Ladies and Gentlemen:

The Health Law Section (the “Section”) of the American Bar Association (the “ABA”) respectfully submits the following comments to the U.S. Department of Health and Human Services Office for Civil Rights (“OCR”) regarding OCR’s Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, published in the Federal Register on December 14, 2018 (the “RFI”).

This letter expresses the Section’s views.¹ No government attorneys or government professionals participated in the drafting or submission of these comments. These comments have not been approved by the House of Delegates or the Board of Governors of the ABA and are not the position of the ABA as a whole. These comments do not represent the policy or views of any government employee who is a member of the Section, its Council, or its Interest Groups.

¹ These comments were prepared by a working group of the Health Law Section’s Interest Groups, including the eHealth, Privacy & Security Interest Group and the Physician Issues Interest Group, and were approved by the Health Law Section’s Council on February 7, 2019. The contributors to these comments include Jared Bruce, Heather Deixler, Amy Fehn, Matthew Fisher, Andrew Gantt, Adam Greene, Elizabeth Greene, Shannon B. Hartsfield, Linda Malek, Jennifer Mitchell, and Elaine Zacharakis. Although members of the Section and others who participated in the preparation of these comments represent clients who may be affected by HIPAA, no such member has been engaged by a client to participate in the drafting or submission of these comments.
The ABA is the largest voluntary professional association in the world. The Section, with over 7,200 attorney members, is the voice of the organized healthcare bar within the ABA. Its members represent clients in all aspects of the healthcare industry, including physicians, institutional providers, clinical researchers, academic institutions, clinical laboratories, pharmaceutical companies, health insurers, hospitals, public health entities, non-profit institutions, government healthcare programs and regulatory bodies, device manufacturers, and healthcare and medical application developers. The Section respectfully submits the comments and suggestions below for consideration by OCR. For some topics, we are providing general comments. For others, we have attempted to provide specific feedback regarding questions posed by OCR.

**Executive Summary**

This letter includes comments submitted by the ABA Health Law Section (also referred to as the “Section”) to respond to the HIPAA RFI by OCR for public input. The comments and recommendations in this letter were developed by a working group of the ABA Health Law Section’s Interest Groups, including the eHealth, Privacy & Security and Physician Issues Interest Groups.

The Section’s comments provide OCR with input on ways that the HIPAA privacy and security rules could be modified to improve coordinated care. In addition, the comments address potential regulatory changes to decrease burdens and obstacles to facilitate efficient care coordination and/or case management and to promote the transformation to value-based health care, while preserving the privacy and security of protected health information.

The letter includes comments by the Section on the following areas in the HIPAA RFI: (1) promoting information sharing for treatment and care coordination; (2) promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness; (3) Accounting of disclosures; (4) notices of privacy practices and (5) additional ways to remove regulatory obstacles and reduce regulatory burdens to facilitate care coordination and promote value-based health care transformation.

In general, the comments and recommendations of the ABA Health Law Section contained in this letter are intended to provide insight on the topics described by OCR in the HIPAA RFI. We believe that these recommendations contained herein provide input on ways HIPAA privacy and security can improve coordinated care as well as identify solutions to address potential regulatory burdens and obstacles.

a. **Promoting information sharing for treatment and care coordination**

The Section is supportive of any improvements that will improve the efficiency of information sharing for treatment and care coordination without imposing undue administrative burdens on
health care providers, or infringing on individual rights already provided by the HIPAA Privacy Rule, 45 CFR Part 160 and Part 164, Subparts A and E. The basic principle of the HIPAA Privacy Rule is that a covered entity may not use or disclose protected health information (“PHI”) except when the Privacy Rule explicitly permits it or the individual subject of the PHI authorizes it. Pursuant to the Privacy Rule, covered entities are permitted to disclose PHI “for treatment, payment, or health care operations,” and pursuant to a valid HIPAA authorization under 45 C.F.R. § 164.508, among other exceptions not pertinent to these comments. When considering changes to the Privacy Rule to promote information sharing for treatment and care coordination, it is paramount that the individual’s right to have his or her PHI kept confidential not be infringed upon. PHI should be protected and disclosed only as permitted by the Privacy Rule or as authorized by the affected individual. We address some of OCR’s specific requests for information regarding the promotion of information sharing for treatment and care coordination below.

Question 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 30-day timeframe for a covered entity to respond to a request for access to PHI is reasonable and should not be altered without considerable thought regarding the potential industry disruption and increased costs of compliance. If the timeframe is modified, any modification should apply consistently to both paper and electronic records. OCR has requested feedback on the current requirement that covered entities “must act on a request for access no later than thirty (30) days after receipt of the request” pursuant to 45 CFR § 164.524(b)(1). In our experience, most covered entities need the standard 30 days to respond to an individual’s request for access; however, covered entities certainly strive to respond to individual requests sooner and expedite responses if the requests are urgent and records are needed sooner than the permitted 30-day period. If the Privacy Rule is modified to reduce that 30-day timeframe, covered entities would be faced with an increased cost and burden associated with the adoption of new policies and implementation of new procedures (perhaps requiring new or additional technology expenditures, additional staff and/or other new resources) in order to meet these requirements. As a result, the existing 30-day requirement to respond to an individual’s request for access should remain the standard until technology reasonably available to all covered entities makes a shorter time frame feasible at a reasonable cost. Shorter time frames would likely create an undue burden on many covered entities, especially smaller and/or less affluent ones.

Question 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?

If there are two different timeframes for response depending on the method of medical record storage (paper records v. electronic storage), this would create new administrative burdens for covered entities. This would defeat one of the goals articulated in the RFI, which is to reduce the
administrative burdens on covered entities. We respectfully suggest that the benefits of establishing different timeframes based on the type of storage medium used would not outweigh the additional administrative burden and associated costs. Therefore, it is our recommendation that the timeframe not be shortened for covered entities to fulfill requests for electronic PHI, and that different timeframes not otherwise be imposed.

**Question 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?**

OCR seeks input on whether the Privacy Rule should be modified to require disclosures for care coordination, case management, and other treatment purposes. Providers are already permitted to disclose PHI for these purposes, as they are considered disclosures for treatment purposes under 45 CFR § 164.501. The Privacy Rule defines “treatment” as:

> The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Providers are typically ready, willing, and able to share PHI for care coordination and case management purposes. The concept is easily accomplished through the existing permitted disclosures under the Privacy Rule. If there is confusion among health care providers regarding what may permissibly be disclosed for treatment purposes, then perhaps further guidance could be issued for clarification. We do not believe it is necessary that the Privacy Rule be modified, as providers are already permitted to share PHI for this purpose and routinely do so. To the extent state laws that are more stringent than HIPAA impede a covered entity’s ability to share PHI for these purposes, perhaps OCR could modify the Privacy Rule to indicate that state law is preempted if it adversely affects disclosures reasonably necessary for treatment purposes.

Additionally, OCR has requested comments on whether disclosures related to care coordination and case management for non-treatment activities, such as population-based care management, should remain subject to the “minimum necessary” standard. We recommend that the minimum necessary standard should continue to apply to these activities. Although we recommend that the minimum necessary standard should continue to apply to these activities, that standard should be flexible enough to accommodate a health care environment with increasing collaboration and connectivity among multiple covered entities. For instance, where covered entities participate in coordinated care models, OCR should allow those care model participants to follow a coordinated approach to defining “minimum necessary” information for the purposes of supporting their activities that do not specifically apply to a treatment, payment, or health care operation function of each care model.
participant. This would allow clinically integrated networks, accountable care organizations, or other population health management activities that do not qualify as organized health care arrangements to engage in meaningful sharing of clinical information with each other. Overall, we would welcome guidance and clarification from OCR as to how the minimum necessary standard should be applied by covered entities engaged in coordinated care models.

OCR has also sought comments on whether covered entities should be required to disclose PHI to health care providers that are not considered covered entities (i.e., a health care provider that does not engage in electronic billing or other covered electronic transactions) for the treatment and payment purposes of both health care providers. Under the current HIPAA rules, non-covered entity health care providers may receive PHI from covered entities for treatment and payment purposes. In order to better protect the PHI of individuals who seek treatment from non-covered entity health care providers, if such disclosures are mandated in the future, we suggest that OCR provide guidance regarding whether entities that meet the definition of a “health care provider” should have state licensure or should meet other requirements. Furthermore, OCR has asked if individuals should be able to restrict or “opt out” of certain types of permitted disclosures, such as disclosures for health care operations. Health care operations are defined by 45 CFR § 164.501 to include certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. If an individual opted out or restricted disclosure of his or her PHI for use in health care operations, then health care providers and covered entities would not be able to efficiently provide effective care and otherwise engage in normal business operations. Granting individuals the ability to restrict PHI for these purposes would create an unworkable situation for covered entities. We do not recommend that OCR modify the Privacy Rule to permit individuals to unilaterally restrict the disclosure of PHI for this purpose, but we do recommend that individuals continue to have the right to request such restrictions.

Question 5(b): Should health care clearinghouses be subject to individual access requirements, thereby requiring health care clearinghouses to provide individuals with access to their PHI in a designated record set upon request?

OCR has requested information on the role that health care clearinghouses could play in directly providing access to an individual’s PHI. While 45 CFR § 160.103 defines a health care clearinghouse and designates it as a covered entity, no clear guidance has ever been issued regarding what entities are classified as health care clearinghouses. OCR could clear up this confusion by clarifying what types of entities are covered as health care clearinghouses through official guidance. Additionally, OCR has requested comment on whether health care clearinghouses should be required to provide individuals with their designated record sets upon request. This question assumes that health care clearinghouses will have access to an individual’s designated record set, which is often not the case. We do not recommend such a requirement be imposed.
Typically, health care clearinghouses act as business associates for another covered entity and as a result, are subject to the HIPAA requirements of a business associate and are required to enter into a business associate agreement a (“BAA”) with the covered entities for whom they use and disclose PHI. It is our recommendation that health care clearinghouses remain bound by BAAs. The majority of covered entities require their business associates to allow the covered entity to respond to an individual’s request for access to their PHI, which should ultimately be the prerogative of the covered entity whose individuals’ PHI is at issue. For example, if a health care provider is acting as the business associate of another health care provider, such health care provider is required to sign, and be bound by the terms of, that BAA, even though the health care provider may also be considered a covered entity. Health care clearinghouses should not be treated any differently.

Question 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?

The 21st Century Cures Act currently defines information blocking as “a practice that, except as required by law, or specified by the Secretary [of the Department of Health and Human Services] is likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information.” 42 U.S.C. § 300jj-52(a)(1). The regulations promulgated by ONC, intended to define and clarify which practices are considered information blocking, should allow for covered entities to have appropriate measures in place to safeguard PHI under the Privacy Rule and not allow its use or disclosure for purposes beyond those allowed under the HIPAA rules. The ONC rules on information blocking should not be used as a weapon to gain unfettered access to individuals’ PHI, nor should they impede the attempts of covered entities to properly shield PHI from unauthorized disclosures under HIPAA. Covered entities should not fear violating the information blocking rules when attempting in good faith to safeguard the security of the PHI they maintain. A balance must be struck between the desire to have information readily accessible and individuals’ privacy interests. As a result, the ONC regulations defining information blocking should be subject to and preempted by the Privacy and Security Rules, as well as more stringent state privacy laws. Moreover, it is our recommendation that clear guidance be provided by OCR and ONC on how the Privacy Rule requirements and forthcoming ONC information blocking rules are to interact. This guidance would be extremely helpful for covered entities to ensure that these regulations are understood and implemented properly.

Furthermore, those who seek financial gain through data mining by claiming health care providers are “information blocking” should not be provided unlimited access to PHI. They are not covered entities or business associates in most instances. They have no obligations to protect information once they obtain it. OCR and ONC should issue guidance that defines information blocking and clearly identifies what practices are considered information blocking with the goal of protecting
individuals from unauthorized uses of their PHI. As previously noted, measures to protect PHI pursuant to the Privacy and Security Rules should not be considered information blocking.

**Question 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 coordination of care with the provision of other services to the individual?

We do not recommend that OCR create an express regulatory permission for these purposes. Individuals who suffer from these conditions should still be afforded the same right to prevent the disclosure of their PHI, unless specifically authorized pursuant to 45 CFR § 164.508, as those that are not suffering from these conditions.

OCR could potentially promote the sharing of this information for such purposes by publishing a standard authorization form that would meet the requirements of 45 CFR § 164.508, and require covered entities to accept the form if properly executed. Recently, Ohio has adopted a standard authorization form, published by the Ohio Department of Medicaid, which, if properly executed, must be accepted by all Ohio covered entities. This new regulation, Ohio Administrative Code Rule 5160-1-32.1, went into effect in December 2018. Ohio adopted this standard authorization form to address the difficulty faced by the Ohio criminal justice program in obtaining records. If OCR adopted a similar type of regulation and published a form that meets the authorization content requirements of 45 CFR § 164.508, then that form could be uniformly used by individuals and required to be accepted by covered entities across the country.

OCR has asked how a general requirement for covered health care providers to share PHI when requested by another health care provider would interact with other laws that restrict the sharing of information. If OCR were to impose such a requirement, we recommend that OCR also include clear guidance regarding how covered entities should interpret OCR’s requirement in light of the preemption language in the HIPAA rules. For example, if a hospice provider in Florida were required to disclose PHI to a treating provider requesting that information, OCR should provide specific guidance regarding how that provider could comply with HIPAA’s requirements, as well as with Section 400.611, Florida Statutes, which requires a patient’s or legal guardian’s authorization for most disclosures.

**Question 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?

Increased public outreach and education on existing provisions of the HIPAA Privacy Rule would be useful, as would additional guidance on state law preemption. Furthermore, guidance would be helpful regarding who is responsible for a data breach that may occur after PHI is shared. For example, if a covered health care provider shares PHI for treatment purposes with a health care
provider that is not a covered entity, but that experiences a data breach, is the disclosing covered entity responsible to provide breach notification if it learns of the breach? What if the non-covered entity health care provider experiencing the breach is not required to provide notice under state law or any other law?

b. Promoting parental and caregiver involvement and addressing the opioid crisis and serious mental illness

We submit the following responses to specific questions from OCR:

Question 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 may interfere with individuals’ ability to direct and manage their own care? How should OCR balance the risk and the benefit?

OCR seeks comment on its consideration of pursuing separate rulemaking that would seek to encourage covered entities to share PHI with family members, caregivers, and others in a position to avert threats of harm to health and safety, when necessary to promote the health and recovery of those struggling with substance use disorders, including opioid use disorder, and/or serious mental illness. Under the current HIPAA rules, covered entities are already permitted to disclose much if not all of this information to these parties.

Under 45 CFR §164.510(b), a covered entity may disclose an individual’s location, general condition, or death to the individual’s family members (broadly defined at 45 CFR §160.103), a close personal friend or any other person identified by the individual. Section 164.510(b)(3) includes permission for the covered entity to use professional judgment in making disclosures to benefit the individual’s health care, even when the individual cannot provide consent due to the individual’s incapacity or in an emergency circumstance.

Where any new set of regulations would not affect entities subject to 42 CFR Part 2 and/or where state privacy laws are more restrictive/protective of patient privacy than the HIPAA Privacy Rule, there would seem to be little benefit in OCR’s implementing a new set of rules unless OCR could justify being able to pre-empt those others laws and regulations. In addition, the risk of patients choosing to forgo care because the law changed in a manner to permit greater disclosure of their PHI is a significant risk and concern.

Instead of promulgating a new set of rules encouraging disclosure, we recommend that OCR establish a sustained and directed promotion of educational materials to covered entities and clinicians to address an often overly cautious approach when requests are made for access to
information. OCR has a number of good resources to help address the seeming lack of knowledge and correct the large degree of misinformation with regard to the scope of permissible disclosures. See, e.g., https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html. Education on what the HIPAA rules actually permit would arm the industry with awareness and help to drive appropriate action in keeping with the existing regulations and OCR’s goals of improving access to information.

**Question 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?

Consistent with the reasoning set forth above, our recommendation is for OCR to address perceived inconsistencies between the HIPAA rules and treatment of serious mental illness by promoting educational materials to covered entities and clinicians, so that when requests are made by family members and other caregivers for information, the proper information is used and disclosed consistent with the provisions of the HIPAA rules. Varied understanding and implementation of the HIPAA Rules unnecessarily impedes the ability of family members and caregivers to be involved in the treatment and care coordination for individuals with SMI. Another impediment, which cannot be addressed by OCR rulemaking, is the fact that state laws relating to privacy and mental health care and treatment are often more protective/restrictive than the HIPAA Privacy Rule. Finally, for the reasons set forth above, we suggest that encouraging more sharing than what is currently permitted under the rules now in effect would run the risk of not improving care and access to information relative to SMI.

**Question 25:** Could changes to the Privacy Rule help ensure that parents are able to obtain the treatment 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?

We do not recommend modification of the Privacy Rule, and instead recommend consistent and appropriate application of the existing Privacy Rule provisions to enable parents, where appropriate (and when necessary, other authorized guardians, individuals acting in loco parentis, or a court), to act on behalf of an unemancipated minor in making decisions related to healthcare, including the minor’s mental health. We similarly do not recommend changes to the Privacy Rule to allow parents of emancipated minors, adult children or spouses greater access to the treatment information of their emancipated minors, adult children or spouses. The Privacy Rule, when applied as drafted,
provides appropriate protection for the individual and sufficient information for the parent or spouse, and we do not believe any modification is necessary or desirable. We recommend continued efforts by OCR to encourage and incentivize covered entities and healthcare providers to understand and uniformly implement the existing Privacy Rule.

In part c) of this question, OCR also sought comments on whether adult children should be allowed to access the treatment records of their parents in certain circumstances where an adult child is not the parent's personal representative. The Privacy Rule provisions provide protections to everyone, including aging parents, regardless of whether they are being treated for early-onset dementia or inheritable diseases. The Privacy Rule’s protections for all individuals should be preserved, but further guidance may be helpful.

45 CFR §164.502(g)(2) provides the implementation mechanism for the use and disclosure of PHI of adults and emancipated minors. As noted by OCR, it defers to state law and requires the covered entity to treat the person who has authority to act on behalf of an adult or emancipated minor in making health care-related decisions as a personal representative of that individual relative to the use and disclosure of the individual’s PHI. An adult child or other individual who is the personal representative of an aging parent should be provided information about the aging parent in the manner permitted by the Privacy Rule.

In cases of newly diagnosed dementia, the personal representative status of adult children may be less clear, raising the risk that the patient’s safety may be compromised if treatment-related communications are withheld from family members while the personal representative status is being determined. 45 CFR §164.510(b) generally allows disclosures to friends and family members involved in an individual’s treatment if the individual does not object to the disclosure or if the health care provider can infer from the circumstances that the patient would not object to the disclosure. Further guidance on the types of situations where an inference could be drawn with regard to suspected dementia patients and their adult children would be helpful.

The Privacy Rule and state laws relating to designation of personal representatives provide important protections to aging/infirm individuals. The Privacy Rule recognizes and accounts for the potential of abuse, neglect, and endangerment situations. See 45 CFR §164.502(5). The Privacy Rule grants discretion to the covered entity to elect not to treat a person as the personal representative of the individual when the covered entity has a reasonable belief that there is a risk of harm to the individual, or when in the exercise of professional judgment, the covered entity determines it is not in the individual’s best interest to treat that person as their personal representative. There are potential unintended consequences, including potential safety and security risks, which will likely arise if an aging or infirm person’s medical information is provided to another simply because of their familial relationship, without such an informed determination by the covered entity. Accordingly, we believe the existing protections do not require modification.
c. Accounting of disclosures

We have the following general comments in response to OCR’s questions regarding the accounting provisions:

Compliance with the Privacy Rule’s requirement to provide an accounting of disclosures upon request has historically placed a significant burden on covered entities, with seemingly minimal benefit based on how rarely individuals actually request such an accounting. In general, we recommend that OCR reconsider the accounting-of-disclosures requirements to better balance the burden on covered entities with the apparently limited benefit to individuals. For example, it seems appropriate to require that the accounting be limited to a significantly shorter time period, as there is no evidence that individuals are particularly interested in learning about disclosures from six years in the past. We recommend revising the time period for accounting for any disclosures to three years or less.

With respect to the HITECH Act’s requirement to expand the accounting-of-disclosures requirement to include disclosures for treatment, payment, and health care operations (TPO) through an electronic health record, the statute provides that HHS’s regulations should take into account the interests of the individuals and the administrative burden of accounting for such disclosures. As discussed above, evidence is lacking that indicates that individuals request an accounting of disclosures with any frequency. Accordingly, any expansion of the accounting-of-disclosures requirements to TPO disclosures should be at minimal administrative burden to covered entities and business associates.

We believe the best way to achieve an appropriate balance between burden and benefit is to leverage the Medicare and Medicaid Promoting Interoperability Programs (formerly known as the EHR Incentive Payments Programs) and their associated EHR certification standards. A future edition of EHR certification standards should require EHR vendors to build a functionality that automates accounting for disclosures. With the touch of a button, EHR technology should be able to create a patient-specific list of disclosures, identifying which outside entities or persons accessed the patient’s record (such as through health information exchange) and when. The list need not attempt (and should not be required) to identify the purpose of the disclosure, as the burden to try to track the purpose of each disclosure would outweigh the benefit. Covered entities and business associates should then only have to comply with increased accounting-of-disclosures requirements with respect to TPO disclosures through EHRs after they have implemented EHR technology that has the additional functionality. The result would be a benefit to patients with minimal burden on covered entities and their business associates.

Question 27: How many requests for an accounting of disclosures do covered entities receive annually and from what percentage of total patients? Of these, how many requests specify a
particular preferred electronic form or format, and to what extent do covered entities provide the accounting in the requested form or format?

Although anecdotal, the experience of the attorneys contributing to these comments has been that covered entity and business associate clients receive a negligible number of requests for an accounting of disclosures each year, with many clients having never received a single request for an accounting of disclosures.

Question 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?

Business associates often do not have a direct relationship with the individual and are ill-equipped to handle requests for an accounting of disclosures from an individual. For example, a cloud services provider that maintains data for a covered entity that includes PHI would likely be unable to respond to an individual’s request for an accounting of disclosures. The cloud services provider may not even have access to the PHI that is maintained on its server.

Question 39: If covered entities are unable to modify existing systems or processes to generate a full accounting of disclosures for TPO (e.g., because modification would be prohibitively costly), should OCR instead require covered entities to conduct and document a diligent investigation into disclosures of PHI upon receiving an individual’s request for an accounting of disclosures for TPO? If not, are there certain circumstances or allegations that should trigger such an investigation and documentation by a covered entity? How much time should a covered entity be allowed to conduct and provide the results of such an investigation?

We recommend against assuming that every request for an accounting of disclosures for TPO results from an individual’s belief that a disclosure was impermissible. Rather, we believe the current requirement at 45 C.F.R. §164.530 to have a complaint process is sufficient to address complaints by individuals when they believe that an impermissible disclosure was made.

Question 40: If OCR requires or permits covered entities to conduct an investigation into TPO disclosures in lieu of providing a standard accounting of such disclosures, what information should the entities be required to report to the individual about the findings of the investigation? For example, should OCR require covered entities to provide individuals with the names of persons who received TPO disclosures and the purpose of the disclosures?

We recommend against requiring covered entities and business associates to specify particular persons, rather than entities, in their accounting of disclosures. Providing an aggrieved patient with the names of specific persons to whom disclosures were made, rather than the names of the entities
with which those persons were affiliated, could in certain cases lead to safety concerns for the named persons.

**Question 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 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?

We believe that OCR should limit any requirements for an accounting of disclosures for TPO to PHI that is disclosed through an EHR, and only after HHS has amended EHR certification standards to require EHRs to produce patient-friendly accountings of disclosures (in contrast to audit logs that may not be readily understood by a patient). We believe that this would be the only way to balance the seemingly limited benefit to patients with the burden on health care providers. In contrast, including paper records in an expanded accounting of disclosures would cause a significant burden to health care providers to track each disclosure of paper records, with likely minimal benefit to individuals.

d. **Notice of Privacy Practices**

In practice, there are concerns that HIPAA Notices of Privacy Practices (“Notices”) are meaningless to the patient and burdensome to the covered entity. We would welcome guidance on how to make the notice more user friendly and meaningful to patients without substantially increasing the burden on health care providers.

e. **Additional ways to remove regulatory obstacles and reduce regulatory burdens to facilitate care coordination and promote value-based health care transformation**

We submit the following responses to certain specific questions from OCR, listed below:

**Question 54(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 care management? What provisions of the HIPAA Rule may inhibit the transformation of the health care system to a value-based care system?**

As recognized by OCR in the RFI, many of the issues surrounding facilitation of care coordination and promotion of value-based health care are addressed by earlier questions in the RFI. Many existing requirements and obligations included in the HIPAA Privacy and Security Rules enable the
use and disclosure of PHI between and among health care providers, health care payors, business associates, and downstream subcontractors of each type of entity.

When considering care coordination, care management, and value-based healthcare, we believe that one of the most important obstacles to overcome is the reluctance of covered entities and business associates to share PHI. Fear of violating requirements established by the HIPAA rules and being called to task for such violations can result in an overly cautious approach to sharing PHI or acceding to individual requests for access. We believe that the issue is not actually the HIPAA rules as currently drafted, but rather a misunderstanding of how to apply those rules, especially in light of current technology. Therefore, we suggest that OCR provide additional guidance on how covered entities and/or business associates are permitted to share PHI, especially in the context of value-based programs. Making more analysis and knowledge available to the healthcare industry can assist OCR in spreading awareness of the full potential and benefit that can be achieved under the HIPAA rules.

Although existing regulations are already consistent with, and potentially helpful for implementing, care coordination and value-based care, we believe that: (i) adding the term “Care Management Network” to the definition of covered entity, (ii) expanding data aggregation uses and disclosures, and (iii) modifying standards for de-identification would result in better alignment between HIPAA and the changing delivery of healthcare.

Amending Definition of Covered Entity

The term “covered entity” is defined at 45 C.F.R. § 160.103 to include health plans, health care clearinghouses, and health care providers that transmit any health information in electronic form in connection with a transaction covered by HIPAA. That is the exclusive list of entities that qualify as covered entities. Any person that performs services on behalf of a covered entity and handles PHI for or behalf of the covered entity is a business associate.

While value-based networks may have different labels, such as accountable care organizations (ACO), clinically integrated networks or independent practice association, they are all focused on managing care for a certain population of patients. We therefore recommend that all such networks be referred to under the HIPAA rules as "Care Management Networks."

In the regulations implementing the Medicare Shared Savings Program (MSSP) administered by the Centers for Medicare and Medicaid Services, an “accountable care organization” is defined as “a legal entity that is recognized and authorized under applicable State, Federal, or Tribal law, is identified by a Tax Identification Number (TIN), and is formed by one or more ACO participant(s) that is(are) defined at § 425.102(a) and may also include any other ACO participants described at § 425.102(b).” (42 C.F.R. § 425.20). Built into the definition is the expectation that a distinct, new
legal entity is formed to be the controlling or governing entity of the ACO. Such a structure is common in all of the Care Management Networks.

From an operational perspective, a Care Management Network typically provides administrative services and manages the operations of the network, such as contracting with payors and participating providers, analyzing data concerning treatment of covered patients, and other similar tasks.

Since a Care Management Network is a distinct legal entity that provides services on behalf of its participating providers who render health care services, the Care Management Network is a business associate under the current HIPAA Rules. As a business associate, the Care Management Network may only use and disclose PHI as permitted by HIPAA and in accordance with the terms of its BAA with its participating providers.

From a practical perspective, however, a Care Management Network acts more like a covered entity than a business associate, since it is the central operating entity that bears responsibility for the operation of the network as a whole. Care Management Networks often perform a number of activities that would constitute treatment, payment or health care operations for purposes of the HIPAA rules, including (i) receiving claims data, and patient information and records; (ii) coordinating care; (iii) establishing distribution methodologies for shared savings and incentive payments; (iv) facilitating data exchange among participating providers; (v) entering into payor contracts on behalf of the network; (vi) establishing standards of care; (vii) conducting utilization review and quality assurance activities; and (viii) providing management activities.

Our suggestion to add “Care Management Network” to the definition of covered entity would align the HIPAA Rules with the practical operations of Care Management Networks. The modification could be achieved by including “Care Management Network” in the existing definition of covered entity and then separately defining that term in the HIPAA Rules by including a modified version of the definition of an ACO existing in other regulations, such as the MSSP regulations, to incorporate value-based networks more generally. For example, a Care Management Network could be defined as a “network of covered entities that organizes and supports patient care activities and information sharing among participants in the Care Management Network to facilitate coordination and cost-effectiveness in the provision of services to patients.”

Designating the Care Management Network as a covered entity, and exempting Care Management Networks from the requirement to enter into business associate agreements with the other covered entities they serve, could also ease issues around data retention, analysis, and application. A covered entity has control over PHI that it receives and can retain such information indefinitely or in accordance with applicable state law. By contrast, a business associate is only permitted to use or disclose PHI on behalf of the covered entities it provides services to, and only for the duration of its relationship with such covered entities. This means that when a participating provider leaves the
network, a Care Management Network would be required to return or destroy PHI created, received, maintained or transmitted from that provider in accordance with the terms of its BAA. As a covered entity, however, the Care Management Network would be able to continue to use and disclose the PHI that it maintains.

*Question 54(b) - What modifications to the HIPAA Rules would facilitate efficient care coordination and/or care management, and/or promote the transformation to value-based health care?*

We believe that expanding the existing definition of "data aggregation" set forth at 45 C.F.R. § 164.501 could open up the ability for different organizations to expand and enhance the ability to analyze data and provide actionable insights to inform value-based care decisions. If PHI could be retained beyond the scope of a covered entity/business associate relationship, then greater accumulations of data could occur that could benefit the design, improvement, and refinement of many types of technology-based tools.

"Data aggregation" is currently defined at 45 C.F.R. § 164.501 to mean the combining by a business associate of PHI received from multiple covered entities "to permit data analyses that relate to the health care operations of the respective covered entities." We believe that this definition should be expanded to permit retention of such PHI to provide analyses to any covered entity.

As currently drafted, a business associate can only use PHI for data aggregation purposes while engaged by the relevant covered entities. If an engagement ends, the business associate must return or destroy the PHI. As such, under the HIPAA rules, a business associate can no longer access such PHI when the agreement ends. This can result in an ongoing ebb and flow of available data that could disrupt an analytics platform. While the business associate could retain de-identified data (if agreed upon by the covered entity and the business associate), such data are not as robust and potentially not as meaningful.

We propose permitting business associates to maintain PHI beyond the termination of the relationship with a covered entity for certain limited purposes, including data aggregation and analysis for purposes that are reasonably related to value-based care. Any such retained PHI would remain subject to all applicable privacy and security requirements under the HIPAA Rules, and business associates would not be permitted to sell or engage in marketing with the retained PHI.

Consideration for modifying the definition can be highlighted with two parallel, but distinct examples. First, permitting Care Management Networks (to the extent they remain business associates) to maintain PHI for data aggregation purposes related to value-based care would allow Care Management Networks to use such information to improve the quality and efficiency of patient care and further promote the transformation to value-based health care. Currently, when a health care provider terminates its participation in a Care Management Network, the Care Management Network must return or destroy that provider’s PHI pursuant to the terms of the applicable BAA and
in accordance with HIPAA Rules (absent some other justification for retention), which arguably impedes the ability of the Care Management Network to effectively coordinate care and develop a comprehensive picture of covered patients. By contrast, if the Care Management Network could maintain PHI to use for purposes related to value-based care, regardless of which participating providers remained in the network, the potential for disruption would be greatly reduced, while the utility of the data available for analytics would be greatly enhanced.

The second example would be a population health vendor that offers a data analytics platform premised upon ingesting data and providing actionable outputs. Such vendors are becoming commonplace and will often contract to be able to de-identify PHI, which means that such de-identified data is no longer subject to the HIPAA rules. If the definition of data aggregation were expanded to allow the vendor to maintain PHI for limited purposes reasonably related to value-based care, then such vendors would be able to use PHI for data analytics, rather than being forced to de-identify PHI, and more data would remain subject to the HIPAA rules. Additionally, the ability to retain PHI could accelerate the development and refinement of tools that will drive success in the transition to value-based care.

*****

Thank you for the opportunity to submit these comments. If you have any questions or would like any additional information, please contact Alexandria Hien McCombs, Chair of the Health Law Section, at (972) 643-1619 (amccombs1@humana.com) or Simeon Carson, Director of the Health Law Section, at (312) 988-5824 (simeon.carson@americanbar.org).

Very truly yours,

Alexandria Hien McCombs
Chair
ABA Health Law Section