wiley

NEWSLETTER

Compliance Roadblocks: Tackling Information Blocking Challenges in Health Care – Part 2

November 2020

Privacy in Focus®

In Part 1 of our information blocking series, we introduced readers to the fundamentals of information blocking, including definitional terms, information blocking exceptions, and compliance deadlines and penalties for health care actors. Since publication of our first installment, the U.S. Department of Health and Human Services published an interim final rule on October 29, 2020 (published in the Federal Register on November 4, 2020), extending the compliance deadline from November 2, 2020 to April 5, 2021.[1] (Interim Final Rule, 85 Fed. Reg. 70064, 70068 (Nov. 4, 2020)). This extension provides additional time for health care actors to revise their policies, procedures, and operations to comply with the information blocking regulations. To assist health care actors with this process, our follow-up article analyzes four common information blocking compliance challenges faced by health care actors today. (For more information on information blocking and common compliance challenges, please listen to our podcast).

Compliance Challenge #1: Scope of EHI That Must Be Shared.

The Department of Health and Human Services (HHS) has repeatedly emphasized the need for interoperable health information technology to enhance patient care across medical platforms. The information blocking rule published by the Office of the National Coordinator for Health Information Technology (ONC) (the "Information Blocking Rule") seeks to promote data interoperability by encouraging access, disclosure, and use of electronic health information (EHI). The Information Blocking Rule's focus on EHI has inevitably spawned questions regarding the *scope* of EHI that health care actors must

Practice Areas

Health Care

Privacy, Cyber & Data Governance

make readily accessible by April 5, 2021.

In an effort to phase-in compliance, ONC has initially limited the definition of EHI to only those data elements represented in the United States Core Data for Interoperability (USCDI) until October 6, 2022.[2] (*Id.* at 70069). Because the majority of USCDI data elements are captured in 2015 Edition certified electronic health record (EHR) systems, most health care actors will be accessing and disclosing data elements already contained within their EHR system for the initial phase of compliance. Beginning on October 6, 2022, however, the definition of EHI expands beyond the USCDI data elements to encompass all electronic protected health information (as defined in the Health Insurance Portability and Accountability Act (HIPAA)) that is included in a designated record set (excluding psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding). (45 C.F.R. § 171.102; Interim Final Rule, 85 Fed. Reg. at 70069; *see also* Information Blocking Rule, 85 Fed. Reg. 25642, 25803-04 (May 1, 2020)).

While ONC has temporarily restricted the definition of EHI until October 6, 2022, it nonetheless encourages health care actors to share as much relevant EHI as possible in response to a request (indeed, ONC believed the USCDI elements would be too limiting in the long-run for data that is capable of exchange). (*See* Information Blocking Rule, 85 Fed. Reg. at 25804). Accordingly, health care actors should consider building and enhancing their data exchange capabilities early to incorporate non-USCDI elements prior to October 2022. This will ensure that health care actors have properly tested their retrieval and exchange systems well in advance of the deadline. As October 6, 2022 approaches, we anticipate seeing more industry guidance on compliance with the EHI definition.

Compliance Challenge #2: Inclusion of Data From Legacy Systems.

Although ONC has explicitly limited the data sets that health care actors are required to make accessible on April 5, 2021, it has not yet directly addressed whether health care actors must retrieve EHI from legacy EHR systems. As written, the Information Blocking Rule requires retrieval of all EHI that contains USCDI data elements through October 6, 2022. While this requirement does not expressly mention legacy EHR systems, the spirit and intent of the Information Blocking Rule is to provide patients with timely access to their EHI. (Information Blocking Rule, 85 Fed. Reg. at 25642-44). This means that ONC likely expects health care actors to retrieve and disclose all EHI containing USCDI elements on April 5, 2021, even if such EHI resides within a legacy EHR system. Health care actors should therefore begin developing protocols, policies, and procedures to provide access to and disclosure of EHI within *all* of their electronic systems. (*See id.* at 25792). To the extent a legacy EHR system contains non-USCDI elements, ONC would likely expect the health care actor to retrieve and disclose those data elements beginning on October 6, 2022.

The difficulty with legacy EHR systems, however, is that oftentimes the extracted data may not present in an easily exchangeable format. If this occurs, health care actors should evaluate whether one of the exceptions to the information blocking prohibition would permit withholding the EHI or disclosing it in an alternate format. For example, the infeasibility exception applies when a health care actor cannot fulfill a request to access, exchange, or use EHI due to a natural or human-made disaster (or other qualifying event), or due to the provider's inability to segment health data that can be disclosed from health data that must be withheld. (45

C.F.R. § 171.204). Alternatively, the content and manner exception permits health care actors to disclose EHI in an alternative format if the actor is "technically unable" to fulfill the request in the specified manner. (*Id.* § 171.301). Health care actors should analyze and apply these exceptions as needed.

Finally, the question presents as to whether health care actors must migrate EHI from legacy systems to new EHR systems. At present, the Information Blocking Rule does not require migration of EHI from legacy systems into a health care actor's current EHR system. However, ONC has noted that the migration of EHI into newer EHR systems produces cost savings and increases quality, efficiency, and security. (Information Blocking Rule, 85 Fed. Reg. at 25910). Retaining legacy or outdated EHR systems can increase connection and system integration costs and inhibit increased efficiency. (*Id.*) Unsurprisingly, ONC perceives the retention of legacy systems as encouraging market fragmentation by prolonging backwards compatibility of newer products to legacy systems. As such, ONC advises sunsetting non-compliant technology in 2022. (*See id.* at 25794). We anticipate that ONC may issue future guidance or rulemaking focused on integration of EHI from legacy systems into current EHRs.

Compliance Challenge #3: Scanned Records From Other Providers.

Health care providers commonly obtain or receive copies of a patient's medical record from numerous sources, including other health care actors. These documents are then scanned into the provider's system and become part of the EHI maintained within the EHR system. A compliance question arises as to whether such scanned data must be available for access, use, and disclosure, even if a health care actor cannot verify or vouch for the quality of the data.

ONC has clearly stated that EHI may not be withheld on the sole basis that it was generated outside the health care facility. As long as the EHI has been incorporated into the health care actor's EHR system, such data likely falls within the definition of EHI, regardless of its origin. That said, ONC has recognized that EHI received from an outside source may require pre-processing to attain a level of accuracy that allows the data to be safely used and disclosed for patient care. (*Id.* at 25832). Under these circumstances, the preventing harm exception to ONC's information blocking requirements allows a health care actor to perform special processing to ensure records are accurately matched, even though such practices may delay data integration and availability. (*Id.*).

Compliance Challenge #4: Confidentiality Agreements and Business Associate Agreements.

Finally, health care actors that are subject to HIPAA routinely enter into downstream contractual relationships that involve the use and/or disclosure of EHI to a third party. Such relationships are often accompanied by a Business Associate Agreement (BAA) or other confidentiality agreement. The language within such agreements is designed to minimize and restrict the use and disclosure of protected health information to its narrow and limited purposes under the contract. These historically permissible contractual restrictions on the use, disclosure, and exchange of EHI, however, can slow (or stop) the sharing of electronic health information, and as such, may now constitute information blocking. Accordingly, Business Associate Agreements must now be reviewed and analyzed under both HIPAA and the new Information Blocking Rule.

Since parties to a BAA may be subject to information blocking allegations and liability under the Information Blocking Rule, (*id.* at 25812), all health care actors should evaluate their current and template confidentiality agreements and BAAs to ensure no provision could be read as impermissibly withholding or delaying the disclosure of EHI. For example, agreements that have bans or limits on EHI disclosure should be scrutinized with particular attention to the Information Blocking Rule's requirements, as should the time periods within which such disclosures must be made. The goal of each BAA and/or confidentiality agreement review is to ensure that the agreement will facilitate use, disclosure, and exchange of EHI as timely as possible under the circumstances, while also complying with all of the HIPAA requirements. To further this goal, health care actors may consider incorporating language into their confidentiality agreements and BAAs that promotes the underlying goals of the Information Blocking Rule, such as provisions that demonstrate a commitment to enhancing interoperability and supporting the rapid access, use, and exchange of EHI. Finally, health care actors should also anticipate that their upstream contractors may issue revisions to confidentiality terms and BAAs over the next several months, all of which should be reviewed by the company's legal and compliance departments to ensure compliance with the dual goals of HIPAA and the Information Blocking Rule.

Conclusion

Legal and compliance challenges will continue to arise and evolve during and after the initial implementation phase for the Information Blocking Rule. We are here to answer additional compliance questions and hope to see you at our December 10, 2020 webinar, sponsored by the Health Care Compliance Association, on Information Blocking: Compliance Challenges, Answers, and Strategies for Risk Mitigation.

---

[1] The Department of Health and Human Services' interim final rule is titled "Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency." The rule is open for comment for 60 days following publication in the Federal Register, i.e., until January 4, 2021.

[2] Prior to the compliance deadline extension, ONC limited the definition of EHI to the USCDI elements until May 2022.