American College of Physicians
Leading Internal Medicine, Improving Lives

May 3, 2021

Dr. Robinsue Frohboese, Acting Director and Principal Deputy
U.S. Department of Health and Human Services
Office for Civil Rights
200 Independence Avenue, SW
Washington, DC 20201

Dear Director Frohboese:

On behalf of the American College of Physicians (ACP), I am pleased to share our comments on the Office for Civil Rights' (OCR) *Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement*. The College is the largest medical specialty organization and the second-largest physician group in the United States. ACP members include 163,000 internal medicine physicians (internists), related subspecialties, and medical students. Internal medicine physicians are specialists who apply scientific knowledge and clinical expertise to the diagnosis, treatment, and compassionate care of adults across the spectrum from health to complex illness.

ACP appreciates OCR's efforts to help expand individuals' rights to access their own digital health information, enhance the process of information-sharing, and improve case management across the entire care continuum. The ongoing COVID-19 pandemic has demonstrated a persistent inability to access and exchange individual health information, including the ability for families and caregivers to better interact with important information related to an individual's care. Yet while many of the proposed changes to the HIPAA Privacy Rule appear to be reasonable ways to facilitate the use and disclosure of protected health information (PHI), they will require significant overhauls in policies and procedures used by practices, extensive staff re-training, and present onerous implementation challenges. Furthermore, existing information exchange capabilities are lacking, and updates have been impeded by the ongoing COVID-19 pandemic. We anticipate confusion if physicians would be expected to tease out these proposals' misalignments with the Office of the National Coordinator for Health Information Technology's (ONC) Information Blocking rule and the Centers for Medicaid & Medicare Services' (CMS) regulations. Additionally, many of the proposals are too general to implement or test in real-world practices and would need to be accompanied with clear guidance on what is and is not required. Although the College agrees with the intent of these proposals, we believe these changes will not elicit *real* benefit until OCR properly accounts for and addresses the true pain points of health information access and exchange in practice and the patient community.

The following contains specific comment on OCR's proposed changes to the HIPAA Privacy Rule:

Definitions: "Electronic Health Record" And "Personal Health Application"

The College commends OCR for adding definitions for the terms electronic health record (EHR) and personal health application (PHA). With over 300,000 health apps available worldwide, and more than 200 being added every day[1], we recognize the hurdles presented in defining these terms. The increasing number of health apps and non-HIPAA covered entities accessing patient health data necessitates our need to clearly define these various mechanisms for storing and accessing PHI. **For this reason, ACP recommends OCR engage in additional discussions with the health care community before finalizing the proposed definitions of EHR and PHA.**

While the College understands the definition of EHR is essential to the proposed rule, it is currently too broad, internally inconsistent, and misaligned with other proposals and current regulations. **Since OCR proposed this definition under the assumption that only health care physicians have EHRs, ACP believes the definition of EHR should be reconsidered to account for non-physician entities that purchase and use EHRs.** There are additional health care industry participants that have access to or maintain EHRs (e.g., payers). As written, the definition allows for non-physicians, such as health plans, to create document repositories to record health data. If OCR seeks to finalize this inclusion, OCR should put forth a definition exclusive to the specific type of entity. Otherwise, physicians will end up managing medical records information that was not created by a medical professional – a burdensome task at a time when physicians are already overburdened, in part by the volumes of information they must now manage.

The proposed definition of EHR is also internally inconsistent under HIPAA. As included in the definition of EHR, OCR has proposed to define "health-related information on an individual" as covering the "same scope of information as the term 'individually identifiable health information'" (IIHI), which is defined at 45 CFR § 160.103. However, by aligning the definition with the broader IIHI instead of PHI – a subset of IIHI – this new definition expands the EHR to include education records covered by the Family Educational Rights and Privacy Act, adult student medical records, and employment records held by an employer. This is internally inconsistent with individual rights and covered entities obligations under HIPAA. It is also inconsistent within the proposed rule, as the newly expanded right to direct a physician to disclose a patient's medical records to a third party only applies to PHI contained in a designated record set and does not include the broader categories of data encompassed in IIHI. **The College recommends OCR resolve the internal inconsistency by aligning the definition of EHR with the scope of information captured in a designated record set.** If OCR were to make this change in the final rule, it would likely limit confusion and lessen administrative burden on physicians.

Another point of concern to the College is that the proposed definition of EHR does not align with terms and definitions already existing in the privacy and security landscape. The College

[1] *The Growing Value of Digital Health*, IQVIA Institute for Human Data Science, 2017.

fully supports the intent of the Cures Act to increase information sharing and improve patient care[2], and we feel that it is important to move the needle forward regarding interoperability. When viewed in totality, however, **the College believes it is counter to the interoperability policy goals to create many different defined data sets and presents a significant burden to physicians and other covered entities tasked with navigating this maze of terms.** If OCR's proposed definition were finalized, a practice's policy would need to account for: "electronic health records", as proposed; HIPAA's traditional "designated record set"; "electronic health information" as defined by ONC in the Information Blocking rule; and the Federal Trade Commissions' Breach Rule's "personal health record". With their varying circumstances and differing segmentations of data (or information) included, traversing this space is an almost impossible ask of physicians. To better facilitate implementation and compliance, **ACP reiterates its recommendation to collaborate with the health care system (and regulators) to better align the definitions used.**

Regarding the proposed definition of PHA, the College raises a number of the same concerns identified above. Notably, since PHAs are neither covered entities nor business associates under HIPAA, they are not subject to the privacy and security obligations of HIPAA. Yet, OCR's proposed rule could force disclosure of potentially all of the patient's medical records to a third-party application outside the protections of HIPAA. If finalized, this increased mandate for sharing with PHAs will put sensitive health information at risk – contrary to the interests of patients, physicians, and the broader health care community. In light of the considerations raised, **OCR should reconsider whether health apps should automatically be considered a "business associate" within the definition of PHA – and thereby subject to heightened privacy and security obligations. The College additionally recommends OCR collaborate with Congress to pass federal privacy and security legislation that appropriately accounts for the increasing role that non-HIPAA covered entities play in health care.**

Right To Inspect, And Form And Format Proposals

ACP supports OCR's proposed changes to facilitate a greater right of access for patients and their support teams. However, the health care system – inclusive of vendors and developers – does not currently have the infrastructure to support such sweeping changes. Even beyond the short-term challenges of social distancing and restricted access to facilities, the proposed right of inspection is not sound. **Though the College supports increased electronic access to health data, we urge OCR to further scrutinize these proposals for the possibility that they exacerbate the digital divide.** As digital health continues to outpace parallel efforts to resolve the root issue[3], the importance of this consideration cannot be understated. The nation's struggle to register older, less educated, and economically disadvantaged patients from Black, Indigenous, Latinx, and other communities for the COVID-19 vaccine is illustrative of this concern around the growing divide. Since these communities' lack reliable internet access, working computers, and have lower health literacy levels than their counterparts, the right of

[2] ACP Letter to ONC Regarding Information Blocking Dates and Health IT Certification Timelines (2020), American College of Physicians, 2020 Dec 4.

[3] *Digital Health Information Disparities in Older Adults: a Mixed Methods Study*, J Racial Ethn Health Disparities, 2021 Jan 7.

inspection (and its downstream effects) should be evaluated against these already-present disparities.

The College also encourages OCR to better account for the numerous privacy and security challenges presented by the right of inspection. Under the proposed right of inspection, a patient may, for example, capture a photograph of their PHI maintained in the physician's EHR. Yet, what happens if the patient accidently captures another individual's confidential information in the background of the photo? Perhaps one could contend the physician minimize other screens and/or not have other information near the 'inspection area' but trying to provide for this sort of access will be operationally complex for physicians and staff. Grey areas exist in common edge cases such as proxy access for adolescent patients' sensitive information or patients with limited English proficiency, as well. **ACP thereby encourages OCR to provide additional guidance on steps physicians may take to mitigate these issues – or reconsider the requirements of the proposed right in its entirety.**

In addition to the aforementioned hesitations, ACP echoes OCR's concern for individuals' privacy and security interests when using a PHA that receives PHI from a physician. Even so, **the College unequivocally opposes the idea that physicians should be required to inform an individual who requests that PHI be transmitted to the individual's PHA of the privacy and security risks of transmitting PHI to a non-HIPAA covered entity.** Physicians are not trained as information security officers; they do not have the knowledge or expertise to offer professional guidance to patients on third-party apps. While larger practices may have compliance/legal teams to address these issues, this is an impossible (and inappropriate) ask for small or independent practices who lack in such resources. PHAs raise significant privacy and security concerns when they access and store PHI. **ACP sees immense potential clinical value in PHAs, and greatly encourages OCR to issue guidance and education to support both individuals and physicians in use of PHAs and other third-party apps.**

Timeliness, And Time And Manner Proposals

While ACP supports the intent of the timeliness and time and manner proposals, we raise significant concern about the burden thereby pushed on physicians. If finalized, OCR's proposed 15 day "turn-around-time" would place new, substantial demands on physicians, staff, their business associates, and other covered entities. Another possible issue is that physicians may become dependent on their health IT vendor to supply the information requested, and thus not have full control on when that information will be available to patients. The proposed rule states "[t]he Department believes that entities can provide individuals access to their information within a time limit less than 30 days", referencing limited anecdotal evidence to support this belief (e.g., eight states currently require covered entities to provide records to patients in less than 30 days and covered entities operating in those states have been able to comply with those requirements)[4]. ACP believes the foundation for the proposed change is lacking; in fact, we believe attention would be better focused on supporting and ensuring

[4] *Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement*, Health and Human Services Department, Office for Civil Rights, 86 FR 9446, 6446, 2021 Jan 21.

compliance within the existing confines of HIPAA.[5] Though we understand OCR's desire to have records produced more quickly, **the College believes that there is insufficient evidence that the benefits from this change would outweigh its costs.**

The proposed production timelines also present challenges in the real-world as physicians will be tasked with understanding how OCR's proposals align in existing structures. For example, CMS' Merit-Based Incentive Payment System (MIPS) Promoting Interoperability (PI) program currently requires that physicians give access to electronic health information (EHI) within 4 days in order to receive a positive numerator.[6] OCR's 15-day proposal is inconsistent with MIPS' "timely access" requirement, and this poses a significant burden to physicians who must address the confusing messaging. There is a similar issue presented when the proposals are viewed in light of ONC's Information Blocking rule, which requires physicians give access to information "without delay".[7] **ACP strongly recommends OCR align production timelines across regulatory programs to ease the burden on physicians and limit confusion in practice.**

Furthermore, **even with OCR's proposed changes to the production timelines, the fact remains that timeliness will continue to be an issue (and present compliance challenges) so long as no comprehensive privacy and security legislation is passed at the federal level.** Since HIPAA does not preempt state law, physicians will still need to comply with any state law provisions that require access in fewer than the proposed 15 days – making for a messy entanglement of laws and regulations. For example, many physician practices extend through multiple jurisdictions, such as the Washington metropolitan area that encompasses the District of Columbia, and parts of Maryland and Virginia. Physicians have long been buried under burdensome regulatory requirements and should not continue to bear the brunt of proposed advancements. **ACP recommends OCR focus on reducing the regulatory and legal burdens within cross-jurisdictional areas.**

Directive To Third Parties Proposals

In conjunction with the right of access production timelines discussed, the tangled nature of the approach to third-party disclosures is problematic. As proposed, the third-party directive gives individuals the right to direct physicians to transmit an electronic copy of PHI in an EHR directly to a third party, within 15 days. Of foremost concern to the College is OCR's proposed provision that physicians honor oral requests to provide such access. Oral requests present an increased likelihood of data breaches due to possible miscommunications about how much PHI to share and with whom. For this reason, **oral requests alone are insufficient in promoting accuracy, and ACP recommends OCR finalize a requirement for information necessary to the exchange to be provided in writing.**

---

[5] *HIPAA Right of Access Survey*, Ciitizen, 2020.

[6] *Merit-Based Incentive Payment System (MIPS) Promoting Interoperability Performance Category Measure*, Centers for Medicare & Medicaid Services, 2020.

[7] *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program final rule*, Health and Human Services Department, Office of the National Coordinator for Health IT, 85 FR 25642, 25642 2020 May 1.

OCR has also proposed to require the same 15-day timeline as included in the right of access proposals. ACP appreciates the intent to speed up access, but the proposed timelines are not realistic and do not fully account for the differing circumstances of the exchange. Setting up a third-party app access and debugging the data exchange could take far longer than 15 days – and through possibly no fault of the practice. It is also likely that the practice will require additional information from the individual to complete the request. Patients often do not have the correct name of their former physician or know where they are located, which may result in processing delays. In this case, additional calls and requests will need to be made – taking time that would count against the proposed timeline. Physicians should not be penalized for attempts to ensure the accuracy of the contact. **Therefore, ACP recommends the proposed 15-day timeline not apply to third party directives, and encourages OCR to account in the final rule that any such timeline should not begin until the practice has all of the information it needs to complete the request. The College also urges OCR to provide further clarification on how the proposed timelines align with existing timeliness requirements in the Information Blocking rule – both in the third-party directive context and as previously discussed.**

With the numerous ways in which one may access or store data, the College commends OCR for taking on these very important challenges. While these distinctions may make sense in theory, practices cannot be expected to differentiate between when individuals are attempting to access their information using an app or services versus when that app or service is *actually* a third party. As proposed, this provision further aggravates privacy and security concerns around EHRs and patient data. It is equally as burdensome on practices who must now determine when a response may likely present privacy or security risks. **ACP recommends OCR provide additional clarification on the circumstances in which the directive request is employed, as well as make clearer the obligations of physicians in these circumstances.**

<u>Reducing Identification Verification Burden Proposals</u>

As stressed throughout our comments, ACP greatly appreciates OCR's attempts to reduce barriers to accessing health data. Provisions specific to this set of proposals will be most helpful to those patient populations who struggle with myriad authorization and verification processes employed in the past. However, the College remains concerned that the proposed "unreasonable" verification measures, particularly those requiring proof of identity, present significant challenges when an individual (or one's personal representative) requests access remotely. Since remote requests are the preferred approach during the pandemic – and will likely be the norm for the foreseeable future – **ACP encourages OCR to provide examples of acceptable identity verification approaches that will minimize burden on the request without creating the opportunity for fraud.**

While it may seem a straightforward matter, the issue of verification standards when a physician or plan submits an individual's access request to another physician or plan cannot be reduced down to just verification. Even before verification, requests must include sufficient identifiers and demographic data to ensure that the records supplied are the records of the requester. A physician must also determine that the record at issue truly belongs to the identified requestor. In these instances, it would be incredibly onerous for OCR to propose that physicians be required to verify the identity and authority of the requestor. **The College**

recommends OCR provide additional guidance on and exceptions to the "unreasonable" measures proposals.

Changes To "Minimum Necessary", "Health Care Operations"; And Application Of "Good Faith" Standard For Certain Disclosures Proposals

Case managers are a very important part of any treatment team, and ACP greatly appreciates OCR recognizing this and providing for proposals that treat case management and care coordination more like treatment activities. The College, generally, is supportive of OCR's proposals to this end.

While ACP is appreciative of OCR's proposed changes to the minimum necessary standard, we are cautious of its eventual effect. If finalized, *all* practices would be required to revise their minimum necessary policies under HIPAA; however, the College is struggling to see the true benefit of this. HIPAA's existing minimum necessary standard already provides covered entities with the flexibility to use the information that they need for a particular purpose, including case management and care coordination, so long as they do not use more than what they need. The proposed change will do very little to result in dramatic changes for case management and care coordination because covered entities will likely continue to use the information that they need for the stated purpose, but not more. **ACP recommends OCR provide greater juxtaposition in the final rule regarding our current standard and the proposed change – and how this may best be implemented in practice.**

The College also cautions against the potential for standards proposals to inadvertently create a new tension between physicians and their patients. OCR has proposed that changes to the minimum necessary standard would remove the disincentive to disclose and request PHI to support care coordination and case management based on the uncertainty about applicable permissions and fear of being subject to penalties for noncompliance resulting from such uncertainty. In the context of disclosures made to prevent harm or lessen threats of harm, ACP agrees that there are benefits to proposals that limit physician liability. **We caution OCR to consider, though, whether it has gone beyond what patients and physicians deem appropriate – and whether impediments within HIPAA are, in fact, relevant to the inhibiting achievement of those goals.** For example, OCR believes that physicians, in particular, do not share enough information because they are nervous about HIPAA penalties; however, we do not know if that is necessarily true. Perhaps it is not so much that physicians do not share information due to fear of penalties as much as it is that physicians simply do not think they should share under the circumstances. OCR should, therefore, consider whether it is necessary to take away what is essentially a right to object to these disclosures.

Thank you for considering our comments on the HIPAA Privacy Rule modifications. The College reiterates its support for and commends OCR's continued efforts to increase individual access to health data and better facilitate case management and care coordination. Though ACP appreciates the proposed changes, no number of modifications can counterbalance the need for expanded federal privacy and security legislation. If you have any questions or would like

additional information, please contact Dejaih Johnson, Analyst for Health IT Policy and Regulatory Affairs, at djohnson@acponline.org.

Sincerely,

Zeshan A. Rajput, MD, MBA, MS
Chair, Medical Informatics Committee
American College of Physicians