COSMOS
Navigate the Compliance Universe

Compliance Today - May 2022
Patient information access automated with the Cures Act

By Kelly McLendon, RHIA, CHPS

Kelly McLendon (kmclendon@complianceprosolutions.com) is Sr. VP Compliance and Regulatory Affairs, CompliancePro Solutions, Exton, PA.


Kelly McLendon

United States healthcare professionals and patients stand upon the cusp of unprecedented, burdensome regulatory changes that will affect automation and how we manage access to patient information while maintaining privacy and security. The 21st Century Cures Act (Cures Act) information-blocking and interoperability regulations are complex, unprecedented, and intertwined with the HIPAA rules.[1] However, diligence in studying the new rules, the government's online guidance, and educational materials such as this article will provide clarity for healthcare providers on how to implement and what automation technology may be used to relieve some of the burdens.

Regulations spur change

The Cures Act from Office of the National Coordinator for Health Information Technology (ONC);[2] Centers for Medicare & Medicaid Services (CMS) final rule;[3] the expected HIPAA final rule;[4] the Coronavirus Aid, Relief, and Economic Security Act;[5] and 42 C.F.R. Part 2 (substance abuse) rules will significantly affect how we manage electronic patient health information. We have a fair amount of guidance and new tools developed, like the Trusted Exchange Framework and Common Agreement,[6] a sample health information exchange trust agreement issued by governmental regulators. However, we have almost no professional practice to learn from, and vendor stakeholders are only now getting their updates and certifications implemented. Therefore, best practice development will follow and will probably take a few years to mature.

Rarely have standards and protocols been published by the government mandating the use of specific healthcare automation approaches to promote access to and exchange of patient information. The 21st Century Cures Act refers to persons and companies subject to those rules as "actors," reflecting a wider scope of parties that can or must access and exchange patient health information. Such access and exchange will become much more commonplace among not only HIPAA entities (e.g., providers and payers), but also non-HIPAA entities such as personal health, mobile health (e.g., smartphone based), and related digital apps, along with innumerable other third parties and their applications that have a stake in healthcare processes involving patients, providers, and payers.

Be aware that these rules cover more than just access by patients to their information. They will address all use cases where actors that exchange patient information will be able to use the rules to manage their requests for most uses for patient information, even if the patient is not directly involved in the transaction. Not allowing appropriate electronic health information (EHI) access, use, or exchange could invoke the new information-blocking rules from the ONC. Today, these rules only have appropriate disincentives for enforcement, but will soon invoke with direct penalties.

Patient's PHI is also EHI

In addition to HIPAA's definition of protected health information (PHI),[7] under the Cures Act, EHI[8] is defined as electronic protected health information contained within a patient's designated record set that may reside within or outside a HIPAA entity. It can be confusing when two different agencies use two different terms for the same basic concept, one of which is derived from the other, but with incomplete synchronization. The Cures Act uses the term "electronic protected health information" only in reference to the definition of EHI, making it unclear what constitutes a designated record set outside of the HIPAA entity.

While industry groups have been working to define the relationships of the HIPAA designated record sets[9] as used by the Cures Act as part of the EHI definition, what makes up a designated record set outside of a HIPAA entity is unclear. Hopefully, more guidance will be forthcoming from the ONC, but also with the expected HIPAA final rule.

Incomplete clarification of what constitutes a designated record set under either the Cures Act or HIPAA rules hampers automation of the components needed to allow large portions of the current processes to be treated with automation. The primary target (all of which are actors) of many of the Cures Act rules are electronic health record (EHR) vendors, which must be certified to perform certain automations, including HL7® Fast Healthcare Interoperability Resources (FHIR®) application programming interfaces (APIs)[10] and EHI exports.[11] CMS also invokes these rules for payers, which do not have certified systems and must create such automations within their own systems.

Healthcare providers' EHR vendors are charged with providing Cures Act–compliant APIs and exports of EHI—requirements that, if failed, could render a vendor's EHR not certified, which few providers can afford from revenue, compliance, or risk perspectives. Therefore, the providers should already be well down the path toward implementing whatever software tools addressing the Cures Act compliance their EHR vendors are able to provide. There may be some costs to healthcare providers involved in using these new Cures Act components within an EHR, but they are included in the Cures Act rules about what costs and licensing may be charged. In general, certified EHR vendors are not allowed to put up unreasonable barriers in the way of their customers using the Cures Act tools they provide as a part of their certified EHR products.

Conversely, payers do not leverage federally certified systems to manage their patient records. Instead, they are using their own systems, mostly custom built and different from the other payers. Under the CMS interoperability and patient access rule of the Cures Act, the payers also will have to provide for the FHIR API and EHI export functionalities from within their systems.[12] There are many parties besides patients that may wish to easily access, with proper authentication, the patient's claims and revenue cycle documentation. Therefore, these new functionalities are being created and will be implemented by each payer.

HIPAA a barrier

HIPAA has often been accused of being a barrier that prevents disclosures of patient information, mostly as a byproduct of misunderstanding its complex rules. The net effect was to limit the free exchange of patient information to authorized or otherwise permissible parties and to make the visions for data exchange difficult to achieve. The expected HIPAA final rules, synchronizing them with the Cures Act, along with various 42 C.F.R. Part 2 substance abuse rule changes, are anticipated to help reduce these HIPAA barriers. Under the Cures Act ONC rules, failure to provide requested records will require the invocation of one of eight information-blocking exceptions, found at 45 C.F.R. Part 171 . Best practices illustrating how to manage HIPAA requests with information-blocking exception invocation and perhaps revocation is yet to be determined in the marketplace.

The intention of the Cures Act rules is not to reduce the importance of HIPAA, although relieving some of the burdensome aspects of HIPAA is a goal. The idea behind the rules is to create process automation affecting large percentages of the patient information access, copies, and exchange requests to be allowed to proceed with little or no human intervention. The scope of these impacts is potentially staggering, with automation used to capture, disseminate, and store patient information that may no longer be under the HIPAA aegis. Without HIPAA protections for health information, the probability of breach and risk will be elevated.

Balancing act

For compliance professionals, there is going to be a great balancing act between the protections provided by HIPAA for patients' information and the Cures Act rules that are intent on opening access to that information. At this point, the most important aspect of the new rules may be the automation of patient access and record management. How and when the vendors (both EHR and ONC-complying non-EHR) plan to deliver their certification-required functionality will need to be discussed by the providers as soon as possible.

Recently, patient information access, copies, and exchanges were only provided for or during treatment, payment, and operations purposes as a patient right of access, as part of a business associate's services for a covered entity, or upon authorized disclosure with certain exceptions. There has been a high standard for proving who is requesting the information and ensuring breaches do not occur. The processes to fulfill access to the patient information requests were and remain manually executed due to a lack of automation from less-than-optimal interoperability, the presence of hybrid paper/electronic records, and the lack of a mandate for more automated exchange of the information. These manual processes are ripe for automation, with their efficiency and speed advantages, but they needed the leverage of federal law to be realized. EHRs will increase their certified automation, as will systems that hold other designated record set patient information. Other vendors will provide compliance-type automation to manage the new processes and reduce that risk. Repetition of access may be reduced with robotic process automation and similar technologies.

Automation of Cures Act processes

Beyond the creation of increased interoperability with APIs and EHI exports, automation points evolving from the new rules include information-blocking incidents and complaint investigations, requests related to interoperability and patient access, patient education for digital/mobile health apps, and similar applications of automation and artificial intelligence. In some ways, new automation applications introduced into the marketplace have become makeshift solutions to assist with managing HIPAA compliance. Interactions of the Cures Act and HIPAA will make compliance more complex, even if eventually it becomes easier to exchange EHI.

Even though the execution of aspects of the Cures Act using information blocking, interoperability, and patient access is not fully visible, implementation is progressing at different paces in differing organizations. There has not been a lot of fanfare surrounding the dates and responsibilities, which reflects a measured approach by the regulators to implementing such a complex mass of new rules. The dates for these rules regarding implementation are complex and will require each organization to work with their records management, compliance, legal and IT staff, and their vendors (especially EHR) to determine the dates they must be compliant.

As these rules are implemented, and with some vendors already releasing their capability for patient information access, there has been significant growth of health information exchanges and networks of patient information. Entirely new applications and services will be required to serve the demand for patient information that will continue to arise. Crucial questions remain as to when and how the vendors will deliver the functionality required for EHI requests and delivery via automated means.

We, as an industry composed mostly of healthcare providers and payers, are only now beginning to see the

changes these rules will introduce into our daily health information management practices. The changes will continue to grow as more guidance is released, the new HIPAA rules are issued, and where and how automation can be introduced into current practices is better determined. Best practices will eventually settle into a new normal, which will in some cases, such as requesting patient information from another provider for treatment purposes, be markedly changed. We must remember the Cures Act rules also will facilitate migration from one EHR to another, removing the barriers put up by EHR vendors to keep such migrations from happening. The result should be good for patient safety as increasingly more information will be available within the primary system being used to manage patient treatment.

Potential issues

In theory, the patients will control the use of their information, but that may be a difficult task, there being so many applications, each with its own privacy notices, user agreements, etc. There will likely be many process changes for actors as to how they allow for and manage patient information access, exchange, use, and storage. The U.S. Department of Health & Human Services believes a widened scope of patient information exchange is warranted to improve patient healthcare quality—primarily from EHI access but also availability for advanced processing such as artificial intelligence—save monies, and accept all the positive benefits that automation and reduction of barriers will foster.

Expanded access, use, and exchange mean that shortly the very controlled environment of the release of patient information will be available to patients and many others with easy, automated, online access to the patients' EHI. For example, patient personal healthcare applications, such as one on a smartphone or watch, will be able to gather patient EHI and provide access to others (hopefully ruled by privacy notices that the patients read and use when authorizing access). Such ease represents a quantum shift for patient health information accessibility, exchange, and usefulness.

Throughout the rise of our mobile society, there have been issues with users not appropriately applying privacy protections in their personal applications. If this becomes the case within the automation of a patient's EHI, such behavior will lead to even more movement of the patient's EHI to third parties not regulated under HIPAA with the Office for Civil Rights enforcement. Failure to have an adequate enforcement presence from both federal and state regulators can portend increased privacy misuse of the EHI. Not only will more parties have the patient EHI, but the failure of the patient to properly control the applications through their privacy notices (if any control is indeed possible) could allow the EHI to get loose on the internet.

The risks to the privacy of patient information will increase as patient EHI propagates to other parties. There may be more incidences of privacy issues and breach allegations arising unless the EHI is directly sourced from a covered entity or business associate under HIPAA. These violations and breaches outside of HIPAA will only have the very rare Federal Trade Commission enforcement (its recent notice to the contrary),[13] which offers far less protection for these patients than HIPAA. But such is the nature of the new rules: more access will lead to more misuse. It is time to allow automation to run at full speed and fully gain the achievable benefits for patient safety and cost savings.

FHIR API and EHI export timeline

According to the API functionality and EHI export capability timeline[14] published by the ONC, the FHIR APIs (and their associated directories) are due at the end of 2022, but the EHI export, including the entire designated record set within the EHR system, is not due until the end of December 2023. This gap has given rise to numerous questions being raised by providers, payers, and the actors involved in executing the rules with best practices. Questions have arisen as to how to be compliant if the EHR automation is not in place. The prevailing thoughts

are similar to the process below, which is given as an example only.

- October 6, 2022: Requests for access need to include, if requested, the entire EHI data set as denoted within the organization's designated record set.
- December 31, 2022: EHR vendors must be certified to offer FHIR APIs actors use to make patient EHI requests. Some will be ready sooner, some may be late, all will vary on what patient information they will return based on the request.
- December 31, 2023: The EHR vendors will have to be certified to be able to export a single patient's entire designated record set (if requested).
    - Related but for a different use case (e.g., EHR transition), the EHRs will also have to provide an export of the entire universe of patient's EHI within that EHR.
- So, if technology is not capable of exporting the entire designated record set if requested, what should be implemented as a practice perspective?
    - It seems likely a content and manner exception will have to be invoked if conditions are met. The content and manner exception allows for a negotiation with the requestor as to the electronic format to deliver what cannot be delivered with the EHR export.
    - If that does not result in an agreed-upon solution, the actor (provider or payer, typically) may invoke the infeasibility exception.
    - There will be processes surrounding tracking which exception is used for which case and any incidents that may arise from complaints, especially to the Office of Inspector General information blocking complaint portal.

In general, there is so much uncertainty in the marketplace about when and how to implement the Cures Act that there is uneven knowledge and planning about how and when to implement these rules. Given that the ONC and its Office of Inspector General enforcers don't seem to be pushing too hard yet, it is unknown when enforcement will start to drive the compliance with the Cures Act of actors like payers and providers. However, even though there is uncertainty in how to move ahead, no organization is relieved from working to implement the rules diligently and begin to use such processes as soon as possible—especially given that the Office of Inspector General has opened its information blocking complaint portal.

Conclusion

Preparation for and implementation of technology to assist with compliance of the Cures Act should be a key area of attention for healthcare compliance managers over the next few years. Certified EHR vendors' (and other related noncertified record management vendors') capabilities are only beginning to be exposed. Professional best practices have not yet arisen, federal guidance is limited, and enforcement experience does not exist as of yet. The best advice at present is to work with your vendors, not just EHR, but all that have electronic records within your designated record sets. Also, review the federally provided educational and rules-based websites to gain as much knowledge as possible, because the implementation will have dramatic effects on the creators of patient information, along with the patients themselves. The rules should be used to facilitate the goodness that is projected to occur; protect your organization; and work toward compliance, which will reduce incidents, complaints, and investigations.

Takeaways

- The new 21st Century Cures Act is a complex set of rules from the Office of the National Coordinator for Health Information Technology and Centers for Medicare & Medicaid Services.
- 21st Century Cures Act rules intertwine with HIPAA and are correspondingly complex, requiring detailed implementation and compliance.
- Industry best practices have yet to evolve to assist implementation and professional compliance practices.
- Healthcare providers must work with their certified electronic health record vendors to understand the capabilities and limitations of their technology related to electronic health information export, application programming interfaces, and patient information access.
- Consider what types of automation other than patient access may be necessary to assist in 21st Century Cures Act compliance.

1 21st Century Cures Act, Pub. L. No. 114-255, §§ 4003, 4004, 130 Stat. 1033, 1165, 1176 (2016).
245 C.F.R. §§ 170, 171 .
3 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. 25,510 (May 1, 2020) .
4 Proposed Modifications to the HIPAA Privacy Rule To Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 85 Fed. Reg. 6,446 (January 21, 2021) .
5 Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, § 3221, 134 Stat. 281, 375 (2020).
6 "Trusted Exchange Framework Common Agreement (TEFCA)," HealthIT.gov, accessed March 9, 2022, https://www.healthit.gov/topic/interoperability/trusted-exchange-framework-and-common-agreement-tefca.
745 C.F.R. § 160.103 .
845 C.F.R. § 171.102 .
945 C.F.R. § 164.501 .
10 Office of the National Coordinator for Health Information Technology, "CURES ACT FINAL RULE: Standards-based Application Programming Interface (API) Certification Criterion," March 2020, https://www.healthit.gov/cures/sites/default/files/cures/2020-03/APICertificationCriterion.pdf.
11 Office of the National Coordinator for Health Information Technology, "§170.315(b)(10) Electronic health information export," March 2019, https://www.healthit.gov/sites/default/files/page/2019-03/170_315b_10_Electronic_health_information_export.pdf.
12 Medicare and Medicaid Programs; Patient Protection and Affordable Care Act; Interoperability and Patient Access for Medicare Advantage Organizations 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, 86 Fed. Reg. 70,412 (December 10, 2021) .
13 Federal Trade Commission, "Statement of the Commission On Breaches by Health Apps and Other Connected Devices," September 15, 2021, https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_
14 Office of the National Coordinator for Health Information Technology, "New Applicability Dates included in ONC Interim Final Rule," October 2020, https://www.healthit.gov/cures/sites/default/files/cures/2020-10/Highlighted_Regulatory_Dates_Certification.pdf.