EHRA

HIMSS Electronic Health Record Association

33 W Monroe, Suite 1700
Chicago, IL 60603
swillis@ehra.org
Phone: 312-915-9518
Twitter: @EHRAssociation

February 8, 2019

Roger Severino
Director, Office for Civil Rights (OCR)
U.S. Department of Health & Human Services
200 Independence Avenue, SW
Washington, DC 20201

Dear Mr. Severino,

On behalf of the Electronic Health Record (EHR) Association, we welcome the opportunity to share our comments regarding the Office for Civil Rights' Request for Information on Modifying HIPAA Rules To Improve Coordinated Care, which was published in the *Federal Register* on December 14, 2018.

EHR Association members serve the vast majority of hospitals and ambulatory care organizations that use EHRs and other health information and technology to deliver high quality, efficient care to their patients. The Association operates on the premise that the rapid, widespread adoption of health IT has and will continue to help improve the quality of patient care as well as the productivity and sustainability of the healthcare system.

The EHR Association welcomes changes to HIPAA and HITECH that remove regulatory barriers to the sharing of protected health information (PHI) to improve interoperability while maintaining the privacy and security of patient data.

However, we believe that HIPAA and HITECH should remain the floor in governing minimum requirements for patient data sharing. In addition, we encourage OCR to harmonize approaches to patient data sharing with other jurisdictions, particularly states, to avoid unnecessary variations that create unintended barriers to sharing data across jurisdictions.

Our responses to this RFI are therefore geared to questions related to health IT, including:

- Removal of barriers to interoperability
- Concerns over policy changes that may require a health IT developer to implement features that compromise the privacy and security of patient data
- Concerns with policy changes that alter the scope of HIPAA away from the floor of patient data sharing

Our responses to specific questions within the RFI follow.

(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 EHR Association does not think that HIPAA should require disclosure of PHI to another covered entity upon their request without limitation under treatment, payment, or operations (TPO). We worry using HIPAA unconditionally in such a way would introduce unintended consequences. Rather, we believe that HIPAA should primarily focus on essential requirements and address clarifications and exceptions beyond the current base as needed explicitly.

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

The original covered entity should manage and direct the TPO disclosures of their PHI.

If a covered entity wishes their business associates to take on this burden, then this can be written into the business associate agreement itself and does not require additional regulation by HIPAA. This would be similar to the model for breach notification (HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414) where HHS guidance reads:

> *"With respect to a breach at or by a business associate, while the covered entity is ultimately responsible for ensuring individuals are notified, the covered entity may delegate the responsibility of providing individual notices to the business associate. Covered entities and business associates should consider which entity is in the best position to provide notice to the individual, which may depend on various circumstances, such as the functions the business associate performs on behalf of the covered entity and which entity has the relationship with the individual."*

Using the same model, the covered entity is ultimately responsible for disclosures, but covered entities may delegate the responsibility to business associates.

(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 non-covered health care provider. Should a HIPAA covered entity be required to disclose PHI to a non-covered health care provider with respect to any of the matters discussed in Questions 7 and 8? Would such a requirement create any unintended adverse consequences? For example, would a covered entity receiving the request want or need to set up a new administrative process to confirm the identity of the requester? Do the risks associated with disclosing PHI to health care providers not subject to HIPAA's privacy and security protections outweigh the benefit of sharing PHI among all of an individual's health care providers?

HIPAA-covered entities should not be required to disclose PHI to a healthcare provider not covered by HIPAA. For providers not covered by HIPAA there is no guarantee that the safeguards required by the HIPAA Security Rule and the HIPAA Privacy rule are in place. HIPAA should never require any disclosure to another provider that is not obligated to provide for the same privacy protections and security measures as HIPAA. Instead, disclosure of PHI to a healthcare provider who is not covered by HIPAA can be directed with patient consent, where the patient takes ownership of the risks.

(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?

HIPAA should remain a floor for providing PHI. As a floor, it is best to remain broadly applicable, rather than attempting to be granular about particular use cases.

In terms of timeliness, patients are offered a variety of ways to access their health information. Each of these types of access have evolved their own timeliness requirements, where appropriate. For example, the Promoting Interoperability program has included requirements that patients be able to "View, Download, or Transmit" the Common Clinical Data Set elements of their record in an EHR within a certain time range.

As there are many use cases for the disclosure of data, HIPAA should remain the floor for timeliness requirements, and such requirements for use case-specific disclosure should remain out of the scope of HIPAA. Instead, HIPAA should allow other policies, specific to a disclosure's use case, govern their own timeliness requirements.

In addition, we encourage OCR to harmonize approaches to patient data sharing with other jurisdictions, particularly states, to avoid unnecessary variations that create unintended barriers to sharing data across jurisdictions.

(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?

The EHR Association supports any policy changes that promote standardization of privacy and security policy between federal and state jurisdictions. We recommend OCR propose a national standard for sharing PHI, encourage states to align to established national standards, and educate states on the burden associated with differences between national and state policies on privacy and security.

(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?

Exchanging patient records inclusive of substance abuse disorder history or risk provides all relevant clinicians with additional insight to efficiently address the patient's challenges related to opioids and opiates. We suggest that OCR take steps, through modernization of HIPAA regulations, to improve patient care by allowing doctors to more easily exchange substance abuse records for the purposes of treatment, payment, or operations. Although not directly related to the Privacy Act itself, OCR can also play an important role in advocating for bipartisan legislation that would bring 42 CFR Part 2 in line with HIPAA Administrative Simplification provisions focused on privacy of health data.

Though identified substance abuse data would be most clinically relevant, the exchange of de-identified substance abuse records to other physicians is also useful in addressing the Opioid problem. However one method provided under HIPAA for de-identification, 164.514 (safe harbor), is outdated and not an appropriate method to de-identify sensitive data for the use case. If we had to recommend one of the two methods provided by HIPAA (Safe Harbor and Expert Determination), we recommend HIPAA's Expert Determination method. We do recognize that Expert Determination is also imperfect and is a logistical burden because an Expert must be hired. An Expert is vaguely defined by HIPAA, and de-identification by Expert Determination is inconsistent. Therefore, we strongly suggest that HIPAA should be modernized to include more current methods of de-identification other than just Safe Harbor and Expert Determination that can be prescriptively applied, noting that it would be a positive development for opioid-related care. In addition, for those who still wish to use Expert Determination, HIPAA should clarify who can be an "Expert" for Expert Determination with specific criteria.

EHRA is aware that sharing substance abuse records brings up patient concerns of losing control of their data. Allowing patients direct control of their records through Opt In/Out rules can address these concerns, however.

Furthermore, although some privacy advocates prefer “Opt In” as a default, we advocate “Opt Out” as a default to encourage the important goal of increasing data sharing and the data available to providers to address the Opioid epidemic. OCR can advocate for “Opt Out” by default and emphasize education of the public on their ability to Opt In / Opt Out as a means of addressing patient concerns about data exchange.

(31) Should the Department require covered entities to account for their business associates' disclosures for TPO, or should a covered entity be allowed to refer an individual to its business associate(s) to obtain this information? What benefits and burdens would covered entities and individuals experience under either of these options?

As stated in our response to question 7c, it would be simpler for the patient if only one entity, the covered entity with which they have a relationship, is the go-to entity for accounting of disclosures of a patient’s PHI. Not only is this easiest for the patient, but it is less challenging to business associates as the covered entity is already responsible for managing their business associates and who has what data. The patient should not be asked to become the manager of those relationships, while business associates may not have the full understanding of the patient’s context and data available elsewhere.

Another example of the difficulties OCR must consider is the burden associated with TPO disclosures, regardless of whether the disclosure is reported by the Covered Entity or a Business Associate.

To explain that difficulty, consider these examples. There are cases where categorizing disclosures as treatment, payment, or operations is straightforward due to circumstance. For instance, if the disclosure is a request from a payer for billing, then the circumstance likely identifies the disclosure is for payment.

However, there are many other cases where categorizing a disclosure is ambiguous. Consider, for example, a contracted professional is a Business Associate working as both a physician assistant at a clinic and also helps with medical billing and coding. If the professional is logged in and looking at a patient’s record, it is unknown if the disclosure is for treatment or for payment. In these ambiguous cases, if a requirement to account for all disclosures is put on a covered entity, then the burden of identifying the purpose of the disclosure will be put on the person entering the data (the professional). Even with proper training, this burden would adversely affect workflow of care providers and their staff and they still may not properly document the right type of disclosure.

Furthermore, due to the multitude of cases and volume of disclosures due to TPO for both covered entities and business associates, a full and correct accounting of all disclosures may be impossible.

(32)(a) For existing EHR systems: Is the system able to distinguish between “uses” and “disclosures” as those terms are defined under the Privacy Rule at <u>45 CFR 160.103</u>? (Note that the term “disclosure”

includes, but is not limited to, the sharing of information between a hospital and physicians who may have staff privileges but who are not members of its workforce).

EHR systems today do not distinguish between "uses" and "disclosures." To do so would requiring implementing the system with roles and/or conventions for user identification that distinguish "access/use" by business associate staff from employed staff. Since the distinction between these staff is often clinically irrelevant (consider a contracted provider versus a staff provider), maintaining such distinctions within an EHR is not common.

Some EHR systems may be able to distinguish or approximately distinguish between "uses" and "disclosures" by circumstance. However, EHRs are not able to distinguish in all cases. There are ambiguous cases where the person disclosing would need to interpret what type of disclosure they are making with additional documentation burden. Similar to the burden of identifying whether the disclosure is T., P., or O. (see 31) this burden may adversely affect workflow for medical staff and they still may not properly distinguish between "use" and "disclosure."

(32)(b) For existing EHR systems: If the existing system only records access to information without identifying whether such access represents a use or disclosure, what information is recorded about each instance of access? How long is such information retained? What would be the burden for covered entities to retain the information for three years? Once collected, what additional costs or other resources would be required to maintain the data for each subsequent year? At what point would retention of the information be excessively burdensome? OCR requests specific examples and cost estimates, where available.

For what information is recorded about accesses, we refer OCR to ASTM e2147-18, "Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems." In addition, minimal fields from 2015 certification would be:

- Date/time
- User ID
- Patient ID
- Type of action (with "pointer" for change/delete actions)
- Type of data accessed

(32)(c) For existing EHR systems: If the system is able to distinguish between uses and disclosures of information, what details regarding each disclosure are automatically collected by the system (i.e., collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the disclosure or accessing the information?

See response to question 32a -- EHR systems today are not able to distinguish between uses and disclosures.

For what information is captured automatically versus manually, the data identified in our response to question 32b are captured automatically. Generally, basic details from the ASTM e2147-18 standard and the recipient info are automatically collected, whereas attributes such as the purpose of the disclosure may or may not be manually recorded.

(32)(d) For existing EHR systems: If the system is able to distinguish between uses and disclosures of information, what data elements are automatically collected by the system for uses (i.e., collected without requiring any additional manual input by the person making the disclosure)? What information, if any, is manually entered by the person making the use?

See responses to 32b and 32c.

(32)(e) For existing EHR systems: If the system is able to distinguish between uses and disclosures of information, does it record a description of disclosures in a standardized manner (for example, does the system offer or require a user to select from a limited list of types of disclosures)? If yes, is the feature being utilized? What are the benefits and drawbacks?

Some EHRs may have standard lists of disclosures, but this is dependent on the functionality of the EHR platform (see response to question 32c). A limited list of types of disclosures may facilitate documentation but would require regular revision to account for emergent types of disclosures. However, we urge caution in advocating for predefined list types that are too granular, as too much granularity will be a burden on providers.

(32)(g) For existing EHR systems: Do existing EHR systems automatically generate an accounting of disclosures under the current Privacy Rule (i.e., does the system account for disclosures other than to carry out TPO)? If so, what would be the additional burden to also account for disclosures to carry out TPO? If not, to what extent do covered entities use a separate system or module to generate an accounting of disclosures, and does the system interface with the EHR system? OCR requests cost estimates, where available.

Though some EHR systems automatically generate an accounting of disclosures, others may not have this functionality. However, accounting for all TPO disclosures would be large burden and may be impossible (see responses to questions 31 and 32a).
Thus, a useful cost estimate is not possible. However, we anticipate it would be very expensive for EHR developers to implement features to support tracking and reporting of TPO disclosures.

In addition, the ongoing administrative and management cost for accounting of all TPO disclosures may be an equally large, if not unrealistic, task for a healthcare organization and its staff.

(33) If an EHR is not currently able to account for disclosures of an EHR to carry out TPO, what would be the burden, in time and financial costs, for covered entities and/or their vendors to implement such a feature?

See response to 32g.

(34) For covered entities already planning to adopt new EHRs, to what extent would a requirement to track TPO disclosures affect the cost of the new system?

As discussed earlier, accurately estimating the cost of accounting for all disclosures for TPO is not possible (see responses to questions 31 and 32g). We anticipate the cost would be high.

Even if such EHR features were available, the ongoing administrative and management requirements of accounting for all TPO disclosures may be an equally large, if not unrealistic task, for a healthcare organization and its staff.

(37) What data elements should be provided in an accounting of TPO disclosures, and why? How important is it to individuals to know the specific purpose of a disclosure —i.e., would it be sufficient to describe the purpose generally (e.g., for "for treatment," "for payment," or "for health care operations purposes"), or is more detail necessary for the accounting to be of value? To what extent are individuals familiar with the range of activities that constitute "health care operations?" On what basis do commenters make this assessment?

Providing disclosure purposes is a burden on clinicians and other staff; and, the more granular the purpose must be, the greater the burden. As discussed before (see response to question 31), not all purposes are able to be assumed by a software system. At the point of care, having clinicians or staff members decide and document the purpose for a disclosure at the TPO level would already be a burden, especially for ambiguous scenarios. To introduce more complexity into the clinician and staff workflow by having them distinguish between disclosure purposes more granular than TPO would be even more burdensome. In addition, the interruption in the clinician workflow in order to document the purpose of disclosure would adversely affect the usability of an EHR.

(41) The HITECH Act section 13405(c) only requires the accounting of disclosures for TPO to include disclosures through an EHR. In its rulemaking, should OCR likewise limit the right to obtain an accounting of disclosures for TPO to PHI maintained in, or disclosed through, an EHR? Why or why not? What are the benefits and drawbacks of including TPO disclosures made through paper records or made by some other means such as orally? Would differential treatment between PHI maintained in other media and PHI maintained electronically in EHRs (where only EHR related accounting of disclosures would be required) disincentivize the adoption of, or the conversion to, EHRs?

For consistency, and in order to avoid inadvertently incentivizing paper records, the accounting of disclosures should apply to all health information management systems including paper, EHRs, and other health IT.

(42) Please provide any other information that OCR should consider when developing a proposed rule on accounting for disclosures for TPO.

The considerations that made accounting of disclosures for treatment, payment, and operations challenging in 2011 have not changed and remain the same challenges the industry faces today. Any new requirements to disclosures for TPO outside of the current requirements will be an undue burden to both covered entities and business associates. This is especially true in ambiguous scenarios, as they will be left to interpretation and likely reported inconsistently, thus calling into question the value of the reported data.

Thank you for this opportunity to share our views and expertise.

Sincerely,

Cherie Holmes-Hy

Cherie Holmes-Henry
Chair, EHR Association
NextGen Healthcare

Sasha TerMaat

Sasha TerMaat
Vice Chair, EHR Association
Epic

HIMSS EHR Association Executive Committee

Dal J Bucciferro

David J. Bucciferro
Foothold Technology

Hans J. Buitendijk
Cerner Corporation

Barbara Hobbs

Barbara Hobbs
MEDITECH, Inc.

Rick Reeves, RPh
Evident

Emily Richmond

Emily Richmond, MPH
Practice Fusion

Courtney E Tesvich

Courtney E. Tesvich, RN
Nextech

About the EHR Association

Established in 2004, the Electronic Health Record (EHR) Association is comprised of more than 30 companies that supply the vast majority of EHRs to physicians' practices and hospitals across the United States. The EHR Association operates on the premise that the rapid, widespread adoption of EHRs will help improve the quality of patient care as well as the productivity and sustainability of the healthcare system as a key enabler of healthcare transformation. The EHR Association and its members are committed to supporting safe healthcare delivery, fostering continued innovation, and operating with high integrity in the market for our users and their patients and families.

The EHR Association is a partner of HIMSS. For more information, visit www.ehra.org.