Special Report

Information Blocking and HIPAA's Right to Access: Compliance Burdens for Healthcare Providers

By Joseph J. Lazzarotti

July 22, 2021

Meet the Authors

Joseph J. Lazzarotti
Principal
908-795-5205
Joseph.Lazzarotti@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity

Since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule became effective in 2003, it generally required covered entities to provide patients timely access to their medical records. Of course, state health laws also have provided similar rights to patients regarding their records, some more and some less stringent than HIPAA.

However, concerns over the level of patient access to records are driving increased emphasis, heightened enforcement activity, and new laws to ensure individuals have easy access to their health information. This includes the two-year-old Office for Civil Rights Right to Access Enforcement Initiative and the new information blocking rules under the 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program.

A critical goal of these efforts is to empower patients to be more in control of decisions regarding their health and well-being. By helping individuals have ready access to their health records, according to OCR, they are better positioned "to monitor chronic conditions, adhere to treatment plans, find and fix errors in their health records, track progress in wellness or disease management programs, and directly contribute their information to research." During the nearly 20 years since the HIPAA Privacy Rule became effective, technological changes now support even greater access rights, including enabling access in real time and on demand.

Questions received over the years from providers inspire this summary of requirements and some best practices for ensuring patients have access to their records and avoiding enforcement actions, headaches, and penalties.

What is the "Right to Access" under HIPAA?

The HIPAA Privacy Rule generally requires HIPAA-covered entities (health plans and most healthcare providers) to provide individuals, upon request, with access to protected health information (PHI) about them in one or more "designated record sets" maintained by or for the covered entity. This includes the right to inspect, obtain, or both, a copy, as well as to direct the covered entity to transmit a copy to a designated person or entity of the individual's choice. This right applies for as long as the covered entity (or its business associate) maintains the information, regardless of the date the information was created, and whether the information is maintained in paper or electronic systems onsite, remotely, or is archived.

When implementing this rule, covered entities and their business associates have several issues to consider, such as:

- What information is subject to the right and what information is not, such as psychotherapy notes.

- Confirming the authority of "personal representative" to act on behalf of an individual.
- Procedures for receiving and responding to requests, such as written request requirements, verifying the authority of requesting parties, timeliness of response, whether and on what grounds requests may be denied, and fees that can be charged for approved requests.

Are certain categories excluded from the Right to Access?

Yes. Categories of information that are excluded from the Right to Access under HIPAA include:

- Information not used to make decisions about the individual
- Psychotherapy notes
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding

An example of information that is not used to make decisions about the individual is information maintained as part of providers' peer review process.

While the Right to Access under HIPAA may exclude certain information, patients may have broader rights under state law that are not preempted by HIPAA. Accordingly, when responding to requests for access, providers must also be aware of the applicable state law requirements.

When must records be provided?

In general, HIPAA requires records to be provided within 30 calendar days from receipt of the request. As with many such timeframes (including the breach notification rule), 30 days is an outer limit. This means that covered entities should endeavor to respond to a Right to Access request sooner if possible.

If the covered entity cannot respond within the initial 30-day period, such as when the information requested is maintained in offsite storage, an extension of up to 30 calendar days is permitted. To take advantage of this extension, the provider must inform the individual in writing during the initial 30-day period of the reasons for the delay and the date by which it will respond. State law also may shorten the time to respond and may not permit an extension. Further, regulations have been proposed to shorten the current 30-day rule to 15 days.

Can requests for access be denied?

Yes, in limited circumstances. Providers must consider the reason for denying access, because the individual may have a right to appeal in some cases.

Examples of circumstances in which a covered entity may deny a request for the Right to Access *without* also being subject to having that decision reviewed include: (i) a request for psychotherapy notes; (ii) a request for information compiled in anticipation of a legal proceeding; (iii) requests in connection with certain research studies; and (iv) a request relating to information obtained by someone other than the provider (*e.g.,* family member) under promise of confidentiality.

In certain other cases, the decision to deny access to an individual is subject to review by a licensed healthcare processional not involved in the original decision to deny

access. These cases include denials based on determinations that (i) access is reasonably likely to endanger the life or physical safety of the individual, or (ii) access to the individual's personal representative is reasonably likely to cause substantial harm to the individual or another person.

Can a fee be charged?

The OCR would prefer covered entities do not impose fees on individuals to access their records. According to the OCR:

> While the Privacy Rule permits the limited fee described above, covered entities should provide individuals who request access to their information with copies of their PHI free of charge.

However, the law permits fees to be charged, provided they are*reasonable, cost-based fees when* individuals request copies of records (or a summary of explanation). Additionally, the following items may be taken into account:

- Labor for copying the PHI, whether in paper or electronic form;
- Supplies for creating the paper copy or electronic media (*e.g.,* CD or USB drive) if the individual requests the electronic copy be provided on portable media;
- Postage, when the individual requests the copies or summary be mailed; and
- Preparation of an explanation or summary of the PHI, if agreed to by the individual.

Covered entities that want to charge a fee will need to think carefully about the calculation of those fees and when they are assessed. State law also may need to be considered.

How is the Right to Access being enforced?

In 2019, the OCR commenced its Right of Access Initiative, an enforcement priority to support individuals' right to timely access to their health records at a reasonable cost. At least one study found providers are struggling to fully comply. Nonetheless, the OCR has announced nearly 20 enforcement actions under its Right of Access Initiative – a full list of enforcement actions is available on the OCR website.

The OCR's enforcement actions have typically resulted in resolution agreements with covered entities. About half of the entities investigated are small providers, including solo practitioners. Monetary settlements to date have ranged from $3,500 to $200,000. In addition, the OCR resolution agreements require the covered entities to develop a corrective action plans to prevent further violations. Examples of required actions covered entities agree to under a Right of Access corrective action plan include:

- Two years of monitoring by the OCR;
- Revise its right of access policies;
- Submit its right of access policies to OCR review;
- Obtain written confirmation from staff that they read and understand the new right of access policies;
- Train staff on the new policies; and
- Every 90 days submit to OCR a list of requests for access from patients and the covered entity's responses.

Taking steps to get compliant with the HIPAA Right to Access rule can enhance greatly

the chance of avoiding an OCR investigation and a covered entity's ability to negotiate a more favorable result.

What is information blocking?

The Cures Act included provisions intended to minimize the interference with the ability of authorized persons or entities to access, exchange, or use electronic health information – in general, "information blocking." The Cures Act authorized the Secretary of Health and Human Services (HHS) to identify, through rulemaking, reasonable and necessary activities that do not constitute information blocking.

The law also empowers the HHS Office of Inspector General (OIG) to investigate claims of information blocking and to provide referral processes to facilitate coordination with the OCR. The goal of these provisions is to support seamless, secure access, exchange, and use of electronic health information (EHI).

The Cures Act defines information blocking as business, technical, and organizational practices that prevent or materially discourage the access, exchange, or use of EHI when an actor knows, or (for some actors like electronic health record vendors) should know, that these practices are likely to interfere with access, exchange, or use of EHI. If conducted by a healthcare provider, the focus here, there must also be knowledge that the practice is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

Which healthcare providers are subject to the information blocking rules?

The Cures Act specifies three categories of entities or "actors" that must comply with information blocking requirements: (i) healthcare providers; (ii) health IT developers of certified health IT; and (iii) health information networks and health information exchange.

"Healthcare providers" is defined broadly:

> *hospital; skilled nursing facility; nursing facility; home health entity or other long term care facility; health care clinic; community mental health center; renal dialysis facility; blood center; ambulatory surgical center; emergency medical services provider; federally qualified health center; group practice; pharmacist; pharmacy; laboratory; physician; practitioner; provider operated by or under contract with the Indian Health Service or by an Indian tribe, tribal organization, or urban Indian organization; rural health clinic; covered entity under 42 U.S.C. 256b; ambulatory surgical center; therapist; and any other category of health care facility, entity, practitioner, or clinician determined appropriate by the HHS Secretary. Readers can examine the full definition at 42 U.S.C. 300jj.*

The rules apply to healthcare providers even if they do not use certified health IT. Moreover, the definition if not limited by size of business or to healthcare providers that are covered entities under HIPAA.

What health information is subject to the information blocking rules?

The information blocking rules apply to EHI regardless of when it was generated.

Until October 6, 2022, EHI is limited to information represented by data classes and elements within the United States Core Data for Interoperability. For example, this

would include eight types of "Clinical Notes" (*e.g.,* history, Review of Systems, physical data, diagnosis, and plan of care): (1) Consultation Note; (2) Discharge Summary Note; (3) History & Physical; (4) Imaging Narrative; (5) Laboratory Report Narrative; (6) Pathology Report Narrative; (7) Procedure Note; and (8) Progress Note. None of these eight types of clinical notes are limited based on the type or specialty of the professional who authors them.

What are some examples of prohibited information blocking activity?

Whether an activity violates the information blocking rules generally requires a fact-based, case-by-case assessment of the circumstances. The assessment would address whether the interference is with the legally permissible access, exchange, or use of EHI; whether the actor engaged in the practice with the requisite intent; and whether the practice satisfied the conditions of an exception.

Examples of activities that could constitute a violation of the information blocking rules include:

- *Restrictive policies:* A physician's office requires written patient consent (as opposed to electronic consent) before sharing any EHI with unaffiliated providers for treatment purposes.
- *Technology-related limitations:* A physician disables the use of an electronic health record capability that would enable staff to share EHI with users at other systems.
- *Unreasonable delays:* A physician is able to provide same-day EHI access in the format requested by their patient or an unaffiliated provider, but instead takes several days to respond. However, if the release of EHI is delayed in order to ensure the release complies with state law, it is unlikely to be considered an interference if the delay is no longer than necessary.

Are there exceptions to the information blocking requirements?

There are eight types of "reasonable and necessary activities" that have been identified as exceptions to information blocking. Those eight activities are grouped into two categories

Exceptions when an actor does not fulfill requests to access, exchange, or use EHI:

- Preventing harm exception
- Privacy exception
- Security exception
- Infeasibility exception
- Health IT performance exception

Exceptions that involve the actors' procedures for fulfilling requests:

- Content and manner exception
- Fees exception
- Licensing exception

Importantly, satisfaction of one or more exceptions requires the actor to have met certain conditions. A discussion of the conditions for each of these exceptions is beyond the scope of this summary, but provider should review those conditions carefully and implement them where possible. However, a provider's practice that does not meet the conditions of an exception will not automatically constitute information

blocking. Instead, such practices will be evaluated on a case-by-case basis to determine whether information blocking has occurred.

If a provider meets the HIPAA timeframe under the Right of Access requirement, will it satisfy the information blocking rule?

Not necessarily. The information blocking regulations have their own standalone provisions. An actor's meeting obligations under another law will not automatically demonstrate the actor's practice does not implicate the information blocking definition.

What are the penalties for violating the information blocking rule?

Under the Cures Act, actors found to have committed information blocking are subject to penalties issued by the OIG:

- *Health IT developers of certified health IT, health information networks, and health information exchanges:* Civil monetary penalties up to $1 million per violation.
- *Healthcare providers:* Appropriate disincentives to be established by the Secretary of HHS.

At this point, additional rulemaking from HHS is needed to outline what "appropriate disincentives" could apply.

When are the information blocking rules for healthcare providers effective?

The final rule on information blocking was set to apply on November 20, 2020, but was delayed to April 5, 2021, due to the COVID-19 pandemic.

What should we be doing?

Providers receive all kinds of requests for medical and other records in the course of running their businesses. Reviewing and responding to these requests no doubt creates administrative burdens. However, buying forms online might not get the practice all it needs, and could put the practice at additional risk if those materials, if compliant, are followed without considering state law or are not implemented properly.

Putting in place relatively simple policies, carefully developing template forms, assigning responsibility, training, and documenting responses can go a long way toward substantially minimizing the risk of OCR enforcement actions or Cures Act penalties. Providers also should consider sanctions under state law that also might flow from failing to provide patients access to their records in a compliant time and manner.

Here are some key takeaways:

- Assess whether the fees being charged for Right to Access are permissible
- Review policies and procedures and modify those that unreasonably delay or prohibit data sharing or access
- Develop written policies to address the information blocking exceptions, including preventing harm, privacy, and security exceptions
- Review business associate agreements to ensure you will be able to comply. Such agreements cannot be used to limit disclosures
- Know your state law

Please contact a Jackson Lewis attorney if you have questions or need assistance.