Briefings on HIPAA

Inside the 21st Century ONC Cures Act

by Dom Nicastro

The Office of the National Coordinator for Health Information Technology (ONC)'s "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" final rule went into effect June 30, 2020.

The applicability date for the information blocking provisions was April 5, 2021, and HIPAA compliance officers should have these provisions on their radar. According to **Gina Bertolini,** a partner in the Research Triangle Park office at Pittsburgh-based K&L Gates LLP, the ONC final rule includes two primary components:

- The adoption of standards and certification criteria for health IT developers
- A general prohibition of practices that constitute information blocking, plus exceptions and penalties

Paradigm shift

The information blocking provisions have the potential to "revolutionize the way health information is accessed, used, and disclosed for a variety of stakeholders in the healthcare industry," according to **Vimala Devassy,** an Atlanta-based partner in BakerHostetler's national healthcare group.

"Although the regulations have widespread implications throughout the healthcare industry, the access-to-information revolution begins with patients themselves," Devassy adds, "as it requires providers make categories of electronic health information [EHI] readily available to patients without delay, which can often result in the provider and patient having simultaneous access to health information."

The regulations are such a paradigm shift that they can almost feel like an alternate reality to those who are steeped in HIPAA compliance, according to Devassy. While HIPAA tends to be much more prescriptive, with bright lines in terms of how health information can be used and disclosed, the information blocking regulations are much more permissive and simply prohibit any organizational or system restrictions that somehow impede the flow of EHI unless one of eight exceptions apply.

"As such, all EHI must be released upon request unless a specific exception applies, which has been difficult for many in the healthcare industry to conceptualize due to extremely broad nature of the disclosures that cannot be restricted under the regulations in contrast to the narrowly drawn disclosures that are permitted under HIPAA," Devassy says.

"While EHI is defined as all electronic protected health information in a designated record set, it only includes those certain data elements in the United States Core Data for Interoperability, such as lab results and clinical notes, until the regulations take full effect in October of 2022."

See this ONC timeline for all relevant effective/other dates.

What is information blocking?

According to ONC, information blocking is a practice by a developer of certified health IT, a health information network, a health information exchange, or a healthcare provider (known as "actors" that, with limited exceptions, are likely to interfere with access, exchange, or use of EHI under the regulations).

Section 4004 of the Cures Act specifies certain practices that could constitute information blocking:

- Practices that restrict authorized access, exchange, or use under applicable state or federal law of such information for treatment and other permitted purposes under such applicable law, including transitions between certified health IT applications
- Implementing health IT in nonstandard ways that are likely to substantially increase the complexity or burden of accessing, exchanging, or using EHI
- Implementing health IT in ways that are likely to:

Restrict the access, exchange, or use of EHI with respect to exporting complete information sets or transitioning between health IT systems

Lead to fraud, waste, or abuse, or impede innovations and advancements in health information access, exchange, and use, including care delivery enabled by health IT

What is not information blocking?

Unlike HIPAA, which has a laundry list of specific compliance obligations (i.e., develop policies and procedures, conduct training, perform security risk assessments, etc.), compliance with information blocking regulations is much more open-ended and requires actors to take a broad view of compliance within the organization and remove any obstacles that could impede EHI unless an exception applies, according to Devassy.

She notes that the exceptions set forth in the regulations under which actions would not be deemed information blocking include:

Preventing harm exception: It is permissible to withhold the requested information if the information may endanger the life or physical safety of a patient or another person and withholding it will significantly reduce risk of harm. However, a blanket determination of harm will not suffice; a truly individualized and reasonable belief that harm will result to a specific patient must be established to fit within this exception.

Privacy exception: Failure to fulfill a request that would violate HIPAA or applicable law would be a permissible exception under the regulations.

Security exception: Withholding EHI that could cause a security risk to an organization would not be deemed information blocking. The regulations do not restrict the ability of actors to have reasonable practices in place to safeguard against security risks.

Infeasibility exception: Inability to provide EHI due to technical limitations related to software or uncontrollable events would not be deemed information blocking.

Health IT performance exception: Inability to provide EHI due to health IT performance issues, such as maintenance/downtime of the electronic health record system, would not be deemed information blocking.

Content and manner exception: If an organization cannot provide EHI in the content or manner in which it is requested, this shall not be deemed information blocking as long as the EHI is provided in a different manner as outlined in the regulations.

Reasonable fees exception: Charging reasonable fees for the EHI in accordance with HIPAA or applicable law would not be considered an impediment to the release of EHI that results in information blocking.

Licensing exception: Actors are permitted to charge reasonable royalties in order to earn returns on the investments they have made to develop innovations without the licensing/royalty requirements being deemed information blocking.

What's no longer permissible?

Some of a health system's previous practices may no longer be permissible under the information blocking regulations. One example, according to Bertolini, is an internal policy or procedure that requires staff to obtain a patient's written consent before sharing any of the patient's EHI with an unaffiliated healthcare provider for treatment purposes, where obtaining such consent is not required by applicable law.

Bertolini also provides other examples of practices that may now be impermissible:

- A health system policy or procedure that delays providing access to EHI (e.g., lab results) to a patient, even though such access is available in the form and format requested by the patient, where state law does not otherwise require a delay
- A refusal to disclose a patient's EHI *to the patient* because the healthcare provider is concerned that the contents of the EHI may cause emotional harm to the patient, where other laws do not require that the healthcare provider withhold the records

Policies and procedures checkup

Kate Stewart, of counsel for Boston-based Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, P.C., says HIPAA compliance officers should familiarize themselves with the ONC Cures Act final rule and keep abreast of developments in the form of new guidance from ONC and future enforcement actions.

“Though the initial compliance date has already passed, compliance officers need to be assessing their initial roll-out of policies and procedures around information blocking and helping their organizations to refine their approach,” she says. “Practically, many organizations likely had to rush their compliance efforts—just a few other things happening in healthcare in the last year—so now is a good time to do a gap assessment and see how things are working.”

Actors and their compliance teams also need to be preparing for the expanded definition of “electronic protected health information” that will come into effect on and after October 6, 2022. That expanded definition will cause the regulations to cover much more patient data than they currently do—EHI definition will no longer be limited to the EHI identified by the data elements represented in the United States Core Data for Interoperability.

“Though HIPAA-covered entities have been dealing with HIPAA’s patient right-of-access provisions for years, and this has been a big source of OCR enforcement lately, compliance goes well beyond the patient right-of-access requirements under HIPAA,” Stewart says. “It requires organizations to look at all of the ways in which they may be blocking access to health information.”

Shift in thinking

John W. Kaveney, partner in the healthcare department at Iselin, New Jersey–based Greenbaum, Rowe, Smith & Davis LLP**,** says the ONC Cures Act has forced compliance officers to think about patients’ health information in a different way.

Whereas HIPAA was designed to create a set of standards to protect patient data from disclosure, Kaveney says, the Cures Act focuses instead on providing patients with prompt access to their EHI, including the promotion of interoperability by utilizing application programming interfaces (API).

“Compliance officers need to be cognizant of the concept of information blocking, or the improper withholding of EHI from a patient, which is strictly prohibited under the Act and subject to yet-to-be-determined penalties,” Kaveney adds. “A lot of organizations are expending significant time and effort to educate their providers about the limited enumerated exceptions to information blocking so as to ensure the avoidance of inadvertent violations of the act by erroneously withholding EHI from patients.”

Due diligence required

The Cures Act requires prompt access of a patient’s EHI be made available to them through a standardized API. Moreover, Kaveney says, with the act’s information blocking provisions, providers have limited bases upon which to withhold a patient’s EHI.

“The greatest impact for healthcare providers is that it requires diligence on their part, not only in timely completing and signing notes and other reports that need to be promptly made available to patients, but also in ensuring that they promptly review lab results and other information that may become available during the treatment of a patient because the patient in many instances is being given real-time access to the same information,” Kaveney says. “This is a significant change from the days when a patient would have to wait for a call from the doctor, once the doctor had a chance to review lab results or other information.”

As for business associates, EHI in their possession is similarly subject to the Cures Act, he adds, and thus it is important for covered entities and business associates to have substantive conversations concerning compliance efforts.

Who needs to get involved?

Because Cures Act compliance involves prompt and generally unrestricted patient access to their EHI, various people within an organization must coordinate their efforts, says Kaveney. Those involved, he says, should include:

- The privacy officer and legal department, to ensure compliance with the Cures Act requirements and education of all those involved
- The IT department, to coordinate and develop functionality to allow patient access to EHI
- Medical staff leadership, to ensure provider cooperation and buy-in and to relay logistical concerns
- The health information management team, to help coordinate the interface of information and access with patients in the community

Establishing an interdisciplinary steering committee to ensure compliance is advisable as the regulations touch so many aspects of the organization, according to Devassy. In particular, she says, it is helpful to have involvement from the following stakeholders:

- The health information management department, as many of the requests for EHI may initially come through this department and/or need to be fulfilled by this department
- The IT department, as it will need to configure the settings and policies within the organization’s information systems to

ensure that they do not result in information blocking
- The legal/risk management department and privacy/compliance officer, to assess whether requests fit within an exception and to assess contractual arrangements and organizational policies to ensure that they do not result in information blocking, as well as to develop policies and procedures and training across the organization
- Physicians and clinical leadership, including from the lab and radiology department, to advise on the impact of the regulations from an operational standpoint and whether requests may fit within an exception, and to encourage clinician buy-in

Compliance requires a multi-stakeholder approach, Stewart adds. Those stakeholders should include representatives from IT, representatives from a medical records or health information management office, and representatives from clinical functions.

“For providers, the rule requires education of practitioners who document notes regarding their patient encounters about how those notes may now be shared,” she says. “Practitioners should be counseled on the fact that their notes may be more widely available to patients and should be drafted with an eye to how the patient may view the descriptions used in the note.”