Health Law Connections
October 2020

Balancing the New Interoperability Rules with Existing Privacy Laws: Challenges for Payers

Jodi Daniel, Crowell & Moring LLP
Alice Hall-Partyka, Crowell & Moring LLP

This article is brought to you by AHLA's Payers, Plans, and Managed Care Practice Group.

Amidst the crises, changes, and new opportunities caused by COVID-19 and while regulatory attention focuses on promotion of telehealth, a tidal wave is about to crash on well-established, 20-year-old health data practices. That wave is interoperability and the liberation of health data into the hands of patients, technology companies, and others that have long been blocked or discouraged from accessing such data because of data holders' practices—including health plans and other payers.

The 21st Century Cures Act (Cures Act),[1] a bipartisan bill signed into law in 2016, included provisions to advance interoperability; support the access, exchange, and use of electronic health information (EHI); and prohibit information blocking, meaning any practice that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. The U.S. Department of Health and Human Services (HHS) released final regulations that are intended to support interoperability—the Office of the National Coordinator for Health Information Technology (ONC) rule that implements the Cures Act and a companion Centers for Medicare & Medicaid Services (CMS) rule that advances the goals of the Cures Act by leveraging other statutory authority.

With the regulations finalized, payers, among other actors, will need to take substantial action to implement the new requirements. A broad range of payers may find themselves within the purview of the new restrictions on information blocking and requirements on electronic data access and will need to review and update existing agreements, policies, and practices. Further, payers participating in federally-funded health care programs, such as Medicare Advantage organizations, Medicaid managed care plans, and qualified health plans participating in federally-facilitated exchanges, will face the task of building new application programming interfaces (APIs) and developing policies regarding individual requests for information through third-party applications. In all these decisions and changes, payers will face difficult questions of how to comply with these new rules that require increased sharing of data without violating their existing obligations to safeguard the same information under the Health Insurance Portability and Accountability Act and regulations thereunder (HIPAA).

Interoperability Rules

On March 9, 2020, HHS issued two separate final rules on interoperability (Interoperability Rules): one by ONC, and the other by CMS. Together the Interoperability Rules represent sweeping and transformative changes to the expectations imposed on payers and other actors related to the access and transmission of patients' EHI. With these rules, HHS has stated that it is putting patients first and enabling an app economy by requiring easy electronic access via APIs to the patients' own EHI through the application of their choice.

ONC Rule

In an attempt to finish the job to promote health information technology (IT) and interoperability that began in 2009 with the HITECH Act,[2] and with that to improve health and health outcomes, ONC and Congress sought to promote modern technology to enable access to EHI and make practices that interfere with interoperability illegal. While interoperability has been technically feasible, policymakers understood that data holders engaged in practices that limited the interoperability of systems and prevented EHI from moving as intended. The term "information blocking" was used to refer to these practices. The 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule[3] (ONC Rule) implements provisions in Title IV of the Cures Act that impact data sharing and relationships among health care entities and with consumers, including by explaining the "actors" to whom the rule applies, the scope of EHI, practices covered by the law, and reasonable and necessary exceptions, which act as safe harbors. The information blocking aspects of the ONC Rule go into effect on November 2, 2020;[4] however, the Office of Inspector General will not enforce information blocking before finalizing its rules regarding enforcement. [We note that at the time this article was submitted, an Interim Final Rule that would extend the compliance date was under review by the Office of Management and Budget].

The Cures Act's information blocking provisions apply to health care providers, developers of certified health IT, health information networks (HINs), and health information exchanges (HIEs), all of which are defined as "actors" under the ONC Rule.[5] The Cures Act defines information blocking as a practice that is "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information."[6] It also requires a certain knowledge element to be met.[7] The ONC Rule defines the scope of activities that are considered information blocking. In the rule, ONC has finalized definitions for terms such as "access," "exchange," and "use."[8] Each of these finalized terms is important for determining whether a given practice may implicate the information blocking prohibition. To comply with the rules, it is critical to identify whether: (1) an entity is subject to the rule; (2) whether there is an "interference" in access to EHI; and (3) whether there is an exception or other facts and circumstances that would justify the practice as reasonable and necessary.

While payers are not in themselves "actors" under the regulation, many health plans may find themselves within the purview of the rule. Some payers may have affiliates or subsidiaries that are health care providers and others may develop software in-house. HINs and HIEs are defined based on the functions they engage in, regardless of how they are defined in the market. A payer (or its associated technology platform) could be an HIE or HIN if it "determines, controls or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information" among more than two unaffiliated individuals or entities, but only for a limited set of purposes drawn from HIPAA: treatment, payment, and health care operations.[9] For example, payers that provide care coordination activities could be HINs if they enable health care providers to share EHI with each other as part of this function.

The regulation also clarifies that the EHI to which the Cures Act's information blocking restrictions apply should be defined in the same way that electronic protected health information (ePHI) is defined in HIPAA, to the extent that ePHI would be included in a designated record set (DRS).[10] While ONC sought to align these new rules with the HIPAA rules, EHI applies to information whether or not the information is covered under HIPAA. De-identified data is not within the scope of the regulation. It is not clear, however, whether price information is included in EHI, but it seems unlikely to cover prices that are not tied to a specific individual given the limitation of EHI to data in a DRS. Until May 2, 2022, actors only will need to comply with the rule for EHI represented in a limited set of data elements represented in the U.S. Core Data for Interoperability Standard (USCDI) standard adopted by regulation.[11]

ONC details eight "exceptions" to the information blocking prohibition,[12] but the agency has shifted its general enforcement approach to treat these exceptions as "safe harbors." A practice that fails to meet all of the conditions of an exception is evaluated on a case-by-case basis, based on facts and circumstances, and does not receive guaranteed protection from civil monetary penalties or from appropriate disincentives by HHS.[13] While each "safe harbor" has detailed, specific requirements, the "safe harbors" generally protect health entities when a practice that limits data access is for purposes of harm prevention, individual privacy, security, infeasibility, and health IT performance improvements.[14] The exceptions for protecting privacy and security are limited. Specifically, if a disclosure is permitted under HIPAA, then it does not meet the privacy exception—even though it would be lawful under HIPAA to withhold that information. The entity is now required to provide access, exchange, or use. As a result, an entity can be in compliance with HIPAA but in violation of the information blocking rules.

Further, the safe harbors allow, in certain circumstances, for entities to limit the content and manner for accessing data, impose fees to recover reasonably incurred costs, and license interoperability elements (defined as a number of things ranging from a particular technology to a technical specification that might be necessary to access, exchange, or use EHI).[15] It is important for actors to analyze their practices and

document their policies in accordance with the exceptions or document the facts and circumstances that factor into each individualized determination.

The ONC Rule also updates ONC's Health IT Certification Program, which sets a baseline standard for functionality of health IT software. Some of the policy updates include adoption of the USCDI standard to replace the Common Clinical Data Set as the default set of data categories that health IT users should expect to be able to exchange; changes to the certification requirements for APIs; implementation of the Real World testing certification criteria for health IT developers with health IT models; and adoption of a condition of certification that protects communications related to certain protected subject areas.[16]

CMS Rule

For payers, the CMS rule may be of more critical importance as it applies directly to health plans. On the same day the ONC Rule was released, CMS released a companion rule on Interoperability and Patient Access (CMS Rule)[17] that requires payers participating in federally-funded health care programs to provide patients with easy access to their claims and encounter information, as well as certain clinical information, through third-party applications of their choice. Through this rule, CMS leveraged its authority over various payers—Medicare Advantage organizations, Medicaid and Children's Health Insurance Program managed care plans, state agencies, and qualified health plan issuers on federally-facilitated exchanges—to advance interoperability and patient access to EHI by imposing standards-based API access and use requirements.

Beginning on July 1, 2021,[18] payers in these federally-funded programs must implement and maintain an API to support patient access to their health information (Patient Access API) and make provider directory information available through a public facing provider directory API (Provider Directory API).[19] Both APIs must comply with the Health Level 7 (HL7) Fast Healthcare Interoperability Resources (FHIR) Release 4.0.1 standard and the payers' obligations under the HIPAA Privacy Rule.[20]

The Patient Access API requirement is intended to make payers use functionalities similar to CMS' Blue Button 2.0 model[21] and allow patients, their representatives, and any third-party apps designated by such patients and representatives to access claims and encounter information (including approved or denied adjudicated claims, encounters with capitated providers, provider remittances, and enrollee cost-sharing) and all clinical data (including laboratory results and medication information), if maintained by the payer.[22] Further, the rule requires payers to provide this API access to requestors no later than one business day after adjudicating a claim or receiving the clinical data from providers, including price-related information such as provider remittances and enrollee cost-sharing information.[23] Starting in 2022, these payers will be required to comply with patients' requests to send their clinical data, whether through

the Patient Access API or otherwise, inclusive of the elements defined in the USCDI version 1 data set, to other payers.[24]

CMS only allows a payer to deny or discontinue access to a third-party application in limited circumstances. Specifically, a payer can deny access "if the payer reasonably determines, consistent with its security analysis under 45 CFR part 164 subpart C, that allowing an application to connect or remain connected to the API would present an unacceptable level of risk to the security of protected health information on the payer's systems and the payer makes this determination using objective, verifiable criteria that are applied fairly and consistently across all applications and developers."[25] In the preamble to the rule, CMS further explained that the "only instance" that a payer could deny access to an application would be if the payer's own systems would be endangered by allowing the third-party application to access the API.[26]

As such, CMS has advised that efforts to prevent enrollees from using certain third-party applications "generally must stop at education and awareness or advice regarding concerns related to a specific app."[27] The rule does require that the payers provide educational resources for enrollees that, at a minimum, explain the general steps an enrollee can take to protect the privacy and security of the health information, including factors to consider in selecting a third-party application and the importance of understanding security and privacy practices of any application to which they entrust EHI, and include an overview of which entities are likely to be covered by HIPAA.[28]

The rule also requires that the payers make provider information available through a Provider Director API,[29] similar to the API with which qualified health plans in the exchanges already are required to comply.[30] The Provider Directory API must include the payer's network of contracted providers, including names, addresses, phone numbers, and specialties, updated no later than 30 calendar days after providers update their information with the plan.[31] Medicare Advantage organizations offering Part D plans also must offer the number, mix, and addresses of pharmacies in their networks.[32] It is expected that these APIs primarily will be used by third-party application developers.

The CMS Rule also finalizes important Conditions of Participation requiring the transmission of electronic admission, discharge, and transfer notifications by Medicare- and Medicaid-participating providers, including hospitals, psychiatric hospitals, and certain critical access hospitals, and enables CMS to publicly list certain providers that are determined to be engaged in information blocking.[33] Additionally, the rule will require states to share Medicare and Medicaid dual enrollee data on a daily basis with CMS.[34]

Challenges for Payers

To comply with the Interoperability Rules, payers will need to consider how best to build an API infrastructure and update existing policies, agreements, and business practices

to align with the new requirements. With each decision, payers may need to grapple with competing considerations: how can they protect the EHI of their enrollees while simultaneously ensuring that they increase access and availability for the beneficial exchange of information?

Interplay with HIPAA

As covered entities under HIPAA, health plans must walk a fine line between the HIPAA requirements and the new Interoperability Rules. EHI, as used in the ONC Rule, is defined with reference to the definition of ePHI in HIPAA, and therefore the prohibitions against information blocking apply to the same sets of health information that payers are obligated to protect and make available to patients under HIPAA.

Whereas previously plans had discretion to share ePHI for certain enumerated permissible purposes under HIPAA, actors, including payers that function as HIEs under the rule or that have health care providers, will now be mandated to share that information under the ONC Rule. ONC emphasizes that the ONC Rule does not require the disclosure of EHI in any manner that would not be permissible under HIPAA or other federal or state law. It goes on to state, however, that if HIPAA or any other law *permits* an actor to provide access, exchange, or use of EHI, then the actor is now *required* to provide that access, exchange, or use of EHI, assuming that the actor is not otherwise prohibited by law from doing so and no exception is available. This is a substantial change from current HIPAA rules, which require disclosures in only two situations: to individuals when requesting access to their own ePHI and to HHS to conduct an investigation.

Further, the information disclosure requirements under the CMS Rule also will significantly affect how payers consider and comply with their HIPAA obligations, particularly the individual's right of access to their ePHI. As health plans develop Patient Access APIs and respond to enrollees' requests for access to claims, encounter information, and clinical data, numerous implementation questions arise regarding the overlapping requirements. Under HIPAA, health plans are required to provide ePHI in a DRS to the individual, in the form and format requested by the individual, if feasible. Under the CMS Rule, payers must provide a subset of this information through APIs to all members. This essentially means that all payers will have an API form and format available with which to respond to individual requests for access. However, if individuals request their entire DRS under their right of access, the scope of their request would likely include some paper, PDF, or fax records, in addition to records kept in structured electronic format. This will likely increase the complexity of responding to individual requests and adds to payers' administrative burden. Unlike health care providers that have APIs as part of their certified electronic health records, payers generally do not have existing APIs and have to build this capability to meet the requirements of the CMS Rule, as well as internal policies and processes for facilitating these requests.

The CMS Rule is not clear on how best to make data available that is not in standard form, but rather in PDF or other unstructured electronic form, and whether providing data existing in PDF form is even required. Regarding the scope of data, under HIPAA, health plans only need to provide ePHI in a DRS, but under the CMS Rule, health plans have to provide clinical data that they "maintain," which may not be part of the DRS (e.g., clinical information collected for health care operations and not payment purposes). This has raised a number of questions about the scope of data that needs to be included in the Patient Access API under the CMS Rule and particularly whether clinical data that is accessed or stored for health care operations purposes must be included. Finally, under the CMS Rule, health plans must provide the requested information within one business day of receipt of clinical data or from the time of adjudication, rather than the 30 days permitted under HIPAA. The one business day time frame will be a challenge based on current operations and the various systems and stakeholders that currently exchange such data.

Payers should review and revise their policies and contracts to allow for patient access to data consistent with these new rules. They may also need to review their business associate agreements in light of these rules. Finally, payers will need to build technical capabilities and map data to specific standards required by the CMS Rule, which may be time-consuming and expensive. CMS acknowledges this cost and states that they assume that payers will increase premiums to pass these costs to patients but that the "benefits created by the Patient Access API outweigh the costs to patients if payers choose to increase premiums as a result."[35]

While payers will need to continue fulfilling all their obligations under HIPAA so long as they or their business associates have access to the ePHI, these obligations may be met, in part, by enabling access to EHI through a third-party application. CMS has advised that, once EHI is no longer under the control of the payer or its business associates, the data is no longer subject to HIPAA and the payer will not be responsible for breaches.[36] Instead, the Federal Trade Commission has enforcement authority over most third-party applications.

Requests from Third-Party Applications

Payers in federally-funded programs who are required to maintain a Patient Access API may want to restrict access to the API to certain verified third-party applications, but in fact can only deny requests to send EHI to third-party applications in limited circumstances. Under the CMS Rule, payers can only restrict a third-party application from accessing the Patient Access API if there is an "unacceptable" level of risk, meaning that the application could endanger the payer's API.

As such, the payers are very limited in their ability to reject requests from third-party applications and are not allowed to reject applications on purely discretionary bases, such as poor quality or user interface, or even based on the application's privacy practices. Further, payers cannot dictate what applications do with patient data once it is

transmitted to them. If an application has a known security problem or does not adequately describe its security or data practices in its privacy policy or attestation, a payer can warn the enrollee but cannot prohibit the enrollee from selecting that application to receive their data.

Payers are encouraged to look to CMS' own app review process, Blue Button 2.0, which involves a minimal level of review of applications. The initial approval process under Blue Button 2.0 is generally limited to a review of the applications' privacy policy and terms of services. On an ongoing basis, CMS may revoke an application's access for technical issues (such as high frequency of issuing queries that impacts the API performance). It does not, however, monitor the ongoing compliance of applications with the API's terms of service.

This lack of flexibility is strikingly different from the discretionary and more comprehensive ways that major technology industry players operate their application stores and review processes. Still, payers may be able to draw from the technical review steps that companies like Facebook and Apple have instituted to help ensure that applications will not inappropriately use their APIs.

At a minimum, payers must develop educational materials to educate and inform enrollees about privacy and security risks. Payers are required to provide educational materials to enrollees to help inform their decision about how to select a third-party application. These materials could include factors for enrollees to consider when making their selection, and whether or not an application has made certain attestations to the payer about its practices. Further, ONC outlines a detailed process for informing enrollees about privacy risks that may provide an opportunity for payers to present a "whitelist" of applications with strong privacy practices, while warning patients about applications that have weaker practices. It is possible to present this factual information to enrollees with a reasonable warning; however, there will be a fine balance between informing enrollees and being viewed by regulators as attempting to discriminate against certain applications or dissuade individuals from providing consent—particularly if those applications are competitors with the payer's own software.

Conclusion

The Interoperability Rules are designed to give patients better access to their EHI and to eliminate barriers between their payers, providers, and other entities that they interact with in the health care system. The increased sharing of information, however, also poses a significant risk to patients of breaches in their health data. And the Interoperability Rules' requirements create several challenges for payers who are trying to balance the competing interests of their enrollees' rights to privacy and desires for increased sharing of their health information.

These rules are complex and many actors and payers have questions about their applicability to specific scenarios. There is an expectation that HHS will provide guidance on the rules to address issues that arise as entities are determining their compliance. Given the potential penalties and the ambiguity, however, it is imperative that health plans carefully consider compliance and consult with counsel to consider how to comply absent guidance.

Endnotes

1. 21st Century Cures Act, Pub. L. No. 114-255 (Dec. 13, 2016).
2. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5 (Feb. 17, 2009).
3. 85 Fed. Reg. 25642 (May 1, 2020).
4. *Id.* at 25946 (to be codified at 42 C.F.R. § 170.101).
5. *Id.* at 25955 (to be codified at 45 C.F.R. §§ 171.101, 171.102).
6. Cures Act, *supra* note 1, § 4003 (implemented at 42 U.S.C. § 300jj).
7. If conducted by a health IT developer, an HIE, or HIN, the Cures Act considers a practice to be information blocking if the actor knows or should know that the practice is likely to violate the restriction; if conducted by a health care provider, the practice is information blocking if the provider knows the practice is unreasonable and likely to violate the restriction. *Id.* See also 85 Fed. Reg. at 25956 (to be codified at 45 C.F.R. § 171.103).
8. *Id.* at 25955-56 (to be codified at 45 C.F.R. § 171.102).
9. *Id.* at 25955-56 (to be codified at 45 C.F.R. § 171.102).
10. *Id.* at 25955 (to be codified at 45 C.F.R. § 171.102).
11. *Id.* at 25956 (to be codified at 45 C.F.R. § 171.103). See Off. of the Nat'l Coordinator for Health IT, USCDI v1 Summary of Data Classes and Data Elements, HealthIT.gov, https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.
12. 85 Fed. Reg. at 25956-61 (to be codified at 45 C.F.R. §§ 171.200-303).
13. *Id.* at 25819-20.
14. *Id.* at 25956-59 (to be codified at 45 C.F.R. §§ 171.200-205).
15. *Id.* at 25959-61 (to be codified at 45 C.F.R. §§ 171.300-203).
16. See *id.* at 25939-55.
17. Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organization and Medicaid Managed Care Plans, State Medicaid Agencies, CHIP Agencies and CHIP Managed Care Entities, Issuers of Qualified Health Plans on the Federally-Facilitated Exchanges, and Health Care Providers, 85 Fed. Reg. 25510 (May 1, 2020).
18. The rule includes an implementation date of January 1, 2021. However, because of the COVID-19 public health emergency, CMS will not enforce the new requirements until July 1, 2021. Ctrs. for Medicare & Medicaid Servs., CMS Interoperability and Patient Access Final Rule (Apr. 21, 2020), https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index.
19. 85 Fed. Reg. at 25513.
20. *Id.*
21. See *id.* at 25515, 25522-23.
22. *Id.* at 25632 (to be codified at 42 C.F.R. § 422.119), 25635 (to be codified at 42 C.F.R. § 431.70); 25636 (to be codified at 42 C.F.R. § 457.730), 25638 (to be codified at 45 C.F.R. § 156.221).
23. *Id.*
24. *Id.*
25. *Id.*
26. *Id.* at 25518.
27. *Id.*

28. *Id.* at 25632 (to be codified at 42 C.F.R. § 422.119), 25635 (to be codified at 42 C.F.R. § 431.70); 25636 (to be codified at 42 C.F.R. § 457.730), 25638 (to be codified at 45 C.F.R. § 156.221).
29. *Id.* at 25633 (to be codified at 42 C.F.R. § 422.120), 25634 (to be codified at 42 C.F.R. § 431.60); 25637 (to be codified at 42 C.F.R. § 457.760).
30. *See* 45 C.F.R. § 156.230(b).
31. 85 Fed. Reg. at 25633 (to be codified at 42 C.F.R. § 422.120), 25634 (to be codified at 42 C.F.R. § 431.60); 25637 (to be codified at 42 C.F.R. § 457.760).
32. *Id.* at 25633 (to be codified at 42 C.F.R. § 422.120).
33. *Id.* at 25637-38 (to be codified at 42 C.F.R. §§ 438.24, 485.638), 25514.
34. *Id.* at 25634 (to be codified at 42 C.F.R. § 423.910).
35. *Id.* at 25528.
36. *Id.* at 25518. *See also* U.S. Dep't of Health and Human Servs., HIPAA FAQ 3011, https://www.hhs.gov/hipaa/for-professionals/faq/3011/where-an-individual-directs-a-covered-entity-to-send-ephi-to-a-designated-app-does-a-covered-entitys-ehr-system-developer-bear-liability.html.