Be Aware of Recent Legal Developments Concerning Right of Access to Patient Information

Two major recent regulatory developments highlight the need for health care organizations to focus on compliance concerning requests for access to patient health information.

HIPAA Right of Access Initiative

As most health care businesses are generally aware, HIPAA has long required[1] that, with limited exceptions, health care providers and other HIPAA "covered entities" must give patients and their personal representatives access to their health information[2] upon request. Covered entities must, in most cases, respond to such requests by providing access within 30 days. Further, covered entities must provide access to records in the form and format requested by the individual if the records are readily producible in that form and format. HIPAA imposes numerous other requirements that govern responses to such requests, including rules concerning permissible charges for producing records.[3]

HIPAA's right of access requirement also applies to health care businesses (i.e., HIPAA business associates) that serve covered entities in roles that involve access to or maintenance of health information. Covered entities will sometimes be unable to provide individuals with sufficient access to their health information without specific action from these business associates.

Until recently, HIPAA's patient right of access requirement was very rarely enforced and, as a result, has not always been a major compliance priority for health care businesses. During 2019, however, we began to see some right of access enforcement activity (i.e., two settlements) by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS) under its new Right of Access Initiative.[4]

Somewhat surprisingly, given that the COVID-19 pandemic has shifted regulatory priorities, 2020 has been a particularly active year for OCR's right of access enforcement, with a grand total of seven OCR settlements announced during the second half of the year thus far. The current settlements announced have involved a wide range of providers—from solo practitioners to a hospital owned by a large national health system—and settlement amounts have ranged from $3,500 to $160,000. All settlements have involved either complete failure to provide requested records or a failure to provide all of the records requested.

OCR's new focus in this area highlights the need for both health care providers and vendors to proactively focus on their right of access compliance and ensure that they are adequately equipped to promptly respond to access requests when they receive them. In practice, we have found that health care businesses most often become confused about: (1) the response timeframes that apply to them; (2) records request fees they are permitted to charge to requesting parties; and (3) format requirements that apply in responding to requests. Thus, it is important for health care providers and vendors to have HIPAA policies that address these issues and adequately train personnel to respond to access requests in the manner required. Further complicating this issue are the additional requirements of the Information Blocking Rule, which is further discussed below.

ONC's New Information Blocking Rule

Adding another dimension to HIPAA's right of access requirement is the anti-information blocking portion of the 21st Century Cures Act (the Cures Act), which was enacted in 2016. The Cures Act went much further than HIPAA's right of access requirement by, in very broad terms, prohibiting actions or practices "likely to interfere with, prevent, or materially discourage access, exchange or use of electronic health information."[5] However, this prohibition needed to be further developed and implemented through regulatory action.

Earlier this year, the Office of the National Coordinator for Health Information Technology (ONC) at HHS released a final rule that further developed the information blocking prohibition (the Information Blocking Rule or the Rule), among other issues.[6] The Rule applies to health care providers, defined very broadly, as well as to developers of certified health information technology (Developers), health information networks (HINs", and health information exchanges (HIEs), which the Rule refers to collectively as "actors." The Rule's information blocking prohibition itself relates to electronic health information (EHI), which is "electronic protected health information" maintained in a "designated record set,"[7] as those terms are defined under HIPAA.[8]

Most importantly, the language of the Information Blocking Rule is so broad that it creates a risk of prohibited information blocking with any number of a business's actions, system configurations, or contract terms. This creates a need for all impacted businesses to adequately understand where information blocking can become an issue and then take steps to comply with the Rule. Some examples of information blocking include the following:

- Denial of access, unreasonable delay in providing access, placing inappropriate conditions upon access, or failing to provide access in the form and format requested when EHI is requested by any number of parties, including patients and their personal representatives, health insurance plans, providers, quality improvement committees, researchers, and other types of parties;
- Configuration of technology to limit system interoperability or exchange of data; or
- Implementing contracts pertaining to EHI or system interoperability elements that interfere with the access, exchange, and use of EHI by imposing commercially unreasonable fees, licensing terms, or other inappropriate requirements.

The items set forth above are only examples of potential information blocking and should not be viewed as comprehensive, since it is currently impossible to state with certainty the full range of potential actions, system configurations, and contract terms that could be considered information blocking. Because information blocking creates a risk of OIG enforcement and the possibility of substantial civil monetary penalties[9] and other consequences, providers and other actors will need to carefully consider their organizational policies, actions, system configuration, and contracts to identify potential information blocking issues.

Notably, the Information Blocking Rule does not require granting access to information or taking any other actions that would violate HIPAA or other federal or state laws. When considering information blocking issues, an important first question is whether providing access to EHI or taking another type of action in a particular situation is effectively prohibited by HIPAA or other applicable law. If the answer is yes, then the Information Blocking Rule does not require the action. However, there are many situations in which HIPAA, for example, will permit but not require granting access to EHI. When HIPAA permits granting access or another action concerning EHI, that action may in the future be required by the Information Blocking Rule, and parties should therefore consider whether the Information Blocking Rule applies when handling access, disclosure, or other questions related to patient data.

Fortunately, the Information Blocking Rule contains several exceptions that providers and other actors may use to take actions that would otherwise be considered information blocking in specific situations. Actors must satisfy all applicable requirements and conditions of a particular exception to be reasonably certain that it will apply. The exceptions include the following:[10]

- An actor may engage in a practice that would otherwise be considered information blocking if, among other conditions, the actor has a reasonable belief that the practice will substantially reduce the risk of harm to a person—e.g., disclosure is likely to endanger life or physical safety;
- An actor may block EHI consistent with certain provisions of federal or state privacy law designed to protect individual privacy;
- An actor may block EHI in order to protect the security of EHI;
- An actor may block EHI to the extent certain extraordinary circumstances make granting the request infeasible;
- An actor may temporarily block EHI for maintenance or to implement improvements to health information technology;
- An actor must generally provide access, exchange, or use of EHI in any manner requested unless it is technically unable to fulfill a request or cannot reach agreeable terms with the requesting party to fulfill the request;
- An actor may charge a reasonable fee for accessing, exchanging, or using EHI if it satisfies certain HIPAA and other requirements (notably, the actor cannot charge for electronic access); and
- An actor may license interoperability elements and negotiate for the same if certain negotiation timing and licensing conditions are met.

Although the compliance date for the Information Blocking Rule was (and technically still is) November 2, ONC will exercise enforcement discretion (relaxed enforcement) for three months after that date, and ONC has also submitted an interim final rule, which is currently being reviewed by the Office of Management and Budget (OMB), to delay the compliance date due to the ongoing pandemic. Further, for providers, the mechanisms to enforce the Rule (i.e., disincentives) have not yet been developed through rulemaking. For Developers, HINs, and HIEs, enforcement of the Information Blocking Rule by the HHS Office of Inspector General (OIG) will not commence until after the OIG implements its related enforcement rule. As of this writing, the OIG has not yet submitted a final civil monetary penalties rule for review by OMB, and there is not yet any sign of another rulemaking for provider disincentives, so it appears that enforcement of the Information Blocking Rule will not begin until sometime in 2021 or possibly later.

In the meantime, providers and others soon to be affected by the Information Blocking Rule should continue to prepare for compliance. Some actions to consider are as follows:

- Work to identify information blocking issues that may arise within a provider or other actor's organization, including considering the types of EHI access, exchange, or use requests it has received in the past and may therefore be called upon to respond to in the future;
- Consider system configurations and settings to identify any information technology issues that could implicate the Information Blocking Rule;
- Implement policies and procedures to address information blocking issues, and update HIPAA policies and procedures to address potential interactions between HIPAA and the Information Blocking Rule (keeping in mind that some actions previously permitted but not required by HIPAA will now be required);
- Educate and train staff members who could be making decisions that implicate the Rule;
- Evaluate whether licensing agreements, HIPAA business associate agreements, or other contracts in place with outside parties contain any provisions that could implicate the Information Blocking Rule; and
- Consider whether there are any instances in which an actor's organization may be able to strategically use the Information Blocking Rule's broad requirements to gain access to beneficial information that was previously unavailable.

Our Chambliss team continues to monitor ongoing legal developments in connection with access to patient information. If you have questions about these regulatory developments, please contact Cal Marshall or another member of theHealth Care team for additional information.

---

[1] – 45 C.F.R. §164.524

[2] – That is, "protected health information" maintained in a "designated record set."

[3] – Most states (including Tennessee) also have laws governing the right of access to health information. Because HIPAA defers to state laws where they give individuals greater rights than HIPAA (e.g., such as by requiring that access be granted sooner than 30 days—Tennessee's rule is "10 working days"), covered entities must take care not to lose sight of state law when responding to access requests.

[4] – https://www.hhs.gov/about/news/2019/09/09/ocr-settles-first-case-hipaa-right-access-initiative.html

[5] – 42 U.S.C.A. §300JJ-52. Also, both the statute and Information Blocking Rule contain an intent standard for the violation of the information blocking prohibition. For Developers, HINs, and HIEs (as defined in the text of the article), the intent standard is "knows, or should know" that a practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI (as defined in the text of the article). For providers, the intent standard is "knows that such practice is unreasonable" and is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

[6] – The 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25642 (May 1, 2020). Separately, the Centers for Medicare and Medicaid Services (CMS) released a similar companion rule addressing health information access that applies to payors participating in federally-funded health care programs.

[7] – Readers should remember that "electronic protected health information" is protected health information that is transmitted or maintained in electronic media. "Protected health information" is a very broad term that can include both health care information and payment/billing information. "Designated record set" is also a very broad term that can include, among other things, medical records, billing records, or any other records used by a covered entity to make decisions about an individual.

[8] – With that said, until May 2, 2022, actors will only be obligated to comply with the Rule with respect to the more limited scope of data elements set forth in the U.S. Core Data for Interoperability Standard, Version 1. These elements may be viewed at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.

[9] – Notably, the OIG's civil monetary penalty authority under the Cures Act does not extend to health care providers. The "disincentives" to be applied to providers will be determined in future rulemaking. However, the "Promoting Interoperability" (Meaningful Use) performance criteria under the Medicare Access and CHIP Reauthorization Act of 2015 (MACRA) include information blocking attestations. As a result, for providers who have provided such attestations, information blocking could negatively impact Medicare reimbursement and potentially even have health care fraud implications.

[10] – These are paraphrased summaries that do not address every specific component of the exceptions, and an actor should carefully review and satisfy all conditions of an exception before relying on it.

Visit our COVID-19 Insight Center for our latest legislative and legal updates, articles, and resources.

The material in this publication was created as of the date set forth above and is based on laws, court decisions, administrative rulings, and congressional materials that existed at that time, and should not be construed as legal advice or legal opinions on specific facts. In some cases, the underlying legal information is changing quickly in light of the COVID-19 pandemic. The information in this publication is not intended to create, and the transmission and receipt of it does not constitute, a lawyer-client relationship. Please contact your legal counsel for advice regarding specific situations.