

February 8, 2019

Roger Severino
Director
Office for Civil Rights
U.S. Department of Health and Human Services
Hubert H. Humphrey Building
200 Independence Avenue, SW
Washington, DC 20201

RE: Request for Information on Modifying HIPAA Rules to Improve Coordinated Care
(RIN 0945-AA00)

Dear Director Severino:

On behalf of the physician and medical student members of the American Medical Association (AMA), I appreciate the opportunity to respond to the request for information (RFI) from the Office for Civil Rights (OCR) on the Health Insurance Portability and Accountability Act (HIPAA) regulations and how these regulations can be revised to promote the goals of value-based care and care coordination while preserving and protecting the privacy and security of a patient's health information. Generally, the AMA does not object to amending existing regulatory exceptions or definitions to promote care coordination and appreciates OCR's exploration of ways to reduce barriers to sharing Protected Health Information (PHI). However, a multifaceted approach that establishes multiple new definitions, permissions, or exceptions would add more burden and complexity to an already confusing law and could go too far in infringing on patients' privacy rights. We encourage OCR to promote information sharing for treatment and care coordination and/or case management through education and positive incentives—not requirements—especially those that value speed over privacy.

The first step of any ultimately successful privacy framework, legislative or regulatory, places the patient first. Each entity seeking access to patients' most confidential medical information must pass the stringent test of showing why its professed need should override individuals' most basic right in keeping their own information private—something that technology can help physicians accomplish in a minimally burdensome way. Moreover, citizens deserve a full and open discussion of exactly who wants their private medical information and for what purpose. Only then may the true balancing of interests take place. These are the ground rules of AMA policy and they should be the ground rules for the federal debate regarding data privacy.

The AMA's approach to privacy is governed by our Code of Medical Ethics and long-standing policies adopted by our policymaking body, the House of Delegates, which support strong protections for patient privacy and, in general, require physicians to keep patient medical records strictly confidential. **AMA policy and ethical opinions on patient privacy and confidentiality provide that a patient's privacy should be honored unless waived by the patient in a meaningful way, de-identified, or in rare instances when strong countervailing interests in public health or safety justify invasions of patient**

privacy or breaches of confidentiality. When breaches of confidentiality are compelled by concerns for public health and safety, those breaches must be as narrow in scope and content as possible, must contain the least identifiable and sensitive information possible, and must be disclosed to the fewest entities and individuals as possible to achieve the necessary end.

These policies and ethical opinions are designed not only to protect patient privacy, but also to preserve the patient-physician relationship. This is particularly important in scenarios involving sensitive health information. For example, striking the correct balance is critical in encouraging individuals with mental illness and/or substance use disorders (SUD) to seek treatment. Consumers are also increasingly concerned with privacy in today's environment (e.g., the Facebook–Cambridge Analytica data scandal). In fact, many industries, states, and countries are moving towards increasing privacy rights and protections, not expanding ways in which information can be shared without an individual's consent.

Health care information is one of the most personal types of information an individual can possess and generate—regardless of whether it is legally defined as “sensitive”—and policymakers must be very cautious in discussions of how to relax regulation around privacy. **We must always ask whether relaxing privacy controls will encourage patients to seek care or potentially deter them. Privacy risks include re-identification of patients through de-identified (or partially de-identified) data, misunderstanding or disregard of the scope of a patient's consent, patient perception of loss of their privacy leading to a change in their behavior, embarrassment or stigma resulting from an unwanted disclosure of information or from fear of a potential unwanted disclosure, perceived and real risks of discrimination including employment and access to or costs of insurance, and law enforcement accessing data repositories beyond their intended scope.**

Additionally, we strongly urge OCR to review comments on the forthcoming information blocking rules from the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) to inform its thinking about the questions asked in this RFI. Many of the questions cannot be properly analyzed without fully reviewing those rules in tandem and OCR should not issue any Notices of Proposed Rulemaking on these topics until CMS' and ONC's rules are finalized.

Moreover, interoperability plays a crucial role with respect to the availability of information. Unfortunately, a patient's medical records are not available to the patient or all of the patient's providers at any given time. Given the current state of interoperability, a clinician cannot go to his or her electronic health record (EHR) and “pull” a patient's PHI upon request. In fact, most clinicians cannot obtain a patient's health information from other clinicians electronically, often resorting to fax or having the patient bring copies of his or her record to the treating provider from the rendering provider.¹ This problem will continue to exist even if OCR requires disclosure of PHI. Of course, the AMA is trying to advance the state of interoperability such that this type of search could occur, but that is likely years away. Changes in technology must occur first; such changes would be a much more effective way to address improved information exchange, protect consent and privacy rights, care coordination, and overall PHI availability than adjusting HIPAA to require PHI disclosure.

¹ This issue persists even if the physician is part of a regional or EHR-based HIE. For example, just as is the case currently in healthcare, there may be 40 different “John Smith”s in an EHR and patient-matching is notoriously difficult.

Importantly, physicians and other covered entities are confused as to HIPAA's requirements and how to comply with the HIPAA security rule. Physicians hear different interpretations from colleagues, staff, administrators, in-house counsel, and private practice attorneys. This confusion, coupled with the fear of OCR investigations, leaves physicians to presume the worst and potentially not disclose PHI out of fear. More needs to be done to ensure that physicians are well-educated on the best approaches to securing and ensuring patient information remains private within an EHR when it is exchanged electronically, and that access is only granted to those who should have access.

Please see our below comments to specific sections and questions from the HIPAA RFI.

a. **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?

The length of time needed to respond to an individual's request for a copy of their PHI will vary with each practice and health care system. Some practices may be able to provide records more quickly if, for example, the practice has relatively few patients, has an established and well-functioning health information management department or employs a full-time privacy officer, or the patient is only asking for a small portion of his or her records. Alternatively, practices with a large number of patients, practices without records management procedures, practices that receive a large number of access requests, and practices lacking employees dedicated to health records management may struggle to expeditiously respond to patient requests (though may still do so within the time required under HIPAA). Additionally, a practice may take longer to respond to established patients with large records as opposed to a patient with relatively small records. Further, a practice may store records of patients who have not recently been seen by the practice in an offsite long-term storage facility, which may take longer to access than the records of current patients.

As it relates to patient access, OCR must consider technology's impact on the ease of data access; namely, EHRs are not designed to export a patient's entire designated record set (DRS). Instead, EHRs provide electronic access to a limited number of data elements (the common clinical data set, or CCDS). To provide a patient with his or her entire DRS—as required under HIPAA—a practice must first be sure to collect information stored both in and out of the EHR. Any information stored in paper records or in other electronic systems (e.g., a practice management system, or PMS) must be scanned or imported into the EHR. At that point, most commonly, the practice must download the file(s) to a CD-ROM or thumb drive. This practice is cumbersome, time-consuming, and may be difficult to do if the DRS includes imaging files, which are often very large.

(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 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?

A patient should always be able to receive his or her records in a timely manner. However, as described above, OCR should also recognize that specific practice response times to access requests will vary depending on the individual practice, the size of the patient's record and what portion of the record the patient is requesting, where the patient's records are located, and, presumably, the number of requests received by the practice.

Shortening the timeframe in which a practice must respond to access requests would almost certainly increase the practice's administrative burden, particularly in practices without personnel dedicated to records management. Administrative staff in small practices often "wear multiple hats" and have multiple disparate responsibilities, so staff can become spread thin when additional responsibilities are added through regulation. The AMA has heard discussions of shortening a patient access timeline to 24 hours; we caution OCR that doing so would be incredibly difficult for some practices for the reasons described in the answers to this and the previous 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? (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?

In theory, covered entities may be able to provide PHI stored electronically more rapidly than PHI stored in other media. However, the timeliness of response to record requests will vary depending on what information the patient wants, where the information is stored, and how a patient wants to receive it. For example, patients can access a patient portal on demand; a patient wanting information that is not available through a portal will have to wait longer to receive such information and may only be able to receive it on a CD or USB.

Further, OCR must consider whether it wants to establish two different timeframe standards depending on whether the information is stored electronically or on paper. Different timelines may be confusing for practices, particularly if records are stored in both mediums. More broadly, covered entities have always been told that HIPAA is agnostic; as OCR notes, the law applies equally to PHI stored in any format. Different timelines for different mediums could alter understanding and interpretation of other aspects of the law. Accordingly, AMA supports one timeframe regardless of modality.

Lastly, OCR should consider complications that could arise based on the location of data a physician uses to inform his or her decision-making (which is one way in which OCR defines a designated record set). For example, a physician may use images to make a decision about a patient's course of treatment. The physician may only have access to view the image as opposed to being able to directly incorporate it into his or her EHR. To obtain a copy, the physician would need to request that the image be mailed to his or her office on a CD or USB. Yet, if a patient asked for a copy of the image, knowing that the physician used it in his or her decision making, the physician would be unable to provide such information and could be violating a regulatory requirement.

(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.

As noted above, a shortened timeframe for responding to access requests could be impracticable for many reasons. Administrative staff have myriad responsibilities, some of which must be prioritized to ensure continuity of and appropriate delivery of care (e.g., prior authorization requests, management of which can amount to two business days per week by the physician and his or her staff).² Again, a shortened response timeframe may become incredibly burdensome if a patient requests his or her entire record and/or has been a patient for many years. It may not be feasible for practices who store old records offsite to provide rapid patient access to those records. In this case, simply accessing the records could take over a week and, if the patient requests the information electronically, staff must scan the information into an electronic format. This process can take over two weeks. The many nuances of this process—not physician unwillingness to share information—make it unrealistic to always expect a quick response to a request for PHI. In sum, federal regulation and policy must balance the goal of prompt patient data access with the limitations placed on physicians and patients by the design and development of health IT (addressed more below), the characteristics of a physician’s practice, and the logistics associated with obtaining a patient’s record.

(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.

This is a solution in search of a problem. The vast majority of patients will not know who or what a clearinghouse is or what its function is. We find it highly unlikely that a patient will seek his or her medical records from a clearinghouse as opposed to his or her treating clinician. Further, a patient’s information may reside with multiple clearinghouses, which would require the patient to seek access from multiple entities, negating any potential benefit of not having to seek information from multiple health care providers. In fact, physicians would likely receive most questions, complaints, and blame from patients regarding a clearinghouse’s use of a patient’s data. This activity would take time away from the physician-patient relationship and the provision of care. Even if administrative staff fields these questions, it is an additional and inappropriate burden and cost on physician practices and the health care system.

(a) How commonly do business associate agreements prevent clearinghouses from providing PHI directly to individuals?

This question is impossible to answer without a survey of all business associate agreements (BAAs) between clearinghouses and covered entities. **HIPAA rightly leaves the matter up to**

² 2017 AMA Prior Authorization Physician Survey, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/arc/prior-auth-2017.pdf>.

the covered entity as it is in the best position to know what type of information is in question and how the information should (or should not) be used and disclosed by the clearinghouse.

Covered entities may opt to allow clearinghouses to directly provide a patient with his or her records to help reduce administrative burden or they may determine that the practice is best-suited to do so; it is a contractual matter and a business decision.

(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 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?

We again note that we do not believe that most patients will know who their clearinghouse is and thus would not request records directly from the clearinghouse. That said, if a patient does happen to identify the clearinghouse that is a business associate of his or her covered entity, a clearinghouse should not be barred from providing a patient with his or her record if the clearinghouse's BAA so permits.

Importantly, BAAs, apply restrictions on the business associate's use and disclosure of PHI beyond patient access rights. Clearinghouses (and other business associates) should remain bound by BAAs even when a covered entity does not permit the clearinghouse to directly disclose PHI to an individual.

(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 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?

Changing BAA requirements would require a statutory change. HIPAA defines a business associate as an entity that performs a function on behalf of a covered entity and requires the parties to enter into a BAA for sufficient assurances that a patient's information will only be used and disclosed in specific ways.

Accordingly, if a clearinghouse is performing a function on behalf of a covered entity, **a clearinghouse should be considered a business associate and required to enter into a BAA.** Unlike a general contract, a BAA is a contract specifically delineating how PHI may be used or

disclosed. It typically imposes most, if not all, of the requirements and prohibitions in the HIPAA rules concerning the use and disclosure of PHI, and the parties can always incorporate additional restrictions on the use and disclosure of PHI into the BAA, though violations of those restrictions would not necessarily implicate HIPAA. In this sense, HIPAA acts as an equalizer. It provides “bargaining power” to covered entities (such as small physician practices) that would not otherwise have leverage against larger organizations or systems.

If BAAs were not required, smaller entities could be forced to accept whatever terms the other party demanded; indeed, even now physician practices are often forced to accept a business associate’s standard BAA (typically with terms favorable to the business associate) if the business associate has a large enough market share. Particularly given that clearinghouses generally use and disclose only claims (rather than clinical) data, removing BAA requirements seems to be more about reducing a clearinghouse’s contractual liability and increasing its opportunity to monetize data exchange than improving patient access to PHI.

(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?

As noted above, a BAA imposes accountability on a business associate to disclose and use PHI only as specified in the agreement. **The covered entity is the steward of the patient’s PHI and has a duty to the patient to protect his or her information. Business associates—including health care clearinghouses—performing business associate functions should always be required to enter into BAAs.**

While it is possible that physician administrative burden may be reduced if the requirement to have BAAs were eliminated, we urge OCR to consider and account for potential unintended consequences that may increase physician administrative burden—and confuse patients—in other ways:

- What will become of existing BAAs if the requirement to have a BAA is eliminated? Any provision of a BAA between a health care provider and another covered entity that conflicts with the adjusted BAA rules would be invalidated—would the rest of the BAA remain in place or would OCR envision the BAA agreement becoming null and void overnight? What about stricter state law pertaining to privacy or contracts?
- How will patients know which entities have rights to access and use of their PHI? For example, while a health care provider must affirmatively provide a Notice of Privacy Practices (NPP) to its patients, HIPAA only requires a clearinghouse to put an NPP on its website and to make it available to any person who asks for it. Given that most individuals do not know what clearinghouse(s) their claims go through, many individuals will not know that their information is being used and disclosed in new ways by new entities. Furthermore, health care clearinghouses do not currently need to develop an NPP if the only PHI they create or receive is as a business associate of another covered entity. Will clearinghouses be equipped to adequately provide patients with an NPP if they are no longer considered a business associate?

- Similarly, will patients be alarmed upon learning that an entity other than their treating clinician has their PHI without their knowledge? Will the patient understand why the other entity has the PHI?
- Who will ultimately be liable for breach responsibilities? If BAA status for covered entities performing business associate functions is removed, non-business associate covered entities may be confused about who is responsible for notifications to various parties in the event of breach. For example, would the creator of PHI (e.g., a clinician) be responsible to the patient given his or her relationship with the patient or would the breaching entity (e.g., a different provider, the payer, or the clearinghouse). Negotiating these types of activities may outweigh the potential burden reduction of not having to craft and enter into BAAs in the first place.

(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 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.

Please see our response to Question 7 below.

(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?

The AMA strongly opposes any mandate or requirement to disclose PHI to another covered entity for any purpose. Requiring a physician to share information against a patient’s wishes strips patients of control over their own data and potentially overrides medical decision-making. It also vastly increases the opportunity for bad actors to request information for illegitimate, malicious, or commercial purposes. This type of activity occurs even now; compelling disclosure would undoubtedly add to the number of fraudulent requests. A requirement that covered entities disclose PHI upon request—especially for purposes beyond treatment—weighs far too heavily in favor of those who seek access to patients’ private information, with inadequate deference to a patient’s fundamental right of privacy.

While specific consent is not required in the case of treatment, the AMA’s Code of Medical Ethics states that patients generally are entitled to decide whether and to whom their PHI is disclosed. Patients need to be able to trust that physicians will protect information they have shared in confidence. They should feel free to fully disclose sensitive personal information to enable their physician to most effectively provide needed services. Physicians in turn have an ethical obligation to preserve the confidentiality of information gathered in association with the care of the patient.³ The AMA’s policy states that “[c]onflicts

³ *AMA Code of Medical Ethics, 3.2.1 Confidentiality*, available at <https://policysearch.ama-assn.org/policyfinder/detail/3.2.1%20Confidentiality?uri=%2FAMADoc%2FEthics.xml-E-3.2.1.xml>.

between a patient's right to privacy and a third party's need to know should be resolved in favor of patient privacy."⁴

The AMA understands and acknowledges that covered entities may occasionally resist the request to share PHI. However, the reasons for such hesitance are varied and are not always unreasonable, as the examples below demonstrate:

- **Fear of enforcement: Physicians often fear that OCR will determine that they have inappropriately shared PHI despite good faith efforts to comply with the HIPAA rules.** While OCR has issued guidance on certain topics, the guidance is not getting into the hands of those who need it, including not only clinicians, but also health care organizations' attorneys and compliance officers. There are numerous ways in which HIPAA permits covered entities to share information (including to family, friends, and caregivers, on which we comment further below) and yet there is hesitance for fear that a misstep will invoke OCR enforcement and hefty fines. The health care community needs better education on how existing HIPAA regulations permit information sharing—not necessarily new regulations, particularly at the expense of patient privacy and autonomy. The AMA would like to collaborate with OCR on ways to ensure covered entities receive the education they need.
- **Patient preference: There are times that a patient does not want certain sensitive information shared beyond his or her physician's practice.** For example, a patient may not want his or her diagnosis of depression shared with his or her dermatologist. The physician can (and should) discuss with his or her patient the benefits and importance of sharing such information if, in the physician's best judgment, such a conversation is warranted. This complication could be much more easily addressed if data segmentation capabilities were made more widely accessible to physicians, and at an affordable cost, as more fully discussed below.
- **Security concerns: Physicians recognize that there are potential security risks inherent in sharing information electronically.** A 2017 first-of-its-kind AMA/Accenture study on physician understanding of HIPAA and cybersecurity (AMA Survey) found that 85 percent of physicians believe it is "very" or "extremely" important to electronically share electronic PHI to provide quality care—they just want to do it safely.⁵ Security concerns may be related to the physician's own electronic record system(s) or that of the recipients.
- **State law: State law may be more restrictive than HIPAA.** Most states permit a physician to make a best-judgment determination about whether and how to share PHI. The AMA also is concerned about how OCR will address state law that prohibits sharing PHI with third-parties (generally for purposes other than treatment, payment, and operations (TPO)) absent a patient authorization given that it would conflict with—and be more restrictive than—HIPAA.
- **Natural disaster: Physicians may not have access to PHI during and following natural disasters and would thus be unable to send such information, even for treatment purposes.** Other federal

⁴ *AMA Policy, Informed Consent and Decision-Making in Health Care H-140.989*, available at <https://policysearch.ama-assn.org/policyfinder/detail/%22Informed%20Consent%20and%20Decision-Making%20in%20Health%20Care%22%20?uri=%2FAMADoc%2FHOD.xml-0-520.xml>.

⁵ *Taking the Physician's Pulse, Tackling Cyber Threats in Healthcare*, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser-public/gouvernement/advocacy/medical-cybersecurity-findings.pdf>.

agencies have recognized that natural disasters can prevent a physician from accessing his or her EHR for an extended period of time.⁶

- **Minimum necessary: Physicians are required to disclose only the minimum necessary information for payment and health care operations purposes. The AMA’s policy supports this principle.** One physician’s idea of minimum necessary may differ from another covered entity’s idea about the same patient’s record and may thus result in what appears to be a withholding of information.

(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 administrative costs arise because covered entities would have to manage and fulfill requests for PHI that previously would not have been fulfilled?

The AMA supports OCR’s goal of encouraging and incentivizing care coordination and case management through information sharing. We understand the many benefits of care coordination and have advocated for numerous steps Congress and the administration can take to promote it. We note, however, that **current HIPAA regulations permit covered entities to use and disclose PHI for care coordination purposes.**⁷ Covered entities should not be required to disclose PHI for care coordination and/or case management merely because many covered entities, their lawyers, and their compliance officers do not understand how HIPAA currently permits such disclosures. **The answer to a lack of education is not stripping a patient of control over his or her privacy rights.** Patient consent continues to be a critical consideration in the use and disclosure of PHI.

The AMA has continuously maintained that an expressed “need” for information—including for care coordination purposes—does not confer a right to such information, particularly when it conflicts with a patient’s wishes. Some parties may reject this principle as too deferential to patients’ rights at the expense of administrative feasibility. However, the AMA believes that this approach properly balances the interests at stake.

(b) Should any limitation be placed on this requirement? For instance, should disclosures for health care 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?

As the Secretary of the Department of Health and Human Services (HHS) has previously noted⁸ and we have stated above, individuals generally do not recognize that their PHI may be used for a multitude of purposes beyond their individual care and payment for that care. Patients reasonably

⁶ *Frequently Asked Questions—Promoting Interoperability (PI) Hardship Exceptions*, available at https://qpp-cm-prodcontent.s3.amazonaws.com/uploads/151/FAQs_PI%20Hardship%20Exceptions_Extreme%20and%20Uncontrollable%20Circumstances%202018%2007%2030.pdf.

⁷ 45 CFR §164.501 (definition of *health care operations*).

⁸ 64 Fed. Reg. 59918 (Nov. 3, 1999) at 59985.

expect that the treatment rendered by their physicians will be revealed to their health plan or other insurer to pay the claim of benefits. However, most patients do not expect, nor do they welcome, unauthorized access to PHI disclosed in the context of a confidential relationship for the wide range of purposes under health care operations. AMA policy calls for “health care operations” to be narrowly defined to include only those activities and functions that are routine and critical for general business operations and that cannot reasonably be undertaken with de-identified information.

We also note the statutory right of patients to request restrictions on disclosure of PHI if the patient pays out of pocket. Requiring disclosure of patient information would effectively remove this right, which could deter some patients from seeking care. As such, the AMA believes that OCR should maintain the right to request restrictions on disclosures and, in fact, encourages OCR to expand it.

If OCR insists on mandated disclosure for any purpose, it should only be among health care providers and for treatment purposes, except where such disclosure would conflict with a patient’s right to privacy. Creating any additional caveats would create a web of regulatory requirements, which would profoundly confuse all parties. Further, payers could request information beyond what is minimally necessary and use such information to discriminate against patients or delay care, either by denying claims or coverage for services, or requiring burdensome prior authorization for a patient’s needed medication, services, or devices.

(c) Should business associates be subject to the disclosure requirement? Why or why not?

For the above reasons, neither covered entities nor business associates should be required to disclose PHI to another covered entity.

(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?

For the above reasons, no covered entities or business associates should be required to disclose PHI to another covered entity.

(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 entity or the noncovered 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?

For the reasons enumerated above, HIPAA-covered entities should not be required to disclose PHI to non-covered health care providers under any circumstances. Additionally, given that non-covered entities are not required to implement HIPAA privacy and security safeguards, implementing a requirement that physicians disclose PHI to such entities could expose physicians and other covered entities to liability. Covered entities may also be less inclined to adhere to their own privacy and security requirements if they know they must send the PHI and they know they are sending information to an entity that does not need to adhere to the same requirements. Even if OCR permitted the information sharing without the need for an additional agreement, practices' risk management staff, privacy officers, and/or compliance counsel would almost certainly create internal policies requiring the practice to enter into new contractual agreements to head off real or perceived vulnerability to liability. This would increase administrative burden and it would cause additional fear of sharing information that may not remain private and within the health care provider community. If OCR creates this requirement, it must offer a safe harbor for physicians to ensure that their good faith efforts to comply with the requirement does not expose them to OCR enforcement or state law privacy requirements.

(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.

With the understanding that the AMA does not support a disclosure requirement, should OCR choose to propose one, it should require non-covered entities requesting information to complete a written assurance that the requested PHI is for TPO purposes. The assurance should relieve the covered entity of any liability incurred by providing—in accordance with the law—information to a non-covered entity who is not actually using the PHI for TPO (though we question why a non-covered entity would need to request PHI for payment purposes). Nevertheless, this requirement would need to be balanced with the administrative burden incurred by requiring the covered entity to review and retain such documentation. OCR must again consider how such a requirement would interact with state laws.

(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?

The AMA supports maintaining the current minimum necessary standard for disclosures to covered entities (i.e., we do not support a requirement to disclose an entire DRS). We also do not support a requirement to disclose psychotherapy notes and note that even patients do not have access rights to their psychotherapy notes.

(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 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?

We believe that timeliness requirements to provide covered entities with PHI should align with those that exist for patients (within 30 days, with a possibility of a 30-day extension if warranted).

(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?

With the understanding that the AMA does not support a disclosure requirement, should OCR choose to propose one, individuals should be able to restrict or “opt out” of certain types of required disclosures. We note that patients may not understand how their information will be shared and may not know what they “should” or “should not” opt out of. Patient privacy illiteracy could thus lead to disclosures of information that the patient wished to keep confidential. We also note that it may be difficult for patients who have multiple providers to remember who all of their providers are, let alone manage their opt out preferences. It may also be difficult to manage downstream disclosures. In other words, if a patient does not opt out of information sharing initially, and a clinician discloses that information to multiple other clinicians, the patient must then contact all of those clinicians to “opt out.” (It would be overwhelmingly burdensome to require a covered entity to perform that task.) It may also prove difficult for covered entities to manage opt out requests if the patient only opts out of sending portions of their record instead of the entire record (though we note that technology could help manage this concern as explained in later sections on data segmentation).

(14) How would a general requirement for covered health care providers (or all covered entities) to share PHI when requested by another covered health care provider (or other covered entity) interact with other laws, such as 42 CFR part 2 or state laws that restrict the sharing of information?

In short, the interaction would be negative for both clinicians and patients, particularly with respect to state laws that restrict the sharing of information. Many covered entities and their risk management teams already misunderstand how HIPAA permits information sharing. Changing the law again would significantly increase confusion in an already complex web of privacy laws.

(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 entity’s professional judgment as to the best interest of the patient, based on the good faith of the entity, or some other standard?

We support OCR's goal of encouraging and incentivizing covered entities to share information, but oppose requiring it. If OCR proposes to require covered entities to share PHI with other covered entities, it should create a safe harbor that ensures that a covered entity will not be subject to HIPAA enforcement penalties when acting in good faith.

(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?

OCR should not take action on the issues discussed in this RFI until ONC's and CMS' forthcoming information blocking rules are finalized. In fact, we are perplexed as to why OCR chose to issue this RFI at this time. As noted above, both rules will inform OCR's and stakeholders' thinking about potential privacy rule revisions, and provisions in those rules are clearly intertwined with the questions asked here. Notwithstanding those concerns, some covered entities (along with their compliance officers, risk managers, and counsel) tend to misapply HIPAA for fear of violating the law and its regulations. As such, they may refrain from sharing information and be accused of information blocking. We suggest that OCR establish a method of quickly evaluating such disputes.

The AMA also urges consistency across HHS as the agency sets policy to promote information sharing and prevent information blocking. For example, there is a discrepancy between the electronic patient information that is made available via the EHR (the common clinical data set, or CCDS) versus the information contained in a patient's designated record set. **Particularly in light of MyHealthEData, many patients will likely believe that EHRs using application programming interfaces (APIs) will provide a "spigot" of data, enabling a free flow of all their information. This is not the case.** To receive his or her entire medical record in an electronic format, a patient will likely still be given a CD or USB drive because APIs may not provide access to all of the information contained in an entire medical record. Physicians have little to no control over data availability in EHRs; this is directly controlled by the EHR vendor. Furthermore, not all EHRs will be able to support any given app. If a patient has an app he or she would like to use, the physician's EHR may not support it, and the physician will have very little leverage against the vendor.

Because of the limitations of the API functionality, agencies across HHS must manage expectations about what information a patient can actually access through an EHR app or patient portal. OCR should take this into account. Guidance is also necessary to clarify that physicians are not information blocking if patients cannot access their entire medical record through a mobile app/patient portal and cannot receive their entire medical record in a format of their choosing (e.g., an app). In sum, federal regulation and policy must balance patient data access with the limitations placed on physicians and patients by the design and development of health IT.

(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?

The AMA does not want OCR to expand the minimum necessary standard for claims management, review of health care services for appropriateness of care, utilization reviews, or formulary development. The Meaningful Use program illustrated that when requirements to exchange data exist, but without minimum necessary standards strongly in place, then the sending health care organization will send everything to ensure they comply with the requirement to exchange. Since semantic interoperability does not yet exist, this becomes an enormous burden on the receiving physician to wade through all the information to find clinically relevant information.

Minimum necessary controls must also be established given the emerging capability of technology to extract bulk data (i.e., the electronic collection of data composed of information from multiple records) out of an EHR. The AMA recognizes the potential benefits of bulk data access for public and population health and quality improvement. Reducing the difficulties inherent in accessing medical information at the individual or population health level is an important goal; however, we have concerns with the potential pitfalls of entities having unprecedented access to patient information. **We urge HHS to take a methodical approach and ensure the physician and patient communities are well-informed and agree with efforts to advance data access at this scale.** Access must be provided for a given purpose and consistent with the minimum necessary standard. Current data request processes, while limiting, are narrowly scoped for specific use cases and involve some level of “gating” that helps prevent improper use and disclosure and helps enforce compliance on both ends of the transaction (collection [query] and disclosure).

While standards like Fast Healthcare Interoperability Resources (FHIR) may support data controls like segmentation, we are concerned those controls are an afterthought in FHIR-based API design and will become a “bolt-on” function—drastically increasing their costs and limiting their usefulness. The AMA has been told that FHIR developer efforts are first focused on “just making the technology work” and that “patient data protections and privacy controls are outside their scope.” The downstream consequences of this approach will negatively impact physicians and patients. Mechanisms to monitor and control data access, patient consent and privacy, and ensure data provenance, governance, and enforce state and federal law must be inherent in FHIR development.

We strongly recommend that OCR consider all ramifications of bulk data access in the context of minimum necessary, including privacy and security of an individual’s electronic health information. Existing standards such as Consent2Share and Data Segmentation for Privacy (DS4P) are not being utilized due to cost, maturity, or lack of adoption. Clearly, increasing ease of access to data is an imperative; however, the agency must also consider the need to hold entities accountable, including assuring that covered entities can comply with HIPAA’s minimum necessary obligations.

(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? 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?

We applaud OCR's recognition that certain individuals can benefit from social service agencies and community-based support programs. Covered entities may already share PHI, even without a patient's consent, with non-covered entity health care providers (including for care coordination purposes). Conversely, covered entities must obtain a patient's authorization before sharing PHI with non-health care providers (which are, by default, non-covered entities), or must sign a BAA. As noted above, patients should have the ability to control the flow of their data outside of the health care system, particularly for purposes beyond treatment. Modifying this aspect of the Privacy Rule (i.e., permitting covered entities to disclose PHI to a non-health care provider without a patient's authorization or BAA) would create a slippery slope for health data privacy. It would likely prove difficult to determine what non-health care providers are entitled to receive PHI without authorization or BAA and could chip away at the framework that exists to protect patients' privacy.

Notwithstanding the above, the AMA recognizes that these social service and community-based support programs often provide significant assistance to individuals who may not otherwise receive it and understands why access to a patient's PHI can be beneficial to an individual particularly in the case of homelessness, limited access to health care services, or patients receiving multiple supports across a spectrum of services. Physicians often struggle with how to best care for these patients without violating HIPAA. Unfortunately fear of OCR enforcement can complicate care coordination efforts when care coordination involves activities beyond health care.

As discussed further below, HIPAA permits physicians to disclose information to caregivers, family, and friends involved in an individual's care if the patient is given an opportunity to object and does not, or if the patient is incapacitated, if, in the physician's best judgment, such disclosure is in the patient's best interest. We do not believe that OCR would impose fines on physicians who, in good faith and in accordance with these rules, disclose PHI to optimize a patient's health. **To help covered entities feel more comfortable with making such judgments—especially considering their fear of OCR enforcement—OCR could explore options for data sharing agreements between covered entities and social service programs in their patients' communities that aim to reduce friction while still maintaining patient privacy.** Information sharing concepts are explored in an issue brief by the National Center for Medical-Legal Partnership, housed within the Milken Institute School of Public Health at the George Washington University.⁹

(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 enforcement official, given the potential to place individuals at legal risk? Should a permission apply to multidisciplinary teams that include law enforcement officials only if such teams are established through a drug court program? Should such a multidisciplinary team be required to enter into a business associate (or similar)

⁹ *Information Sharing in Medical-Legal Partnerships: Foundational Concepts and Resources*, available at <https://medical-legalpartnership.org/wp-content/uploads/2017/07/Information-Sharing-in-MLPs.pdf>.

agreement with the covered entity? What safeguards are essential to preserving individuals' privacy in this context?

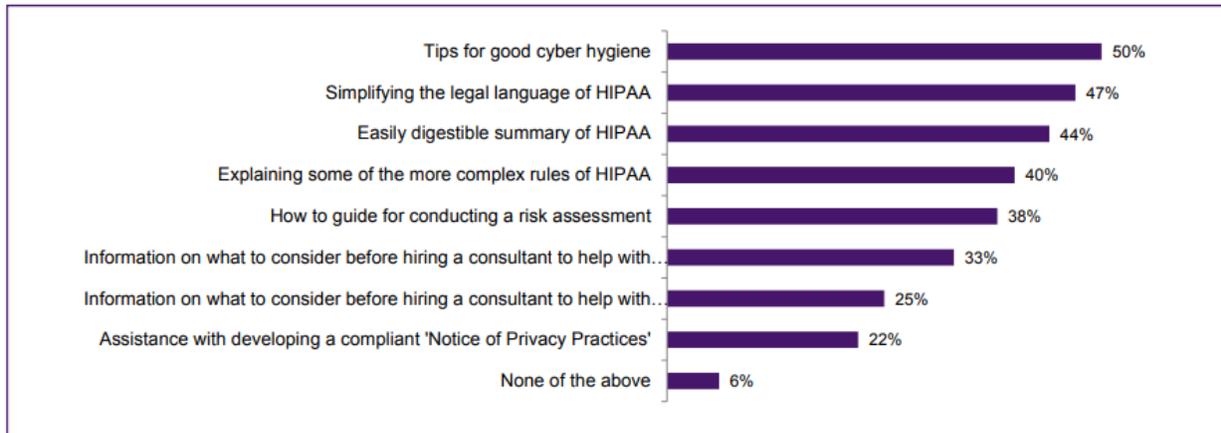
The AMA is strongly opposed to any privacy rule permitting law enforcement agencies access to medical records or individually identifiable health information, including PHI, (except for any discretionary or mandatory disclosures made by physicians and other health care providers pursuant to ethical guidelines or to comply with applicable state or federal reporting laws) without the express written consent of the patient, or a court order or warrant permitting such access. Any requesting law enforcement entity should be allowed access to medical records only through a court order. Our position is that a strong legal standard, accompanied by a set of parameters on need and use, is essential to protecting not only personal medical information, but also the confidence of individuals in their government.

This is not an abstract concern. Physicians and their patients have repeatedly experienced the intrusion of law enforcement into patients' personal medical information when no need for identifiable information is established and no protections are provided. The unfortunate result is less—rather than greater—confidence in the law enforcement and judicial systems of this country.

(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?

The graph below shows physician responses to a question in the AMA Survey that asked, “Which of the following would enable you to feel more confident that you are keeping your practice secure?”¹⁰ While the question focused on security, we believe the results are also applicable to privacy. Four out of the top five responses concern HIPAA, and three of the five explicitly ask for simplified, digestible, and uncomplex explanations of HIPAA.

¹⁰ *Taking the Physician's Pulse, Tackling Cyber Threats in Healthcare*, available at <https://www.ama-assn.org/sites/ama-assn.org/files/corp/media-browser/public/government/advocacy/medical-cybersecurity-findings.pdf>. Please note that formatting issues prevent options sixth and seventh from the top in the graph to look identical. Their full responses are, “Information on what to consider before hiring a consultant to help with cybersecurity,” and “Information on what to consider before hiring a consultant to help with HIPAA compliance,” respectively.



Base: n=1,300; Q21: Which of the following would enable you to feel more confident that you are keeping your practice secure? (multiple responses)

Additional guidance on federal privacy requirements (both HIPAA and 42 CFR Part 2 (Part 2)) would greatly help to advance the goal of promoting greater electronic information exchange, which has the potential to greatly improve care coordination while maintaining patient confidentiality. Unfortunately, guidance developed to date does not seem to make its way to its intended audience. Many physicians contact the AMA months or even years after guidance is released asking questions about privacy laws. As such, health care providers frequently report that privacy laws inhibit their ability to exchange information even when such laws, in fact, do permit information sharing. Indeed, we encounter many industry stakeholders beyond health care providers who misunderstand privacy laws and thus perpetuate confusion about how such laws permit information sharing. Finally, certain guidance focuses on overly simplistic use cases. Physicians need and want guidance that helps them navigate the “grey areas” of privacy law, such as whether HIPAA permits text messaging, how to distinguish between patient-directed third-party access to protected health information and a third-party access request for information, and even distinctions between how to share mental health information generated by a general medical facility versus (SUD) information generated in a Part 2 facility. As such, we urge OCR to strategize around ways to ensure physicians, patients, and other health care industry stakeholders are alerted to new and existing guidance that contains answers to common, real-world clinical scenarios. The AMA would like to work with OCR to amplify its educational efforts.

(21) Are there provisions of the HIPAA Rules that work well, generally or in specific circumstances, to facilitate care coordination and/or case management? If so, please provide information about how such provisions facilitate care coordination and/or case management. In addition, could the aspects of these provisions that facilitate such activities be applied to provisions that are not working as well?

The AMA appreciates that HIPAA permits physicians to make certain disclosures according to their best judgment (e.g., when a patient is incapacitated or when there is a serious and imminent threat of harm to health). We also applaud OCR’s explicit assurance to physicians that the agency “[will] not second guess

a health professional’s judgment about when a patient seriously and imminently threatens their own, or others, health or safety.”¹¹

Similarly, we appreciate that HIPAA disclosures are generally permissive, not mandatory. Thus, to the extent physicians feel constrained by the professional ethical obligations of their specialty, etc., HIPAA does not require them to disclose information in perceived non-conformance with these obligations.

b. Promoting Parental and Caregiver Involvement and Addressing the Opioid Crisis and Serious Mental Illness

A widespread perception exists that HIPAA prevents physicians from sharing information—especially related to behavioral health and SUD—with families and caretakers. This is not true. The HIPAA Privacy Rule does not prohibit communication with a patient’s family members (not only parents), friends, or others involved in the patient’s care. The HIPAA Privacy Rule never prohibits physicians from listening to family members or other caregivers who may have concerns about the health and well-being of the patient, so the physician can factor that information into the patient’s care. In fact, there is no record of OCR or the Department of Justice ever pursuing civil or criminal HIPAA enforcement against covered entities sharing information with family or caregivers to facilitate treatment or payment.

To be clear, in recognition of the integral role that family and friends play in a patient’s health care, the HIPAA Privacy Rule allows often routine—and sometimes critical—communications between health care providers and these persons.¹² OCR guidance helps to “translate” the regulations into understandable direction.¹³ Where a patient is present and has the capacity to make health care decisions, health care providers may communicate with a patient’s family members, friends, or other persons the patient has involved in his or her health care or payment for care, so long as the patient does not object. The provider may ask the patient’s permission to share relevant information with family members or others, may tell the patient he or she plans to discuss the information and give them an opportunity to agree or object, or may infer from the circumstances, using professional judgment, that the patient does not object. Where a patient is not present or is incapacitated, a health care provider may share the patient’s information with family, friends, or others involved in the patient’s care or payment for care, as long as the health care provider determines, based on professional judgment, that doing so is in the best interest of the patient.

We caution that attempting to define terms such as “serious mental illness,” “significantly diminished capacity,” “identified responsible caregiver,” etc., may tend to constrain rather than enhance physicians’ professional discretion. Similarly, additional regulation may create new standards and avenues for administrative review of physician decisions regarding when and how to communicate with patients’ family, friends, and caretakers.

¹¹ *HIPAA Helps Caregiving Connections—HIPAA helps mental health professionals to prevent harm*, available at <https://www.hhs.gov/sites/default/files/hipaa-helps-prevent-harm.pdf>

¹² 45 CFR § 164.510(b). See also *HIPAA Privacy Rule and Sharing Information Related to Mental Health*, available at <https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf>.

¹³ *Information Related to Mental and Behavioral Health, including Opioid Overdose*, available at <https://www.hhs.gov/hipaa/for-professionals/special-topics/mental-health/index.html>.

Additionally, we reiterate that state laws that are more stringent (i.e., more protective of patient privacy) trump the HIPAA Privacy Rule, such that many of the perceived information-sharing legal barriers (to the extent that they actually exist) are rooted in state law, not HIPAA (and would not be fixed by HIPAA changes).

We also have some concerns that this RFI may inadvertently perpetuate misunderstanding by raising questions about the permissibility of sharing information with family members and caregivers. Indeed, OCR has issued guidance addressing many of the topics below (referenced in each question), noting that “HIPAA Helps Caregiving Connections” with respect to behavioral health, serious mental illness, SUD, and opioid use disorder (emphasis added).

The AMA supports care coordination activities and the numerous benefits that can result from coordinated care. However, we would oppose efforts to eliminate the opportunity for a patient to object to such disclosures. OCR should be creating policy that empowers patients within the health care system, as opposed to limiting their autonomy and decision-making power. OCR should not regulate its way out of administrative inconvenience based on misunderstanding, particularly given the high stakes of patients needing to feel confident that their health information will remain private. Instead, it must find better ways to educate clinicians, risk management teams, and health care attorneys.

(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?

Changes to the Privacy Rule are not needed to help address the opioid epidemic. As OCR’s own guidance notes, “HIPAA regulations allow health professionals to share health information with a patient’s loved ones in emergency or dangerous situations – but misunderstandings to the contrary persist and create obstacles to family support that is crucial to the proper care and treatment of people experiencing a crisis situation, such as an opioid overdose.”¹⁴ The guidance further states, “health care providers have broad ability to share health information with patients’ family members during certain crisis situations without violating HIPAA privacy regulations.”¹⁵

In many cases, if a patient wants to share SUD information, he or she will tell the clinician where he or she has received treatment and the physician can obtain those records with the patient’s consent. If a patient does not want to share SUD information with his or her clinician (and given the current lack of interoperability among health IT systems), it is very unlikely that the clinician would be able to locate the patient electronically even if the law is changed. Further, if a clinician *is* able to locate the correct patient’s SUD record, the patient may not be aware of the clinician’s access to such information.

Surprising a patient with his or her SUD records when the patient has not provided consent for the clinician to receive them may erode trust in his or her relationship with his or her physicians.

¹⁴ *How HIPAA Allows Doctors to Respond to the Opioid Crisis*, available at <https://www.hhs.gov/sites/default/files/hipaa-opioid-crisis.pdf>.

¹⁵ *Id.*

While important work is being done to remove stigma and regard SUD as a medical issue like any other medical issue, the fact remains that “disclosure of SUD-related information can have serious consequences” and SUDs are “widely stigmatized.”¹⁶

We also highlight that most substance abuse is illegal, which is decidedly unlike any other medical issue.¹⁷ Additionally, while HIPAA indeed protects patient privacy, HIPAA breaches also occur all the time and are increasing every day.¹⁸ Increasing the exchange of SUD data heightens the risk of inappropriate disclosure of such data, the consequences of which could be exponentially more harmful to the patient than the improper disclosure of one’s hypertension (examples include loss of housing,¹⁹ loss of child custody,²⁰ discrimination from medical professionals,²¹ loss of benefits,²² or loss of employment,²³ among others²⁴). In fact, before enacting a law requiring that police and prosecutors obtain warrants before searching in sensitive patient information in the state’s prescription monitoring database, Massachusetts allowed police and prosecutors to view patient medical records without warrants nearly 11,000 times—or about 20 times per day—between August 2016 and March 2018.²⁵

The AMA understands and agrees with the goal of ensuring that physicians have a patient’s entire medical record to review and help them provide holistic care for their patients. The AMA encourages patients to consent to share SUD information to help clinicians provide coordinated and holistic care. However, we believe that to have truly coordinated care, patients must be willing and active participants. Patients who do not want their SUD information shared are the very patients who would likely be deterred from seeking treatment if they did not have control over how such information is shared.

¹⁶ *Medicaid and CHIP Payment and Access Commission’s (MACPAC) statement in its June 2018 Report to Congress on Substance Use Disorder Confidentiality in Regulation and Care Integration in Medicaid and CHIP (MACPAC Report)*, available at <https://www.macpac.gov/wp-content/uploads/2018/06/Substance-Use-Disorder-Confidentiality-Regulations-and-Care-Integration-in-Medicaid-and-CHIP.pdf>

¹⁷ “Police say people who overdose in one central Ohio community will now be charged with a criminal offense.” See <https://www.wkbn.com/ohio-news/overdose-victims-cited-in-one-ohio-city/1067863977>.

¹⁸ “2018 was a record-breaking year for healthcare data breaches,” available at <https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/>, stating,).

¹⁹ *Alcohol, Drug, and Criminal History Restrictions in Public Housing*; Marah A. Curtis, University of Wisconsin-Madison; Sarah Garlington, Boston University; Lisa S. Schottenfeld, Mathematica Policy Research; available at <https://www.huduser.gov/portal/periodicals/cityscpe/vol15num3/ch2.pdf>.

²⁰ *Parental drug use as Child Abuse*, Child Welfare Information Gateway, available at <https://www.childwelfare.gov/pubPDFs/drugexposed.pdf>.

²¹ *Stigma among health professionals towards patients with substance use disorders and its consequences for healthcare delivery: systematic review*; Drug Alcohol Depend. 2013 Jul 1;131(1-2):23-35; van Boekel LC1, Brouwers EP, van Weeghel J, Garretsen HF, available at <https://www.ncbi.nlm.nih.gov/pubmed/23490450>.

²² *Follow-up of Former Drug Addict and Alcoholic Beneficiaries*; Mikki D. Waid and Sherry L. Barber; Research and Statistics Note No. 2001-02, available at <https://www.ssa.gov/policy/docs/rsnotes/rsn2001-02.html>.

²³ *The Americans with Disabilities Act and “Current” Illegal Drug Use*, available at <https://corporate.findlaw.com/litigation-disputes/the-americans-with-disabilities-act-and-current-illegal-drug.html>.

²⁴ *Discrimination Against Patients With Substance Use Disorders Remains Prevalent And Harmful: The Case For 42 CFR Part 2*; Health Affairs; Karla Lopez; Deborah Reid; available at <https://www.healthaffairs.org/doi/10.1377/hblog20170413.059618/full/>.

²⁵ *Police in Massachusetts Must Get a Warrant to Access Patient Data*; American Civil Liberties Union Massachusetts; Kate Crockford; available at <https://www.aclum.org/en/publications/victory-police-massachusetts-must-now-get-warrant-access-sensitive-patient-data>.

Consequently, those patients would be kept out of the treatment system without even providing them a chance to better understand the benefits of holistic care coordination.

We agree with the Medicaid and CHIP Payment and Access Commission's (MACPAC) statement in its June 2018 Report to Congress on Substance Use Disorder Confidentiality Regulation and Care Integration in Medicaid and CHIP (MACPAC Report) that "clarifying guidance on existing regulations... would be a meaningful step to help providers, payers, and patients understand rights and obligations under the current law as well as existing opportunities for information sharing."²⁶ This clarification should include regulations in Part 2 to clarify ways in which clinicians can share data covered by Part 2 without need for additional written patient consent. **Additionally, the AMA believes that there are workable solutions to electronically track patient consent through EHRs that would be more effective in providing physicians with access to sensitive medical records while maintaining robust patient privacy protections** (see more on data segmentation below).

(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?

We appreciate OCR's multiple guidances on this topic, as we have heard from clinicians who do not understand that they are permitted to share behavioral health information in the same way that they are able to share other PHI.²⁷ As OCR notes:

HIPAA permits health care providers to disclose to other health providers any PHI contained in the medical record about an individual for treatment, case management, and coordination of care and, with few exceptions (i.e., psychotherapy notes maintained separately from the medical record), treats mental health information the same as other health information. Some examples of the types of mental health information that may be found in the medical record and are subject to the same HIPAA standards as other protected health information include:

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

²⁷ *HIPAA Helps Caregiving Connections—HIPAA helps mental health professionals to prevent harm*, available at <https://www.hhs.gov/sites/default/files/hipaa-helps-prevent-harm.pdf>; *HIPAA Helps Caregiving Connections—HIPAA helps family and friends stay connected with loved ones who have a substance use disorder, including opioid abuse, or a mental or behavioral health condition*, available at <https://www.hhs.gov/sites/default/files/hipaa-helps-stay-connected.pdf>; *When Your Child, Teenager, or Adult Son or Daughter has a Mental Illness or Substance Use Disorder, Including Opioid Addiction: What Parents Need to Know about HIPAA*, available at <https://www.hhs.gov/sites/default/files/when-your-child.pdf>; and *HIPAA Privacy Rule and Sharing Information Related to Mental Health*, available at <https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf>.

- medication prescription and monitoring;
- counseling session start and stop times;
- the modalities and frequencies of treatment furnished;
- results of clinical tests; and
- summaries of: diagnosis, functional status, treatment plan, symptoms, prognosis, and progress to date.

HIPAA generally does not limit disclosures of PHI between health care providers for treatment, case management, and care coordination, except that covered entities must obtain individuals' authorization to disclose separately maintained psychotherapy session notes for such purposes. There are no extra protections or barriers for mental health records (with the extremely limited exception of psychotherapy notes maintained separately from the mental health record).²⁸ (emphasis added)

We reiterate that lack of education is a central barrier to exchanging SMI information in accordance with how HIPAA currently permits. We support OCR's efforts to increase outreach to physicians on this topic and would like to assist the agency with such efforts.

Please see the answer to Question 22 for additional concerns that apply to disclosure of SMI as well as SUD.

(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.

We are not aware of any instances in which HIPAA (not state law) has prevented a parent from gaining access to their minor child's health information—SUD, behavioral health, or otherwise. To the extent that other stakeholders report such experiences, we question whether HIPAA was correctly applied/interpreted and would again highlight the need for increased education.

(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?

As described above, HIPAA permits covered entities to disclose PHI to family members—regardless of age—if, in the judgment of the physician, it is in the best interest of the patient and the patient does not object. This allows adult children, spouses, parents, and personal representatives to participate in an individual's care. With respect to minors, existing HIPAA provisions are adequate, as they allow states to make determinations about who can access a minor's medical record and provide minors with access to certain confidential services.

²⁸ *HIPAA Privacy Rule and Sharing Information Related to Mental Health*, available at <https://www.hhs.gov/sites/default/files/hipaa-privacy-rule-and-sharing-info-related-to-mental-health.pdf>.

Further, the AMA recognizes the importance of providing confidential care to adolescents is critical to improving their health and believes that while physicians should aim to involve parents in the care of their minor children, the physician should make determinations, in their best judgment, as to whether parental involvement or access to the minor's PHI would not be beneficial. Physicians should inform the minor patient's parent(s) or guardian, if present, in situations where such involvement is necessary to avert life- or health-threatening harm to the patient or others. Physicians should also encourage the minor patient to involve his or her parents and offer to facilitate conversation between the patient and the parents. In sum, federal and state law should support physicians and other health care professionals in their role in providing confidential health care to their adolescent patients while permitting physicians to inform parents about a minor's treatment if allowed by state law and if the minor (with decision-making capability) does not object.

c. Accounting of Disclosures

The AMA agrees with OCR's belief that the proposed access report requirement would create undue burden for covered entities without providing meaningful information to individuals. Thus, AMA supports OCR's intention to withdraw the 2011 Notice of Proposed Rule Making.

With the implementation of the HITECH Act requirement regarding the accounting of disclosures, the AMA believes that physicians and other HIPAA-covered entities should only be required to produce accounting of disclosures reports based off of information maintained in an EHR that has the functionality to readily produce reports that are not burdensome to create and are meaningful to patients. Physicians should not be required to produce information from other non-EHR systems that contain PHI including practice management and billing systems.

The AMA believes that OCR should exempt certain categories of disclosures that are subject to the accounting requirement including disclosures about victims of abuse, neglect, or domestic violence; disclosures for health oversight activities and disclosures that are required by law (including disclosures to HHS to enforce the HIPAA administrative simplification rules). Exempting these types of disclosures will help minimize the reporting burdens of physician practices, other covered entities, and their business associates.

Importantly, patient safety work product must be excluded from any accounting of disclosures. The Patient Safety and Quality Improvement Act of 2005 clearly indicated that the confidentiality and legal protections of patient safety work product must remain intact to encourage the voluntary reporting of patient safety events. Without legal and confidentiality protections, the goal of the act to advance culture, process, and system changes that ultimately enhance patient safety in the delivery of health care would unravel.

Physicians should have the option to furnish an accounting of disclosures reports on behalf of their business associates or the option to furnish an accounting of disclosures report limited to information from the physician's EHR and provide the patient with a list of the physician's business associates so that the patient can directly contact the business associates for a report.

Moreover, regardless of whether a covered entity can provide a full accounting disclosure or conduct an investigation, OCR should not require covered entities to provide individuals with the names of persons who received TPO disclosures. AMA has serious safety concerns over any requirement to identify the names of individuals who receive PHI (with the exception of solo practitioners). Disclosure of the name of the recipient could interfere with patient care or pose other potential harms to the patient, the recipient, or the physician practice.

d. Notice of Privacy Practices

The AMA supports eliminating or modifying the requirement for covered health care providers to make a good faith effort to obtain individuals' written acknowledgment of receipt of a provider's Notice of Privacy Practices (NPP). Requiring an organization to obtain acknowledgement of a NPP that is not comprehensible and does not provide meaningful choice or control for patients over their information does not promote privacy or the doctrine of confidentiality. AMA policy requires that confidentiality be protected and only allows the disclosure of information with a patient's authorization or when an objective analysis concludes that the benefits of disclosure outweigh risks to patients' privacy.

Removing the written acknowledgement requirement would reduce administrative burden by decreasing the amount of paperwork to print and store; it would also limit unneeded compliance monitoring. However, the AMA also believes that OCR should have appropriate safeguards to ensure that patients can access the information contained within an NPP as easily and clearly as possible. The level of detail included in describing uses and disclosures for health care operations should be adequate to alert the patient to the multiple categories for which their information is being used, particularly given that OCR has developed model NPPs. Patients generally enter a physician's office or a hospital believing that the information they provide is going to their individual care and benefit. Activities that use patients' information for marketing and other non-routine categories or for the benefit of a population or group should be explained with more specificity.

e. Additional Ways to Remove Regulatory Obstacles and Reduce Regulatory Burdens to Facilitate Care Coordination and Promote Value-Base[d] Health Care Transformation

(26) 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.

Remove the Presumption of Guilt

We reiterate that HIPAA is already tremendously complex for practicing physicians. Privacy and security safeguards should be effective, practical, flexible, and affordable to implement, and should not hinder the necessary flow of health information. The proposed solutions may add new layers of complexity, potentially exacerbating the tendency to adopt a presumption of non-disclosure out of fear of breach. One potential way to reduce this fear is for OCR to remove the presumption of guilt (i.e., breach) when unsecured PHI is inappropriately used or disclosed by covered entities and business associates. **The presumption of guilt on covered entities creates potentially unnecessary burden, stress, and compliance costs on physicians. Instead, HHS should base the duty to report a breach on a harm threshold.** An unauthorized use or disclosure of unsecured PHI should be reported only if the use or

disclosure poses some harm to the affected individual(s). OCR should also clearly indicate that a breach notification is not required when a covered entity performs a risk assessment and determines that there is minimal risk of harm due to an impermissible use or disclosure of unsecured PHI.

Prioritize Data Segmentation

At times, providers more tightly restrict the flow of data because of uncertainty about how the law applies to it. Fortunately, technology can assist physicians with increasing the flow of information while maintaining privacy and a patient's consent. To do so, information should be "tagged" to identify where the information originated, for what purposes it can be disclosed, and to whom. **This will still be critical regardless of whether and how OCR modifies HIPAA.** The need for data segmentation is important as data is increasingly generated outside of the clinical setting, and can help ease burden associated with using and disclosing multiple types of sensitive data such as SUD, HIV-status, genetic information, minors' health information, and reproductive health information. While we recognize that segmentation efforts do not seem to have been prioritized by developers, such technology currently exists, as recognized by ONC's Draft Report to Congress (Draft Report) on reducing regulatory and administrative burden relating to the use of health IT and EHRs:

"[With respect to difficulty implementing Part 2 and integrating such information into EHRs,] HHS has recognized these implementation challenges and encourages the use of health IT to help clinicians appropriately share sensitive information while complying with legal requirements and respecting patient privacy preferences. For example, technical standards exist for electronically tagging health information to indicate privacy considerations, including legal requirements, within a patient record or summary of care document within the EHR, and SAMHSA supports ONC's Data Segmentation for Privacy initiative [DS4P] to support clinicians sharing of health information in accordance with patient choices. These tags on data elements, segments, or whole documents can then be used by automated access control solutions to prevent unauthorized access to patient data."²⁹

ONC recommended in its Draft Report that HHS monitor, test, and support development of technical standards for data segmentation. We wholeheartedly agree with this recommendation, and strongly urge the administration to demonstrate its commitment to greater interoperability and privacy protections by prioritizing data segmentation in development, testing, and policy-making. We note that while technology exists to segregate data and software can help to electronically manage patient consent (e.g., Consent2Share), we have heard from physicians and health systems that such segregation functionality is costly to implement, and that open-source consent management software can be prohibitively expensive to incorporate into a customized EHR.

We urge the administration to recognize the pressing need for data segmentation to be made accessible and affordable to physicians. Such capabilities will enhance interoperability, strengthen the patient-physician relationship through a patient's increased confidence that a physician will not

²⁹ *Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs*, available at <https://www.healthit.gov/sites/default/files/page/2018-11/Draft%20Strategy%20on%20Reducing%20Regulatory%20and%20Administrative%20Burden%20Relating.pdf>, p. 44.

share data in a way that violates the patient’s trust, and improve care coordination and patient outcomes resulting from a physician’s ability to access sensitive information. Furthermore, such data segmentation capabilities would help to ease the burden stemming from physicians’ compliance with state privacy laws. Congress and HHS should reject the approach of legislating and regulating around these problems and instead focus on developing data segmentation standards and software, while ensuring that such technology is widely available and affordable.

Issue Guidance to Clarify the Use of Text Messaging

The AMA has received requests from physicians about using standard (SMS) text messages with patients. Speaking at the HIMSS Health IT conference in Las Vegas on March 6, 2018, the Director of OCR said that health care providers may share PHI with patients through text messaging, but covered entities and their risk managers are hesitant to do so in the absence of formal guidance from OCR. We appreciate previous guidance from OCR and ONC on the use of email, which increased understanding of how PHI can be transmitted electronically while still complying with HIPAA.³⁰ We encourage OCR to issue similar guidance specifically related to text messaging. Such guidance would help covered entities understand how they may or may not use text messaging in the course of patient care, including care coordination and communication with family and caregivers, and decrease fear of HIPAA violations leading to OCR enforcement.

Permit Multiple Paths to Security Rule Compliance

As noted above, “2018 was a record-breaking year for healthcare data breaches”³¹ and as health systems and other covered entities continue to amass enormous quantities of valuable health data using new health information technology, cyber attacks will continue to increase. In fact, the AMA Survey found that 83 percent of physician practices have experienced some form of cybersecurity attack and one out of two physicians surveyed are “very” or “extremely” concerned about future cyber attacks in their practice. In addition to potentially resulting in breaches, cyber attacks can have a significant impact on medical practices by causing service interruptions and downtime, adding operational expense, and posing risks to patient safety.

We appreciate the flexibility of the Security Rule’s requirements because physician practices are varied and have different security needs, resources, and skill levels. Many practices understand that they need robust plans to ensure their systems and patients are protected, yet struggle with conducting security risk analyses as outlined by HIPAA. **To best assist clinicians with implementing good security practices (also known as “cyber hygiene”), the AMA encourages OCR to help reframe the conversation around securing health information from punitive requirements (e.g., fines and penalties associated**

³⁰ *Does the HIPAA Privacy Rule permit health care providers to use e-mail to discuss health issues and treatment with their patients?*, available at <https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-health-care-providers-to-use-email-to-discuss-health-issues-with-patients/index.html>; *Does the Security Rule allow for sending electronic PHI (e-PHI) in an email or over the Internet? If so, what protections must be applied?*, available at <https://www.hhs.gov/hipaa/for-professionals/faq/2006/does-the-security-rule-allow-for-sending-electronic-phi-in-an-email/index.html>; and *Guide to Privacy and Security of Electronic Health Information*, available at <https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf>.

³¹ *Analysis of 2018 Healthcare Data Breaches*, available at <https://www.hipaajournal.com/analysis-of-healthcare-data-breaches/>.

with security failures) to developing positive incentives that encourage ways to bolster practice resilience and protect patient information.

One such incentive is to permit “multiple paths to compliance” with HIPAA’s Security Rule. OCR could revise 45 CFR §164.306(b) to include a new clause (i.e., 45 CFR §164.306(b)(3) stating that covered entities that adopt and implement a security framework (such as the NIST Cybersecurity Framework) or take steps toward applying the Health Industry Cybersecurity Practices³² (the primary publication of the Cybersecurity Act of 2015, Section 405(d) Task Group) are in compliance with the Security Rule. This modification would help make cybersecurity more understandable and attainable to physicians, particularly those that are most vulnerable due to lack of resources and expertise. The whole health care system—including patients—benefits when PHI is kept private and secure. The NIST Cybersecurity Framework and the Health Industry Cybersecurity Practices best practices utilize industry experts to identify the most pressing risks and develop safeguards to help to address these risks. OCR’s adoption of this change would empower physicians who think cybersecurity is an insurmountable task and may not even try to recognize that good cyber hygiene is within their reach.

Conclusion

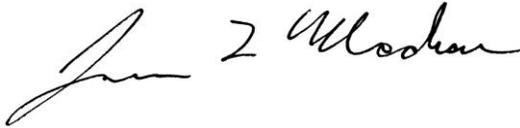
We applaud OCR’s efforts to promote the goals of value-based care and care coordination while preserving and protecting the privacy and security of a patient’s health information. Patient trust in the health care system can only be assured when all entities that maintain a patient’s health information have an obligation to maintain the confidentiality of that information and when patients truly have autonomy and control over decisions to disclose or retain their personal information. Thus, if a clearinghouse, payer, or other health care provider is performing a function on behalf of a covered entity, they should be considered a business associate and be required to enter into a BAA. Furthermore, the AMA **strongly** opposes any mandate or requirement to disclose PHI to another covered entity for any purpose. If OCR insists on mandated disclosure of PHI for any purpose, it should only be among health care providers and for treatment purposes, except where such disclosures would conflict with a patient’s right to privacy. Such disclosures are easy for patients and clinicians to understand; any additional caveats would create a web of regulatory requirements, which would profoundly confuse all parties.

³² *Health Industry Cybersecurity Practices*, available at <https://www.phe.gov/Preparedness/planning/405d/Pages/hic-practices.aspx>. By way of background, in 2015, Congress passed the Cybersecurity Act of 2015 (CSA), which includes Section 405(d), Aligning Health Care Industry Security Approaches. In 2017, HHS convened the CSA 405(d) Task Group, leveraging the Healthcare and Public Health (HPH) Sector Critical Infrastructure Security and Resilience Public-Private Partnership. The Task Group is comprised of a diverse set of over 100 members representing many areas and roles, including cybersecurity, privacy, healthcare practitioners, Health IT organizations, and other subject matter experts. The Health Industry Cybersecurity Practices they developed aim to raise awareness, provide vetted cybersecurity practices, and move organizations towards consistency in mitigating the current most pertinent cybersecurity threats to the sector. The publication seeks to aid healthcare and public health organizations to develop meaningful cybersecurity objectives and outcomes.

Roger Severino
February 8, 2019
Page 29

We again thank OCR for the opportunity to respond to this RFI. If you have any questions or wish to discuss our comments further, please contact Laura Hoffman, Assistant Director, Federal Affairs, at laura.hoffman@ama-assn.org.

Sincerely,

A handwritten signature in black ink, appearing to read "James L. Madara". The signature is written in a cursive style with a large initial "J" and a stylized "M".

James L. Madara, MD