), or only a subset of covered entities? If so, which entities and why?	Yes, requirements to disclose PHI should apply uniformly across all CEs.
9	Currently, HIPAA covered entities are permitted, but not required, to disclose PHI to a health care provider who is not covered by HIPAA (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for treatment and payment purposes of either the covered	CEs should be required to disclose PHI at the request of the patient. However, disclosures to entities not covered by HIPAA should only be permitted at the direction of the patient. .

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	entity or the non-covered health care provider. Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all of an individual's health care providers?	
10	Should a non-covered health care provider requesting PHI from a HIPAA covered entity provide a verbal or written assurance that the request is for an accepted purpose (e.g., TPO) before a potential disclosure requirement applies to the covered entity receiving the request? If so, what type of assurance would provide the most protection to individuals without imposing undue burdens on covered entities? How much would it cost covered entities to comply with this requirement? Please provide specific cost estimates where available	We see the development of trust frameworks and process to verify appropriateness of requests to be a critical workstream – especially if sharing for treatment is made compulsory. This will be a valuable policy exercise to prevent nuisance requests and various commercial entities from requesting every bit of data they became aware of so as to aggregate larger and more salable profiles of consumers/patients.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

11	Should OCR create exceptions or limitations to a requirement for covered entities to disclose PHI to other health care providers (or other covered entities) upon request? For example, should the requirement be limited to PHI in a designated record set? Should psychotherapy notes or other specific types of PHI (such as genetic information) be excluded from the disclosure requirement unless expressly authorized by the individual?	Yes, we envision that exceptions or limitations to require disclosure of PHI would be warranted. The DRS encapsulates a reasonable (if not difficult to operationalize) universe for requests to apply, and we would support psychotherapy notes to remain excluded from disclosure requirements. Psychotherapy notes as defined by HIPAA should continue to be restricted from disclosure. Although this is a topic that is often a subject of much misinformation, the current psychotherapy notes provision does not apply to all aspects of notes related to the provision of psychotherapy. The supreme court case of Jaffee v. Redmond is at the heart of the protection of psychotherapist-patient privilege.[8] For this reason, many people (particularly most people whose professional identity is as a psychotherapist) see the confidentiality of any psychotherapy related notes as sacrosanct (i.e., should never be shared with anyone). In addition, we recommend genetic information be excluded from such requests unless the patient specifically requests that it be disclosed. It is widely accepted in the research field that the genetic data is de-identified. This allows the use and sharing of genetic data in a much more permissive manner compared to other data elements that are considered *protected health information* (PHI) and sensitive. Genetic data is also not one of the 18 identifiers specified by HIPAA and therefore are not subject to the same federal protections as other defined PHI data types (e.g. fingerprints, full facial pictures, email addresses). The National Human Genome Research Institute recognizes that "each person's DNA sequence is unique and ultimately, and there is enough information in any individual's DNA sequence to absolutely identify

[8] The Federal Psychotherapist-Patient Privilege. Jaffe v. Redmond, 518 U.S. 1. http://jaffee-redmond.org/

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

		her/him."[9] As early as 2004, researchers have shown that a person can be uniquely identified with access to just 75 single-nucleotide polymorphisms (SNPs) from that individual.[10] There is growing awareness in the scientific community on the increasing availability of genetic data, potential privacy breaches due to either intentional sharing of it with non-covered entities since it is considered de-identified or an unintentional breach due to hacking.[11] Given these and other factors, we recommend that genetic data at the genome scale should be considered PHI.
12	What timeliness requirement should be imposed on covered entities to disclose PHI that another covered entity requests for TPO purposes, or a non-covered health care provider requests for treatment or payment purposes? Should all covered entities be subject to the same timeliness requirement? For instance, should covered providers be required to disclose PHI to other covered providers within 30 days of receiving a request? Should covered providers and health plans be required to disclose PHI to each other within 30 days of receiving a request? Is there a more appropriate timeframe in which covered entities should disclose PHI for TPO	We view the necessity to share PHI for treatment purposes as a more urgent scenario than for payment or operations. Thus, a request for PHI for treatment purposes should be fulfilled more quickly. As stated previously, if the information requested is part of the CCDS/USCDI, the timeliness requirement should align with CMS policy of 36 hours. In most instances, we view the 30 days requirement as unreasonable, and would favor a period of 5 business days, with an option to extend this period another 10 business days. When a patient requests or approves a request for disclosure to an NCE, the same time period(s) should apply. If the patient didn't request or approve this, the data should not be disclosed.

[9] "Use of Human Subjects in DNA Sequencing." n.d. National Human Genome Research Institute (NHGRI). Accessed February 7, 2019. https://www.genome.gov/10000921/

[10] Lin, Zhen, Art B. Owen, and Russ B. Altman. 2004. "Genetics. Genomic Research and Human Subject Privacy." Science 305 (5681): 183.

[11] Evans, Barbara J. 2018. "HIPAA's Individual Right of Access to Genomic Data: Reconciling Safety and Civil Rights." American Journal of Human Genetics 102 (1): 5–10.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	purposes? Should electronic records and records in other media forms (e.g., paper) be subject to the same timeliness requirement? Should the same timeliness requirements apply to disclosures to non-covered health care providers when PHI is sought for the treatment or payment purposes of such health care providers?	
13	Should individuals have a right to prevent certain disclosures of PHI that otherwise would be required for disclosure? For example, should an individual be able to restrict or "opt out" of certain types of required disclosures, such as for health care operations? Should any conditions apply to limit an individual's ability to opt out of required disclosures? For example, should a requirement to disclose PHI for treatment purposes override an individual's request to restrict disclosures to which a covered entity previously agreed?	Patients should be able to opt out of disclosure of certain types of data – at a minimum genetic information – and potentially others, as well.
15	Should any new requirement imposed on covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) require the requesting covered entity to get the explicit affirmative authorization of the patient before initiating the request, or should a covered entity be allowed to make the request based on the	The party that wants the data should get the patient's permission and include this written, signed permission along with the disclosure request. The party getting the request should not have to hunt down the patient and ask for permission.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	entity's professional judgment as to the best interest of the patient, based on the good faith of the entity, or some other standard?	
16	What considerations should OCR take into account to ensure that a potential Privacy Rule requirement to disclose PHI is consistent with rulemaking by the Office of the National Coordinator for Health Information Technology (ONC) to prohibit "information blocking," as defined by the 21st Century Cures Act?	OIG and OCR must coordinate where oversight and enforcement responsibilities lie. OCR and ONC should jointly establish a committee similar to ONC's HITAC that works to ensure consistency of rulemaking across the organizations. No fewer than 1/3 of the committee's members should represent patients' interests.
17	Should OCR expand the exceptions to the Privacy Rule's minimum necessary standard? For instance, should population-based case management and care coordination activities, claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development be excepted from the minimum necessary requirement? Would these exceptions promote care coordination and/or case management? If so, how? Are there additional exceptions to the minimum necessary standard that OCR should consider?	Population health should be covered under HIPAA as part of operations. Minimum necessary standard needs guidance under a population health rubric. We also recommend expansion on minimum necessary in context of BAs providing Clinical Decision Support (CDS) as a service, quality improvement, and clinician education. To optimize utility and sophistication of CDS interventions, and to reduce documentation-related burnout, circumventing the need for duplicative data entry is essential.
18	Should OCR modify the Privacy Rule to clarify the scope of covered entities' ability to disclose PHI to social services agencies and community-based support programs where necessary to facilitate treatment and	Yes, so long as the patient agrees to the sharing of their information to social service agencies and community-based support programs.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	coordination of care with the provision of other services to the individual? For example, if a disabled individual needs housing near a specific health care provider to facilitate their health care needs, to what extent should the Privacy Rule permit a covered entity to disclose PHI to an agency that arranges for such housing? What limitations should apply to such disclosures? For example, should this permission apply only where the social service agency itself provides health care products or services? In order to make such disclosures to social service agencies (or other organizations providing such social services), should covered entities be required to enter into agreements with such entities that contain provisions similar to the provisions in business associate agreements?	
19	Should OCR expressly permit disclosures of PHI to multi-disciplinary/multi-agency teams tasked with ensuring that individuals in need in a particular jurisdiction can access the full spectrum of available health and social services? Should the permission be limited in some way to prevent unintended adverse consequences for individuals? For example, should covered entities be prevented from disclosing PHI under this permission to a multi-agency team that includes a law	OCR should not permit disclosures to multi-disciplinary / multi-agency teams; doing so would create a gigantic loophole that could render the rest of the rule meaningless. If there is a patient-determined need for disclosure, that patient can initiate the process. If other agencies want information, they can ask the individual for permission as individual agencies, so the patient knows what agencies want the data and (broadly) how many individuals may be able to access the PHI. Allowing blanket multi-agency requests that aren't transparent to the patient creates the potential for erosion of civil liberties, promotion of discrimination based upon health and personal characteristics, and exacerbation of health disparities.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	enforcement official, given the potential to place individuals at legal risk? Should a permission apply to multi-disciplinary teams that include law enforcement officials only if such teams are established through a drug court program? Should such a multi-disciplinary team be required to enter into a business associate (or similar) agreement with the covered entity? What safeguards are essential to preserving individuals' privacy in this context?	
20	Would increased public outreach and education on existing provisions of the HIPAA Privacy Rule that permit uses and disclosures of PHI for care coordination and/or case management, without regulatory change, be sufficient to effectively facilitate these activities? If so, what form should such outreach and education take and to what audience(s) should it be directed?	Whether it is sufficient or not, public outreach and education is necessary. The current HIPAA website provides a great deal of helpful information already, but additional education and outreach would be helpful. Sessions for hospital legal counsel, health information managers, and hospital EHR security officers would be especially good, if they aren't already being done, since these individuals are typically the ones who are front-line decision-makers in how to interpret HIPAA.
	Promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness	
22	What changes can be made to the Privacy Rule to help address the opioid epidemic? What risks are associated with these changes? For example, is there concern that encouraging more sharing of PHI in these circumstances may discourage individuals from seeking needed health care services? Also is there concern that encouraging more sharing of PHI	From the standpoint of the opioid epidemic, the greatest challenges are not with the Privacy Rule per se, but in the common interpretations of the Privacy Rule and in the constraints imposed by 42 CFR Part 2 on information sharing. Although the Privacy Rule itself allows sharing of information for treatment purposes, health care providers are often concerned about sharing that information out of confusion about what HIPAA permits and out of confusion about the requirements and restrictions of 42 CFR. Thus, there is a tendency to be very reluctant to

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	may interfere with individuals' ability to direct and manage their own care? How should OCR balance the risk and the benefit?	share any information at all related to substance use related events (e.g., overdose, evidence of withdrawal) or substance use disorder treatment. The interpretation of "holding oneself out" as providing assessment or treatment for substance use disorder is particularly fraught with confusion and people become confused about what information that they might have gotten from a substance use treatment program can be mentioned in a note and then released to others. As things stand now, however, some information about an individual's opioid use disorder may be subject only to HIPAA (e.g., information about emergency care received for opioid use, some medications for opioid use disorder prescribed in a non-CFR 42 program) whereas other information that can be equally important to providing comprehensive and coordinate opioid use disorder treatment is not available except through cumbersome and confusing consent processes. These information gaps can be life-threatening, for example, when other treating clinicians are unaware that a patient is receiving methadone in a 42 CFR program and this information is not available in prescription drug monitoring program databases or external prescribing databases. It is possible that some individuals may not seek out treatment in an opioid use disorder treatment program due to concerns about inappropriate use of that information and these concerns would apply under HIPAA protected information and 42 CFR protected information. Nevertheless, it may be preferable to address inappropriate use of the information rather than blocking or restricting access in a way that limits effective treatment. There are several ways in which patients are often concerned about disclosure of information related to an opioid use disorder. One concern relates to the fact that there continues to be discrimination against

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

		individuals for substance use disorders within the health care system just as there continues to be discrimination and health care disparities for individuals with other conditions (e.g., mental health conditions, obesity), aspects of prior history (e.g., reproductive or mental health history), or demographic factors (e.g., age, sex, race, ethnicity, sexual orientation, gender identity, religion, national origin, socioeconomic status). Discrimination and care disparities related to each of these characteristics (including the presence of or treatment for an opioid use disorder) should be addressed directly through increased education and mechanisms to report discrimination that affects clinical care. Another area in which disclosure of an opioid use disorder can be problematic relates to the legal system (e.g., legal charges related to use or possession; divorce or child custody related issues), employment, professional licensing, and insurance related considerations (e.g., health disability insurance, long-term care or life insurance). Regulations might be better focused on eliminating use of this information in these or similar contexts rather than focusing on restricting disclosures that are necessary for treatment or related-purposes. A third area in which individuals are concerned about disclosures relates to inadvertent disclosure to individuals in their community, workplace or social circle. Within a health care organization, many individuals have access to records for legitimate purposes of treatment, payment or operations. Depending on the size of the organization and the size of the surrounding community, it would not be uncommon for an acquaintance of the patient to inadvertently learn information that a patient may view as sensitive. Although it would be difficult to eliminate all such inadvertent disclosures, technology can be used (and incorporated into regulation) to proactively restrict information access to specific individuals based on

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

		information such as neighboring addresses or requests by patients to block access to specifically named persons (e.g., ex-spouse, work supervisor, perpetrator of prior domestic violence). For individuals with high-profile occupations or high-public visibility, regulations could require that an EHR be able to restrict information access to a limited set of users (either as specified by the individual, his or her treating clinical or facility administrators).
23	How can OCR amend the HIPAA Rules to address serious mental illness? For example, are there changes that would facilitate treatment and care coordination for individuals with SMI, or ensure that family members and other caregivers can be involved in an individual's care? What are the perceived barriers to facilitating this treatment and care coordination? Would encouraging more sharing in the context of SMI create concerns similar to any concerns raised in relation to the previous question on the opioid epidemic? If so, how could such concerns be mitigated?	There is a number of key barriers to facilitating treatment, care coordination and family involvement for individuals with serious mental illness. A major barrier is related to misinterpretations of what HIPAA actually requires. The current HIPAA website already provides a great deal of helpful information, but additional examples of common clinical situations as well as enhanced education and outreach would be beneficial. In addition to education aimed at providers, outreach should be targeted to health care attorneys, health information managers, and EHR security officers because these individuals often encourage providers to avoid releasing any information to minimize HIPAA-related risks. Another barrier to information release can relate to 42 CFR Part 2 (for individuals with serious mental illness and co-occurring substance use disorders) and to state laws, which may be more restrictive than HIPAA in terms of mental health or substance use disorder treatment information. Aligning 42 CFR with HIPAA would eliminate that potential barrier and states could also be encouraged to align their laws regarding mental health information release. The issues related to discrimination and inadvertent but potential damaging release of information described in the answer to question 22, would also apply here and the same potential mitigation approaches would be relevant. Reducing barriers to family involvement can be partially mitigated by improving provider and health system understanding of HIPAA. Clinicians and health care organizations often

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

		assume that HIPAA prohibits communicating with family members unless the patient gives express permission to do so. They often fail to understand (and fail to tell families) that family members can always provide information to treating clinicians (e.g., by phone or in writing). Although there may be some clinical circumstances in which family involvement may not be helpful to the patient, involving family members is beneficial in most cases. Despite this, some educational programs have historically focused on patient autonomy to the exclusion of family and support network contacts. In overcoming this barrier, professional organizations and educational programs can also play a role by encouraging greater family member involvement and teaching about the nuances of clinical communication with family and support networks, including HIPAA related considerations.
24	Are there circumstances in which parents have been unable to gain access to their minor child's health information, especially where the child has substance use disorder (such as opioid use disorder) or mental health issues, because of HIPAA? Please specify, if known, how the inability to access a minor child's information was due to HIPAA, and not state or other law.	Rule about parental access to teenage and pre-teenage children's medical records vary from state to state and institution to institution, and are not driven by HIPAA per se. These rules generally are designed to balance the parent's right of access with the children's right to privacy. In general terms, parental access may be limited in the case of adolescent health records around sex and sexuality, and drug use. From our standpoint, this is reasonable. It is incumbent on the treating healthcare provider to discuss with adolescents whether they want to share their health information with parents and guardians in the case of these medical issues. With that, privacy control remains with the adolescent in these sensitive diseases. Undermining the ability of teenagers to hid STIs and reproductive issues from their parents would be detrimental to care.
25	Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment	As above, decisions about health data privacy related to certain conditions and issues currently rests with the adolescent. We recommend that this

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	information of their minor children, especially where the child has substance use disorder (including opioid use disorder) or mental health issues, or are existing permissions adequate? If the Privacy Rule is modified, what limitations on parental access should apply to respect any privacy interests of the minor child? a) Currently, the Privacy Rule generally defers to state law with respect to whether a parent or guardian is the personal representative of an unemancipated minor child and, thus, whether such parent or guardian could obtain PHI about the child as his/her personal representative; if someone other than the parent or guardian can or does provide consent for particular health care services, the parent or guardian is generally not the child's personal representative with respect to such health care services. Should these standards be reconsidered generally, or specifically where the child has substance use disorder or mental health issues? b) Should any changes be made to specifically allow parents or spouses greater access to the treatment	aspect remains. Where HIPAA can be modified to make this standard across the country rather than a state-by-state law, would help. Conditions where adolescents should retain control include sex and sexuality, and issues around drug use. Mental health may also be appropriate for this. HIPAA should not be modified to allow parents or guardians access to these in all cases. When children reach the age of maturity, they should retain right of control over who accesses their health information so long as they are legally competent. Adults should retain full right of control over who accesses their health information so long as they are legally competent. For the adult losing competence, such as from dementia, they should be ruled incompetent before giving up control of their health information.

	information of their children or spouses who have reached the age of majority? If the Privacy Rule is changed to encourage parental and spousal involvement, what limitations should apply to respect the privacy interests of the individual receiving treatment? c) Should changes be made to allow adult children to access the treatment records of their parents in certain circumstances, even where an adult child is not the parent's personal representative? Or are existing permissions sufficient? For instance, should a child be able to access basic information about the condition of a parent who is being treated for early-onset dementia or inheritable diseases? If so, what limitations should apply to respect the privacy interests of a parent?	
	Accounting of disclosures	
30	In what scenarios would a business associate make a disclosure of PHI for TPO through an EHR? What is the average number of such disclosures for a given individual in a calendar year, if known?	One prominent example of this kind of "disclosure" is when a BA provides CDS and clinician education as a service. We recommend that a BA serving this role be seen as an extension of the CE such that sharing of data be regarded as permitted TPO.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

31	Should the Department require covered entities to account for their business associates' disclosures for TPO, or should a covered entity be allowed to refer an individual to its business associate(s) to obtain this information? What benefits and burdens would covered entities and individuals experience under either of these options?	An individual should have the ability to easily understand which data was disclosed and to whom. The goal should be to ensure that when patients want this information they can easily obtain it – either through the CE directly or through a centralized repository of BAs. At a minimum, we need a standard way to capture and convey disclosures across BAs and CEs leveraging IT.
35	A covered entity's Notice of Privacy Practices must inform individuals of the right to obtain an accounting of disclosures. Is this notice sufficient to make patients aware of this right? If not, what actions by OCR could effectively raise awareness?	No. Development of a universal document developed under OCR's authority, written by health literacy experts in patient-friendly language, that must be distributed annually by all CEs under threat of criminal penalty, would increase patient awareness of the right to obtain an accounting of disclosures.
36	Why do individuals make requests for an accounting of disclosures under the current rule? Why would individuals make requests for an accounting of TPO disclosures made through EHRs?	Individuals make requests because they are curious, because they want to see if health care providers/organizations actually do what they say they will, because they think that requests for accounting of disclosures will make health care organizations more likely to follow the rules, because they may incorrectly believe that they are supposed to receive an accounting, or because they have had a negative experience (e.g., loan or insurance denied, health-related questions asked in job interview) and want to find out if their health care providers/organizations disclosed PHI without their permission.
41	The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed	Increasingly, patients are receiving services to restore, maintain, and/or improve their health through providers that do not use EHRs (e.g., personal trainers, wellness program staff, community and senior centers, libraries, faith-based organizations, and others). Because such entities typically do not make the provision of health care-related services their primary activity, and may not even have a record of which individuals

	through, an EHR? Why or why not? What are the benefits and drawbacks of including TPO disclosures made through paper records or made by some other means such as orally? Would differential treatment between PHI maintained in other media and PHI maintained electronically in EHRs (where only EHR related accounting of disclosures would be required) disincentivize the adoption of, or the conversion to, EHRs?	attended health-related programming (e.g., which members of a senior center attended balance training classes), requiring such organizations to provide accounting of disclosures) could be burdensome enough to incentivize such organizations to cease providing health-related services. However, providers whose primary activity *is* health-related service provision, (e.g., personal trainers) should be required to provide accountings of disclosures whether they use EHRs or not.
	Additional ways to remove regulatory obstacles and reduce regulatory burdens to facilitate care coordination and promote value-based health care transformation	
54	In addition to the specific topics identified above, OCR welcomes additional recommendations for how the Department could amend the HIPAA Rules to further reduce burden and promote coordinated care. a) What provisions of the HIPAA Rules may present obstacles to, or place unnecessary burdens on, the ability of covered entities and/business associates to conduct care coordination and/or case management? What provisions of the HIPAA Rules may inhibit the transformation of the health care system to a value-based health care system? b) What modifications to the HIPAA Rules would facilitate efficient care	Aligning privacy requirements at the state and federal level is important as is aligning 42 CFR as already described. <u>Clarifications on non-secure communications</u> A common point of confusion/consternation with HIPAA involves methods of communication such as email, text messages, phone video apps and other unsecured forms of communication. Despite knowing that these communication methods are not "secure" or "HIPAA compliant" many patients/families still prefer to use them for communication with providers because they are readily available, more familiar and more usable than patient portals. For providers, these other forms of communication may also be less cumbersome than communicating through the portal. Individuals who are actively involved in patient care on the units may use regular text messages frequently, no matter how often they are told not to do so. Supervisors try to have staff avoid giving identifiable information, but they will text, for example, "Are you ready to see the delirious pt on

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

	coordination and/or case management, and/or promote the transformation to value-based health care? c) OCR also broadly requests information and perspectives from regulated entities and the public about covered entities' and business associates' technical capabilities, individuals' interests, and ways to achieve these goals.	15N yet?" or "The labs on the 15N pt are positive for Staph." The providers know who they mean, but someone intercepting the message would not. Thus, some clarifications would be helpful in terms of allowing non-secure communication with patients if the patient specifically prefers this and in terms of ONC posting lists of phone apps that are known to be HIPAA compliant (or not), since this is a common point of discussion/confusion among clinicians. <u>Enabling observational, data-driven research</u> For many years, AMIA has sought to facilitate the use of EHRs to improve care through a number of important avenues. Following the widespread implementation of EHRs, the potential to use in a secure manner the data now stored in siloes throughout the healthcare system to improve care through 'data analytics' had never been greater. Indeed, recouping substantial value from this national investment in EHRs can only be expected if greater access to this information is forthcoming. Among changes to HIPAA overwhelmingly supported by the House in 114th Congress H.R. 6 is language that includes the use of health data for research purposes within the definition of "health care operations." At present TPO excludes studies whose "primary purpose" includes the "obtaining of generalizable knowledge", or improvements of care beyond the institution or organization. Sharing knowledge to increase value-based care across healthcare is prevented. This has resulted in data silos that are an important reservoir for care improvements for both individual patients

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814

		and populations that can impact on both individuals as well as communities. In an era of ubiquitous EHRs, this language is a major impediment to a transformation to value-based care. Changing this regulation would offer the same degree of privacy protection as in the past while allowing data research to transform our healthcare system. There are clear limits to this revision that deserve comment. Only a Covered Entity, or a Business Associate under a contract (BAA) with a Covered Entity is permitted to use PHI for research and neither can share or disclose this information with others. All such data stays within the protection of HIPAA rules. It cannot be shared with others, e.g., pharmaceutical companies, marketers, or anyone else. Also, the language doesn't *require* an entity to use their data for research. Rather, it permits its use for such a purpose. Further, the "minimum necessary' requirement would apply as well disclosing the practice in its HIPAA Notice of Privacy Practices. If a Covered Entity preferred to seek individual consent for such a use of health data it could do so and use of an IRB for reviewing the design and methods for protecting confidentiality are still available for use. Very importantly, the change in the definition of TPO for research is limited solely to PHI has no implications for other existing requirements, e.g., informed consent for research with the potential for physical harm to the patient, etc. Today, we need a learning health care system in which results of studies that can improve care in one institution might directly inform others, as well, so that value-driven care expands as quickly as possible across the system. However, one must be able to determine if the desired results are potentially generalizable and not due simply to the particular characteristics of patients in one facility. With EHRs now in general use, failing to utilize

		this resource for improving care seems beyond lamentable, in light of our health care system's well-known current performance. In summary, despite the HIPAA provisions of HR 6 not being in the version of the 21st Century Cures Act signed into law in December 2016, we urge OCR and the Department to consider including use of health data for data research purposes within the definition of "health care operations" at section 164.501 of part 164, with the modifications to the rules for disclosure for health care operations at section 164.506 that were in HR 6.

American Medical Informatics Association | AMIA
4720 Montgomery Lane, Suite 500 | Bethesda, Maryland 20814