



June 2, 2022

The Honorable Xavier Becerra
Secretary
Department of Health and Human Services
200 Independence Avenue S.W.
Washington, D.C. 20201

The Honorable Lisa J. Pino
Director
Office for Civil Rights
Department of Health and Human Services
200 Independence Avenue S.W.
Washington, D.C. 20201

Re: HHS-OS-2022-0007; Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended

Dear Secretary Becerra and Director Pino:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 127,600 family physicians and medical students across the country, I write in response to the Request for Information, “Considerations for Implementing the Health Information Technology for Economic and Clinical Health (HITECH) Act, as Amended,” as [published](#) in the April 6, 2022 *Federal Register*.

The HITECH Act, as amended, requires HHS to consider “recognized security practices” that entities covered by the Health Insurance Portability and Accountability Act (HIPAA), and their business associates, demonstrate were in place for the previous 12 months when making determinations regarding penalties, audits, and remedies to resolve potential violations of the HIPAA security rule. OCR seeks comment to understand how covered entities (including physician practices) and business associates understand and are implementing recognized security practices.

The AAFP has long [supported](#) policies that guarantee the appropriate security of protected health information while working to [improve](#) patients’ access to their data, as well as the ability to share patients’ health information across the care team. We are strongly supportive of making data reliably interoperable while maintaining patient confidentiality.

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 also has legitimate purposes outside of the patient-physician relationship. Access to, and use of data, should always be based on the patient’s expressed desires and valid authorizations. The sharing of information among physicians and other clinicians [should](#)

STRONG MEDICINE FOR AMERICA

President
Sterling Ransone, MD
Deltaville, VA

President-elect
Tochi Iroku-Malize, MD
Islip, NY

Board Chair
Ada Stewart, MD
Columbia, SC

Directors
Andrew Carroll, MD, *Chandler, AZ*
Steven Furr, MD, *Jackson, AL*
Teresa Lovins, MD, *Columbus, IN*
Jennifer Brull, MD, *Plainville, KS*
Mary Campagnolo, MD, *Borderstown, NJ*
Todd Shaffer, MD, *Lee’s Summit, MO*

Gail Guerrero-Tucker, MD, *Thatcher, AZ*
Sarah Nosal, MD, *New York, NY*
Karen Smith, MD, *Raeford, NC*
Samuel Mathis, MD (New Physician Member), *Galveston, TX*
Amanda Stisher, MD (Resident Member), *Owens Cross Roads, AL*
Amy Hoffman (Student Member), *State College, PA*

Speaker
Russell Kohl, MD
Stilwell, KS

Vice Speaker
Daron Gersch, MD
Avon, MN

Executive Vice President
R. Shawn Martin
Leawood, KS

focus on facilitating care coordination, patient wellness, and the expressed wishes of the patient themselves.

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 over the last several years.

To that end, the AAFP [urges](#) OCR to coordinate closely with the HHS Office of the Inspector General (OIG), Centers for Medicare and Medicaid Services (CMS) and the Office of the National Coordinator for Health IT (ONC) when developing enforcement policies, regulations, and guidance. Health IT and information sharing regulations have changed dramatically with the implementation of the 21st Century Cures Act. Physician practices are now expected to continue to comply with HIPAA, which requires them to safeguard the confidentiality of patients' electronic health information, while also complying with information blocking regulations, which penalize them for failing to share information. Complying with both sets of regulations and their accompanying enforcement frameworks puts physicians in a frustrating, challenging position. These regulations must be harmonized to meaningfully improve patients' access to their health data and advance interoperability while also safeguarding patient privacy and security. **The AAFP strongly urges OCR to work with OIG, CMS, and ONC to ensure that the regulations governing the sharing and protection of patients' health information create a clear, easy to understand framework for physicians and other covered entities to operate within.** With these goals in mind, we are pleased to offer the following pieces of feedback on your questions.

What recognized security practices have regulated entities implemented? If not currently implemented, what recognized security practices do regulated entities plan to implement?

The AAFP and our members support the standards, guidelines, and best practices established through current law and regulation. Specifically, best practices established by the National Institutes of Standards and Technology (NIST) have been useful across a number of domains in health care, including cybersecurity best practices, patient identification and authentication, HIPAA Security Rule compliance, and a number of other areas.

As noted in our [confidentiality policy](#), in the digital space, electronic health information communication systems must be equipped with appropriate safeguards (e.g., encryption; message authentication, user verification, etc.) to protect physician and patient privacy and confidentiality. Individuals with access to electronic systems should be subject to clear, explicit, mandatory policies and procedures regarding the entry, management, storage, transmission, and distribution of patient and physician information. We agree with OCR that the NIST HIPAA Security Rule Toolkit, security checklist protocols, and cybersecurity framework are all useful tools for covered entities and business associates.

However, we note that cybersecurity continues to be a daunting and rapidly changing task for covered entities. While this is true of all sizes of organizations, maintaining an up-to-date and robust cybersecurity footing is an overwhelming task for small and medium physician practices.

Varied implementation of security practices across different physician practices is expected and enforcement practices should acknowledge this variation rather than hinder it. OCR must take this variation into account when determining the magnitude of fines and security practices that constitute “exercising reasonable diligence.” **Enforcement policies should not disproportionately penalize small or rural practices, practices serving underserved communities, or other physician practices that may not have the financial resources to invest in a multitude of security measures.** Enforcement policies must not take a uniform approach and should be flexible to allow for appropriate variations in practice characteristics.

While HITECH aims to encourage covered entities to take all steps to safeguard patient data, current information blocking regulations penalize physicians for failing to share information, unless they meet very specific, burdensome exceptions. For example, in order to interfere with the access, exchange, or use of EHI in order to protect the security of EHI (i.e, comply with the [security exception](#)) physician practices must tailor their use of the exception to specific security risks. In other words, physician practices have to be able to identify and document the specific security risks that are posed by sharing a patient’s health information. Physician practices are not equipped to identify and document the security risks posed by other practices’ EHR systems, application programming interfaces (APIs), or third-party applications. As a result, practices are compelled to provide access to or share a patient’s health information to avoid being penalized for information blocking. This framework runs directly counter to the goal of HITECH. **OCR must account for these competing regulations in its development of enforcement policies and ensure physicians and other covered entities are not punished for sharing data in compliance with information blocking regulations.**

Relatedly, physician practices should not be penalized or otherwise held accountable for the security flaws of APIs and third-party applications that may ultimately result in a breach. The AAFP and several of our partners recently [wrote](#) to ONC to share our concerns with the security of patient information being transmitted through APIs. Third-party applications are also not governed by HIPAA. The AAFP supports ongoing efforts to ensure the security of third-party apps as they connect patients to their health data, but physicians are unequipped to assess the security of APIs and third-party apps and do not have the authority to govern app functionality or security. **OCR’s enforcement regulations must explicitly outline that security flaws of third-party apps will not be the responsibility of the physician.** OCR should also work with ONC, CMS, and OIG to address existing security flaws and require apps to keep patients’ data private and secure.

Implementing appropriate security safeguards while maintaining the appropriate sharing of patient health information in the current regulatory environment is difficult and burdensome for physicians to navigate. **Enforcement policies developed by OCR need to account for the entire regulatory framework physicians must comply with, not just HITECH.**

Should the Department recognize as harm the release of information about a person other than the individual who is the subject of the information (e.g., a family member whose information was included in the individual’s record as family health history) for purposes of sharing part of a

CMP or monetary settlement? If yes, should the individual who is not the subject of the information be permitted to receive a portion of a CMP or monetary settlement?

No, the Department should not recognize as harm the release of information about a person other than the individual who is subject of the information when the regulated/covered entity or business associate has made reasonable effort to ensure that the individual to whom the information is being sent (in the case of an individual access request) or other covered actor (in the case of treatment, payment, or operations (TPO) authorization) is the subject of the information and the use of the data transfer is authorized. We believe this is consistent with current law. Under the current rule, "Breach" excludes:

Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in future use or disclosure in a manner not permitted [by the Privacy Rule]. 45 C.F.R. 164.402.

As noted above, we believe the right to privacy is personal and fundamental. We do not propose the limitation of the right or suggest that careless disclosure should go unchecked. However, **when the regulated/covered entity or their business associate takes all appropriate care to ensure that information disclosed for individual use or TPO purposes is authorized, we do not believe that covered entities should be punished.**

This view is consistent with the Information Blocking regulations promulgated by ONC and the Interoperability and Patient Access rule advanced by CMS. As mentioned previously, penalty for failure to share information is certain under these regulations and we've [repeatedly](#) called for coordination with these agencies. Given this new paradigm, it is probable that instances of releases of information for individual access or TPO will occur and that information disclosed may extend too far in an effort to avoid information blocking penalties. This disclosure, though, when done in good faith and with all appropriate care, should not subject covered entities or their business associates to breach sanctions. Since current certified EHR technology is not semantically interoperable, we are also likely, under this new paradigm, to see data about other individuals buried in another patient's record (such as genetic data or family history data) be shared even with good faith efforts by covered entities to expunge such data before appropriately sharing the larger record.

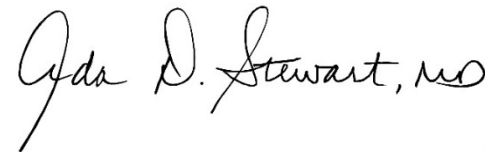
Further, current technology does not provide physicians with the ability to readily segment out individual data elements or certain portions of a patient's medical record when sharing information. In all, without the ability to segment certain data elements or portions of a patient's medical record, complying with information blocking regulations will unavoidably result in the sharing of all or most data in many situations, including sensitive data or data about other people. Given the absence of a technical solution that can be readily and reasonably used by physician practices, OCR must not penalize 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 this RFI. Should

Secretary Becerra and Director Pino
June 2, 2022
Page 5 of 5

you have any questions, please contact Meredith Yinger, Manager, Regulatory Affairs, at (202) 235-5126 or myinger@aafp.org.

Sincerely,

A handwritten signature in black ink that reads "Ada D. Stewart, MD". The signature is written in a cursive style with a large initial 'A' and a long, sweeping underline.

Ada D. Stewart, MD, FAAFP
Board Chair, American Academy of Family Physicians