



May 6, 2021

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

Re: RIN 0945-AA00; Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement

Dear Acting Director Frohboese:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 133,500 family physicians and medical students across the country, I write in response to the [notice of proposed rulemaking](#) (NPRM) Health Insurance Portability and Accountability Act (HIPAA) privacy rule, as published in the January 21, 2021 version of the *Federal Register*.

The AAFP has long [supported](#) policies that improve patients access to their data, as well as the ability to share patients' health information across the care team, while also protecting patients' fundamental right to privacy and the patient-physician relationship.

The AAFP's [confidentiality](#) policy states the right to privacy is personal and fundamental. A confidential relationship between physician and patient is essential for the free flow of information necessary for sound medical care. Only in a setting of trust can a patient share the private feelings and personal history that enable the physician to comprehend fully, to diagnose logically, and to treat properly. Medical information may have legitimate purposes outside of the physician/patient relationship. However, patients and physicians must authorize release of any personally identifiable information to other parties. Any disclosure of medical record information should be limited to information necessary to accomplish the purpose for which disclosure is made.

The AAFP is also a staunch advocate for reducing administrative burden and removing unnecessary regulatory requirements that are placed on physicians and take their time away from providing patient care. The AAFP applauds the Office of Civil Rights (OCR) for prioritizing these principles in this NPRM.

We note that OCR proposes significant changes to the HIPAA Privacy Rule while the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare and Medicaid Services (CMS) are also implementing sweeping regulatory changes to improve patients' access to their health data and advance interoperability. These changes, as well as those proposed by OCR in this NPRM, will require family physicians to change their administrative workflows and invest in a variety of new technologies to ensure compliance. **We strongly encourage OCR to**

STRONG MEDICINE FOR AMERICA

President Ada Stewart, MD Columbia, SC	President-elect Sterling Ransone, MD Deltaville, VA	Board Chair Gary LeRoy, MD Dayton, OH	Directors James Eilzy, MD, <i>Washington, DC</i> Dennis Gingrich, MD, <i>Hershey, PA</i> Tochi Iroku-Malize, MD, <i>Bay Shore, NY</i> Andrew Carroll, MD, <i>Chandler, AZ</i> Steven Furr, MD, <i>Jackson, AL</i> Margot Savoy, MD, <i>Media, PA</i>	Jennifer Brull, MD, <i>Plainville, KS</i> Mary Campagnolo, MD, <i>Borderntown, NJ</i> Todd Shaffer, MD, <i>Lee's Summit, MO</i> Danielle Carter, MD (New Physician Member), <i>Jacksonville, FL</i> Anna Askari, MD (Resident Member), <i>Palm Desert, CA</i> Cynthia Ciccotelli (Student Member), <i>Yardley, PA</i>
Speaker Alan Schwartzstein, MD Oregon, WI	Vice Speaker Russell Kohl, MD Stilwell, KS	Executive Vice President R. Shawn Martin Leawood, KS		

coordinate closely with ONC and CMS to harmonize regulatory requirements related to information sharing and health information technology (IT).

Adding Definitions for Electronic Health Record or EHR and Personal Health Application

OCR proposes to define electronic health record (EHR) and seeks comment on the proposed definition. The AAFP is concerned that the proposed definition and use of the term EHR will be confusing for physicians and increase the burden associated with complying with HIPAA and other regulations. It is not clear how this definition of EHR aligns with electronic health information (EHI), which is used in information blocking and interoperability regulations to facilitate the sharing of information. **We recommend that ONC align the definitions of EHR and EHI and avoid creating an additional term to describe similar types of patient's health information.**

While we appreciate that OCR referred to the AAFP's own definition of EHR when developing this proposal, we note that our definition was not created for the purpose of determining what information should be shared with a patient or third-party, as OCR's proposed definition is. We are concerned that the proposed definition requires physician practices to share information that is not sharable with existing certified EHR technology (CEHRT). **The EHR definition should be a working definition that limits what must be shared to the types of data that are reasonably available and sharable using CEHRT. The definition should also align with the definition of a designated record set.** To this end, billing records should only be included in the definition if they are included in the designated record set.

OCR also seeks comment on the proposed interpretation of "health care clinicians and staff" as it relates to the proposed EHR definition. The AAFP supports using the term "clinician" instead of "provider" as it more accurately represents the role of physicians and other non-physician clinicians. We agree that staff should be incorporated into the definition, but OCR should clarify the difference between those staff who are required to protect PHI versus those that must support disclosure of information. To support patient confidentiality, the broadest definitions of staff should be used to mandate an action to protect PHI, while a narrower definition should be used when mandating an action to disclose or facilitate disclosure of PHI.

In the NPRM, OCR proposes and seeks comment on the proposed definition of personal health application (apps). The AAFP believes that apps can help improve patients' access to their health data but remain concerned with the lack of protections for individuals regarding how their information is used and shared. We also recognize apps are not regulated by HIPAA. We recommend that OCR increase protections for individual patients by encouraging app developers to improve transparency around the app's collection and use of an individual's information.

Strengthening the Access Right to Inspect and Obtain Copies of PHI

OCR proposes to add a new right that would enable individuals to take notes, videos, and photographs, and use other personal resources to view and capture PHI in a designated record set as part of their right to inspect the PHI in person. Physician practices would be required to provide this access without imposing a fee.

The AAFP supports patients' rights to inspect their health care record and agrees this should include taking pictures, videos, or notes. We do not support the proposal that restricts covered entities,

including physician practices, from imposing a fee for the right to inspect the health record. The AAFP has [previously](#) raised concerns related to the costs imposed by information blocking and other regulations that practices are required to incur and cannot be reimbursed for. Current CERHT does not have the functionality to establish a restriction to view only one individual's record. Therefore, in addition to providing a convenient place, the practice must also incur staffing costs for practice staff to navigate the EHR on behalf of the patient to ensure other patients' PHI is protected. Even if such a CEHRT functionality was available, the patient would likely not know how to navigate the EHR and therefore would still require the assistance of practice staff. For these reasons, we think it is reasonable for practices to charge a reasonable fee, particularly when the patient invokes this right outside of an active care encounter.

We also note that practices are likely to encounter other logistical challenges if this requirement is finalized as proposed. Many practices may not have dedicated space where a patient can take photographs or videos without intruding on the privacy of other patients. OCR should consider instead allowing physician practices to establish their own standard procedure for making PHI available to patients in person, instead of specifying the procedure in regulation.

Modifying the Implementation Requirements for Requests for Access and Timely Action in Response to Requests for Access

OCR proposes to expressly prohibit a covered entity from imposing unreasonable measures on an individual exercising the right of access that create a barrier or unreasonably delay the individual from obtaining access. The AAFP supports this proposal and we do not believe that OCR should require or prohibit the use of any specific measures that may be used to verify a patient's identity.

OCR proposes to shorten covered entities' required response time to no later than 15 calendar days (from the current 30 days) with the opportunity for an extension of no more than 15 calendar days (from the current 30-day extension). The AAFP agrees that covered entities should provide patients a copy of their PHI as soon as practicable and, in many instances, physician practices will be able to do so within 15 days. However, we are concerned that there will be circumstances where a practice is unable to fulfill the request for disclosure within the proposed timeline. For example, practices may struggle to retrieve old records and make them available to the patient should those records be near the time in which the covered entity would be legally able to destroy them. It may be also particularly challenging to accommodate a patient's request for their entire medical record within the proposed timeframe. We believe in this case 30 days may not be sufficient to make these available to the patient. We recommend that OCR develop an exception policy to provide practices the flexibility they will inevitably need to fulfill more burdensome requests.

OCR seeks comments on other time limits for covered entities to submit, or respond to, an individual's access request. **The AAFP opposes any time limits that are shorter than 15 calendar days.** We are concerned that various regulations apply different timelines for which physician practices must respond to patients' requests for information. We continue to believe that the Department should work to harmonize the various regulatory requirements imposed on physician practices, but this should not result in a shorter timeframe than 15 calendar days.

Addressing the Individual Access Right to Direct Copies of PHI to Third Parties

OCR proposes that covered health care providers would be required to respond to an individual's request to direct an electronic copy of PHI in an EHR to a third party designated by the individual when the request is "clear, conspicuous, and specific"—which may be orally or in writing (including electronically executed requests). The proposed requirement would replace the current requirement that a request to direct an electronic copy of PHI in an EHR be in writing, signed by the individual, and clearly identify the designated person and where to send the copy of the PHI.

The AAFP appreciates that the intent of this proposal is to make it easier for patients to orally request that a covered entity provide records access to another covered entity or third party. We agree that HIPAA should not mandate a written request by a patient to authorize a disclosure of their PHI, particularly to another covered entity, but we have concern with mandating that an oral request is sufficient to require a covered entity to disclose PHI to a third-party. We are concerned that simply requiring an oral request to disclose PHI to a third-party may not sufficiently protect patients' privacy. The AAFP is concerned that this would result in a variety of unintended consequences, ultimately eroding patients' privacy and exposing physician practices to additional security risks. For these reasons, we do not believe that OCR should require a physician practice or other covered entity to accept an oral-only authorization.

The AAFP instead recommends that OCR allow covered entities to have a standard process to authorize disclosure of PHI. Having a standard process will ensure that the right information for each request is captured by the covered entity, appropriately logged for tracking purposes, and completed in a timely manner without jeopardizing patient privacy or data security. For example, practices could implement a standard policy to require written authorization for the sharing of particularly sensitive information to non-covered entities, while allowing oral-only authorization for other types of disclosures. OCR should only require that the standard process is clearly defined and not allow the use of written authorization to unnecessarily prohibit disclosures. We believe that covered entities can have such standard processes and not place undue barriers to patient's authorizing disclosure of their PHI.

OCR seeks comment on whether a covered physician should be required to inform an individual who requests that PHI be transmitted to the individual's personal health application of the privacy and security risks of transmitting PHI to an entity that is not covered by the HIPAA Rules. We note that, if the exceptions to the minimum necessary standard are finalized as proposed, HHS is mandating that covered entity share PHI as authorized by the patient regardless of any privacy concerns that the covered entity holds. It seems that it is the responsibility of third-party application developers and HHS to notify the patient of the privacy and security risks of transmitted PHI outside of the protection of HIPAA. Family physicians will not be able to adequately determine the privacy and security risks for many of the applications that will be available in the market for patients. They are also not well equipped to explain the various risks of sharing information to patients. Therefore, the any notification would be generic and likely list the most serious of risks including nefarious actors. At most, a covered entity could link to a standard federal government web page that informs the patient of the privacy and security risks. **The AAFP strongly believes that this burden should not be on physicians or any other clinicians.**

OCR seeks comments on whether there are instances in which a covered entity can deny an individual's request for disclosure. As we stated earlier, we agree that there should not be a mandate by HIPAA to require a written authorization by the patient for PHI disclosure, but we believe that HIPAA should also not mandate a covered entity to accept an oral only authorization. Covered

entities should be allowed to have a standard process to collect authorization requests to ensure that the correct information is collected and that the request can be appropriately tracked to ensure a timely completion.

Covered entities should always be permitted to deny a request when the disclosure is prohibited by state or other law or when it conflicts with the patient's wishes regarding the privacy of their PHI. We are also concerned that, without the ability to charge reasonable fees or be permitted to deny disclosure requests, physician practices will be required to aggregate data on behalf of patients and be overrun with disclosure requests. **The AAFP strongly urges OCR to ensure that the costs, technical challenges, and administrative burdens associated with this proposal do not fall on physician practices.**

Adjusting Permitted Fees for Access to PHI and ePHI

OCR proposes to prohibit covered entities from charging fees for certain disclosures of electronic PHI and amend the fee structure for responding to requests to direct records to a third party. **The AAFP agrees that individuals should have access to their health information and that cost should not be a barrier to accessing this information. However, we oppose changes to the Privacy Rule to either prohibit or require covered entities to charge fees. Physician practices should be permitted to impose reasonable, cost-based fees when patients request copies of their medical records.** For many practices, fulfilling these requests is likely to take substantial staff time and could detract from patient care. Physician practices should be able to recoup these costs and guard against an overwhelming increase in administrative burdens associated with fulfilling these requests. The AAFP, like OCR, will continue to encourage covered entities that charge fees for copies of PHI to waive fees or provide flexibility in payment (such as delaying charges or accepting payment in installments, without delaying the provision of copies) for individuals who are unable to pay upfront due to an emergency or a lack of resources.

OCR proposes to require covered entities to post estimated fee schedules on their websites for access and for disclosures with an individual's valid authorization and, upon request, provide individualized estimates of fees for an individual's request for copies of PHI, and itemized bills for completed requests. The Department seeks comments on appropriate enforcement of this requirement. Though we are strong advocates for price transparency, the AAFP recommends against imposing these additional regulatory and administrative requirements on physician practices. Requiring physician practices to provide individualized estimates of fees each time a patient requests copies of PHI will increase the cost of fulfilling such requests and likely cause unnecessary delays. Further, the AAFP urges OCR not to create legal consequences associated with fee estimates.

Creating an Exception to the Minimum Necessary Standard for Disclosures for Individual-Level Care Coordination and Case Management

The minimum necessary standard requires covered entities to take reasonable steps to limit the use or disclosure of, and requests for, protected health information to the minimum necessary to accomplish the intended purpose. OCR proposes to add an express exception to the minimum necessary standard for disclosures to, or requests by, a health plan or covered health care provider for care coordination and case management. Family physicians provide extensive care coordination and management services and the AAFP recognizes the value of readily exchanging information in order to improve care coordination. This is a primary reason we have long advocated for

interoperability and the prohibition of information blocking. However, as we stated in our [comments](#) on OCR's HIPAA RFI, **the AAFP opposes additional exceptions to the minimum necessary standard, including for care management and coordination.**

We remain concerned that health plans 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. Retaining the minimum necessary requirement is essential to maintaining patients' trust in their physicians and other clinicians. Health plans do not have a right to access patient's health information unless the patient has explicitly requested or authorized such a disclosure. We caution OCR against finalizing this proposal, which could severely erode patient privacy and the patient-physician relationship.

Clarifying the Scope of Covered Entities' Abilities to Disclose PHI to Certain Third Parties for Individual-Level Care Coordination and Case Management That Constitutes Treatment or Health Care Operations

OCR proposes to create a new section of HIPAA that would expressly permit covered entities to disclose PHI to social services agencies, community-based organizations, home and community-based service (HCBS) providers, and other similar third parties that provide health-related services. Under this provision a health plan or a covered health care provider could only disclose PHI without authorization to a third party that provides health related services to individuals; however, the third party does not have to be a health care provider. Instead, the third party may be providing health-related social services or other supportive services—e.g., food or sheltered housing needed to address health risks.

Primary care physicians provide extensive care coordination and management services and often refer patients to community-based organizations to address their social needs. The AAFP strongly believes that addressing social determinants of health is critical to helping patients achieve their optimal health. Accordingly, we support the addition of this subsection, but we are concerned that it allows covered entities to disclose PHI without the patient's explicit authorization. The AAFP supports disclosure of PHI to social and community organizations when that disclosure is consistent with a patient's express wishes. **We again reiterate that patients should control when and where their information is shared.** We also note that there are a variety of situations where such a disclosure to a community-based organization or other agency could cause significant discomfort or harm to a patient, jeopardizing their safety and the patient-physician relationship. We do not recommend finalizing this subsection as proposed.

Encouraging Disclosures of PHI when Needed to Help Individuals Experiencing Substance Use Disorder, Serious Mental Illness, and in Emergency Circumstances

OCR proposes to replace the current standard, which allows covered entities to exercise professional judgement when disclosing information in the best interest of patients, with a good faith belief. The Department also proposes a presumption that a covered entity was acting in good faith absent evidence that the covered entity acted in bad faith. Despite current regulations permitting the disclosure of clinically relevant mental health records, many do not believe they are able to make these disclosures due to the HIPAA Privacy Rule. For these reasons, the AAFP supports these proposals and agrees that presuming physicians and other covered entities are acting in good faith

could improve the sharing of necessary information for the purposes of coordinating or managing a patient's care.

We note that maintaining patient privacy is particularly essential for patients with substance use disorders and severe mental illness, who may forgo needed treatments if they do not feel that their health information will be both private and secure. OCR should take steps to ensure that this change does not result in unintended consequences, such as causing patients to lose their housing, employment, child custody, or other rights if the covered entity shares information against their wishes. This is particularly true for Black, Indigenous, and other patients of color, undocumented individuals, and others who often disproportionately harmed by the criminalization of substance use.

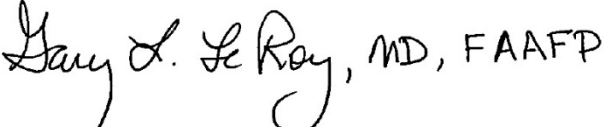
While we are supportive of the proposal to apply the good faith belief standard, **the AAFP is strongly opposed to regulatory changes that would expand the ability of covered entities to disclose PHI against a patient's wishes or in a manner that is inconsistent with the patient's privacy preferences.** In order to protect patient safety and wellbeing, as well as preserve the patient-physician relationship, we urge OCR to ensure that the patient's own preferences regarding the disclosure of their health information are always prioritized.

Eliminating Notice of Privacy Practices Requirements Related to Obtaining Written Acknowledgement of Receipt

OCR proposes to eliminate requirements to obtain an individual's written acknowledgment of receipt of a direct treatment provider's Notice of Privacy Practices (NPP) as well as the six-year retention requirement. **The AAFP strongly supports these proposals and urges OCR to finalize them. As we noted in our [comments](#) on OCR's HIPAA RFI, removing the written acknowledgement requirement would reduce administrative burden, such as the need to administer, store, update and monitor compliance.** We do not believe the current requirements add significant value for patients or their physicians.

The AAFP appreciates the Department's efforts to preserve and protect the privacy and security of a patient's health information. Thank you for the opportunity to comment on the NPRM. Should you have any questions, please contact Meredith Yinger, Senior Regulatory Strategist, at (202) 235-5126 or myinger@aafp.org.

Sincerely,



Gary LeRoy, MD, FAAFP
Board Chair
American Academy of Family Physicians