White and Williams LLP

Information Blocking: What Providers and Programmers Need to Know

Part One: Ramped Up Enforcement Against Healthcare Providers
By: William D. Kennedy and Michael Horner
Healthcare Alert
4.22.22

Federal enforcement of the 21st Century Cures Act's (the Cures Act) prohibitions on improper blocking of electronic health information is ramping up. The Cures Act already targets technology developers and health information networks for penalties; now, enforcement is on the way against healthcare providers who improperly block the exchange of information.

Background

The 21st Century Cures Act was signed in December 2016 by President Obama to accelerate medical product development and healthcare innovations. By removing barriers to the necessary and efficient sharing of electronic health information (EHI), the Final Rule released by the Office of the National Coordinator for Health Information Technology (ONC) gives patients access to the essential data in their own electronic health record. Until October 5, 2022, for the purposes of the information-blocking definition, EHI is limited to a specific, federal data set that includes eight types of clinical notes that must be shared if requested. After October 5, 2022, providers and health information networks must make available ***all*** requested electronic health information that they have. (Psychotherapy notes are excluded from the definition of EHI for purposes of information-blocking.)

Examples of information blocking may include:

• Requiring a patient's written consent before sharing the patient's EHI with unaffiliated providers;

• Charging excessive fees that make exchanging electronic health information cost prohibitive;

• Adopting policies or contractual arrangements that restrict or prevent sharing information with patients or their healthcare providers;

• Erroneously citing the HIPAA Privacy Rule as a basis for refusing to share information;

• Healthcare providers or IT vendors that limit or discourage sharing information with other providers or with users of other IT systems;

• Erecting technological barriers that diminish the EHI portability with different IT systems, services, or applications that follow nationally recognized standards;

• "Locking in" patients or providers to a particular technology or healthcare network because their electronic health information is not portable.

The 21st Century Cures Act provides eight categories of "safe harbor" exceptions under which it may be proper to restrict or block the transmission of electronic health information. Where specific preconditions are met, five exceptions permit outright information blocking to prevent harm, to protect a person's privacy, to protect the security of the electronic data, during times needed for system upgrades and where sharing information is technically infeasible. The remaining three safe harbors focus on the content and manner in which data is shared, fees charged for sharing data and developers' licensing of interoperability elements of the electronic health

information.

Penalties

The anti-information blocking portion of the 21st Century Cures Act targeted software developers who incorporated into their platforms technology that blocked users from sharing medical information with other developers' platforms. Originally, these practices were sometimes touted as being necessary to be HIPAA-compliant, yet they had the practical effect of protecting a programmer or practice's proprietary possession of patients' healthcare information. The 21st Century Cures Act empowers the HHS Office of Inspector General (OIG) to issue civil monetary penalties of up to $1 million against software developers, networks or exchanges that interfere with the proper exchange of electronic health information.

At the time of its passage, the 21st Century Cures Act omitted specific penalties for healthcare providers who improperly blocked information; it focused more on programmers and networks. Yet as software developers and networks comply with the Cures Act, more than 75% of the complaints about information blocking in the past year have focused on providers reportedly blocking the proper flow of information. Patients and providers alike have cited suspected improper conduct by hospitals, healthcare facilities, physicians, and other providers. Filing a complaint is easy — those who are frustrated by information blocking may file complaints with the Office of National Coordinator. The Cures Act authorizes the HHS Office of Inspector General to investigate any claim of information blocking. The identity of complainants is protected from disclosure under the Cures Act.

In public comments during the March 2022 Global Health Conference of HIMSS (the non-profit Healthcare Information and Management Systems Society) and again during an April 2022 Annual Meeting of the ONC, HHS Secretary Xavier Becerra announced that plans to enforce the Cures Act against healthcare providers that improperly block information are a "top priority." Information blocking, Secretary Beccera said, leads to stress for patients and families, along with frustration for staff. Becerra criticized an instance where a patient was told to wait weeks for access to test results while their physician was on vacation. "That is not the kind of customer experience any of us should expect, certainly not in the 21st century, from our healthcare system."

HHS anticipates announcing a specific enforcement regiment of civil monetary penalties by the end of 2022. Likewise, the Centers for Medicare and Medicaid Services (CMS), the largest payer and regulator of medical practices, has announced its interest in levying civil monetary penalties for providers that improperly block the sharing of electronic health information.

Practice Pointers

Health systems, hospitals, practitioners and private practices will want to get ahead of the forthcoming penalty announcements by carefully focusing on compliance with the 21st Century Cures Act and its regulations. Organizations ought not merely assume their electronic medical records vendor is taking care of everything.

Both to comply with the law and defend themselves against any future allegations of impropriety, organizations will want to establish a specific, clear, codified process for evaluating information requests. It is vital that the necessary staff members know where the safe harbors are — and where they are not.

Likewise, providers should create careful and accurate documentation of any instance in which it refuses to share requested information. Some organizations are developing checklists or logs that memorialize who has requested what information, the organization's evaluation of the request and its response. By developing a thoughtful compliance process to evaluate each specific request, healthcare organizations will be well-prepared to defend against unwarranted complaints filed with the ONC by frustrated

record-seekers.

White and Williams has a team of attorneys experienced in the prohibition of information blocking. If you have any questions or would like further information, contact William D. Kennedy (kennedyw@whiteandwilliams.com; 215.864.6816), Michael W. Horner (hornerm@whiteandwilliams.com; 856.317.3658), Michael O. Kassak (kassakm@whiteandwilliams.com; 856.317.3653, Victor J. Zarrilli (zarrilliv@whiteandwilliams.com; 856.317.3672) or Frank A. Bruno (brunof@whiteandwilliams.com; 215.864.6225).

In Part Two of our series on "Information Blocking: What Providers and Programmers Need to Know," we will highlight how even before HHS announces provider penalties, providers who may be experiencing improper blockages of EHI from other entities can work to stop the blockage. Part Three will focus on the balance between HIPAA compliance and adhering to the prohibitions on information blocking.