Balancing Patient Access and Privacy

The Impact on healthcare providers and their patients of the March 9, 2020 Office of The National Coordinator (ONC) Final Rule

Authors:

Rita Bowen, MA, RHIA, CHPS, CHPC, SSGB
Vice President, Privacy, Compliance and
HIM Policy, MRO

Sue Chamberlain, MSCTE, RHIA, CDIP,CCS-P
Vice President, Compliance and Education, RRS Medical

Jaime James, MHA, RHIA
Senior HIM Consultant, Legislative Policy and
Compliance, MMRA

TABLE OF CONTENTS

GLOSSARY OF TERMS

API Maintenance of Certification Requirements — addresses ongoing requirements that must be met by Certified API developers in order to remain in good standing under the ONC Health IT Certification Program.

Electronic Health Information(EHI) — Refers to patient data stored in electronic form that are collected and shared for healthcare delivery and public health purposes.

Information Blocking — Information blocking is defined as the intentional withholding (a practice that is likely to interfere with, prevent or materially discourage access, exchange or use) of patient health information by an actor either from provider to provider, or from provider to patient**.** Info blocking rules apply to portals and apps but not to information received from HIM or an ROI vendor.

Interoperability — the ability of computer systems, devices or software to exchange and make use of information.

On-Demand Access — Refers to patients directly accessing electronic health information through an app or portal.

USCDI — United States Core Data for Interoperability (USCDI) is a standardized set of health data classes and constituent data elements for nationwide, interoperable health information exchange.

BALANCING PATIENT ACCESS AND PRIVACY

About this white paper

This white paper provides insights, education and strategies to help hospitals, health systems and other healthcare provider organizations balance the government's imperative to increase patient access, as described in the March 9, 2020 ONC Final Rule, with the necessary oversight to ensure patient privacy.

The recommendations in this paper are designed to serve as a guide for health information management (HIM) professionals, inhouse attorneys and compliance officers as they work to utilize the influx of new technology tools that enhance patient access to medical records without compromising privacy.

Background

The Centers for Medicare & Medicaid Services (CMS) and the Office of the National Coordinator for Health Information Technology (ONC) on March 9, 2020, released separate but related final rules addressing interoperability, information blocking, patient access to data and electronic health record (EHR) certification criteria. The Final Rules expand on the policies promulgated in the 21st Century Cures Act (Cures Act), directing ONC and CMS to develop policies that foster the interoperable exchange of health information between stakeholders.

These rules comprise some of the most extensive new healthcare data sharing policies that the federal government has ever implemented, requiring both public and private entities to share health information between patients and other parties. That said, this paper will focus specifically on the significant concerns about patient privacy and security that are raised by the ONC Final Rule and it will describe how stakeholders can mitigate those risks.

The Goal of the ONC Final Rule

The ONC Cures Act Final Rule implements interoperability and information blocking requirements outlined in the 21st Century Cures Act. The Act aims to put patients in charge of their health records which is a key piece of Health and Human Services (HHS) work toward a value-based health care system.

The ONC Final Rule enables the health care delivery system to deliver an “app economy” that provides patients, physicians, hospitals, payers and employers with innovation and choice. Through the delivery of modern smartphone and software apps, patients and providers will see benefits in accessing electronic health information (EHI). Patients will have more convenient and easier options to gain on-demand access to their EHI whenever and wherever they need it. In addition, there will be the increasing ability for patients to choose apps that will assemble and read their records.

Providers will be able to make patient information available through application programming interfaces (APIs) in a low-cost, automated way and without “special effort” saving them time and money. Providers will benefit from a competitive app market place. Improved interoperability allows different information systems and applications to connect and remove barriers that prevent patients electronic access to their health information. Patient's use of third-party applications or devices of their choice will improve continuity of care and data exchange across systems to provide the best healthcare outcomes for individuals as well as the communities.

Meaningful Use efforts have evolved into the 'promoting interoperability program' as CMS focuses on improving the exchange of healthcare data, as well as patient access. Patients and caregivers often have medical decisions (the type of care, the place of care) made for them by third parties. The intent is to provide patients with the power of information through apps and other methods that ensure portability of their electronic health information (EHI). Healthcare providers and their Healthcare IT modules i.e., EHRs are required to provide access to EHI as well as the ability to push that EHI to third-party sources, as requested by the patient to support better outcomes.

Currently, access to records is managed by an organization's release of information (ROI) department or an ROI vendor. In recent years, EHR patient portals have become an additional source of data but the information is limited and, in some cases, incomplete. However, the new rule will most likely escalate portal access (electronic access) to a level that will most likely influence the request process for patients.

Access to **data** is different than access to **records.** Data is a much broader definition encompassing an entire patient snapshot but can stand on its own outside the system as well. Records need to be attached to a specific patient to make sense.

The exchange of patient information between providers has also evolved with the use of EHR’s. The new rule will likely simplify access to patients’ healthcare history, which should positively impact care, as well as reduce traditional continuity of care ROI requests.

The changes in the Certification Criteria that are part of the May 9, 2020 ONC Final Rule will assist stakeholder vendors in meeting the needs of the industry with set standards and protocols.

Information blocking: Who, What & When

Information Blocking Applies To

Yes	No	
☑	□	Health Care Providers
☑	□	Health IT Developers of Certified Health IT
☑	□	Health Information Networks or Health Information Exchanges
□	☑	Business Associates

The Information Blocking provisions apply to specific “actors.” The 'actors' in the new rule are defined as Health Care Providers, Health IT Developers of Certified Health IT, and Health Information Networks (HIN) or Health Information Exchanges (HIE). Business Associates are not considered actors and thus are not subject to the Information Blocking rules.

Information blocking is defined as the intentional withholding (a practice that is likely to interfere with, prevent or materially discourage access, exchange or use) of patient health information by an actor either from provider to provider, or from provider to patient. This definition has some industry experts questioning what exactly qualifies as “intentional.” The ONC final interoperability rule tried to clarify that definition by defining eight exceptions that will not be considered information blocking.

Eight Information Blocking Exceptions

Exceptions that involve not fulfilling requests to access, exchange, or use EHI

1. Preventing Harm Exception
2. Privacy Exception
3. Security Exception
4. Infeasibility Exception (has a 10 day response requirement)
5. Health IT Performance Exception

Exceptions that involve procedures for fulfilling requests to access, exchange or use EHI

6. Content and Manner Exception
7. Fees Exception
8. Licensing Exception

Generally, the effective date for the certification portion of ONC's Final Regulation is 60 days after publication in the Federal Register, which was May 1, 2020. Compliance for other components of the Final Regulation occur six months from its publication. However, due to COVID-19, there is a three-month delay (enforcement discretion) in the implementation of some of the elements. For the CMS final rules, the timeline for providers to share admission, discharge, and transfer (ADT) notifications and certain payer interoperability requirements has been delayed to the spring of 2021.

Compliance with information blocking and associated conditions of certification are required by November 2, 2020 plus an additional three months due to the enforcement discretion, moving the deadline to February 2, 2021. Health plans will need to share clinical information with each other, at the patient's request, by January 1, 2022. CMS still plans to report actors publicly that are found to be engaged in information blocking starting later in 2020.

Risks Associated With the ONC Final Rule

While the ONC Final Rule provides for some of the most sweeping enhancements to patient access, it also raises significant concerns about patient privacy and security. In this section, we explore some of the many security and privacy areas of concern and the associated risks for health care providers.

Although HIPAA rules remain in effect, patients can send their PHI to third party applications and devices that the patient owns and controls. Once that is done, the covered entity is no longer responsible for the security of the PHI. The responsibility for protection shifts to the patients. However, patients may not be fully aware of the pitfalls of asking for information to be sent unencrypted or in another unsecured manner. As a result, the onus may fall on providers to provide education. That said, providers can't discourage patients from using their API of choice. Patient information that is no longer under the purview of HIPAA rules and supported by Health Information Management (HIM) experts i.e. patient information that is at higher risk of breach and unauthorized access.

Covered entities are still responsible for employing reasonable safeguards for the transmission of Protected Health Information (PHI) to a third party. Some third-party applications will be certified under the Health IT Certification Program which would further assure providers and patients that HIPAA and industry standard privacy and security measures are in place for these apps. However, Health IT Certification is voluntary. Not all patient-facing consumer apps may be certified or subject to HIPAA rules. The ONC Final Rule supports an individual's ability to choose which third party developer and app are best for receiving all or part of their EHI from a health care provider. Education may be provided by actors to assist patients in making the best choice in the selection of an app, whether it be certified and non-certified.

The ONC Final Rule also strongly encourages actors to educate patients and individuals about the risks of providing other entities or parties access to their EHI. This education would not be considered information blocking by an actor so long as the educational information provided is not misleading, factual, unbiased and non-discriminatory among other requirements. Despite this education, it will be incumbent on patients to understand the risks associated with obtaining and sharing their information through these apps. Placing the onus on the patient, in conjunction with how applications are developed, continues to raise concern about the privacy and security of patient health information.

It's important to note that an EHR is not just one thing; it is a collection of data and information from multiple sources that need to be connected, ideally using a national set of standard definitions. Interoperability is not just connecting EHRs but also looking at the data elements within. Questions related to identifying different types of data and the level of data quality must be asked and answered. For example, do providers, even within the same office, place the same information in the same data element? How are non-standard data elements captured i.e., 'dictated' progress notes, pathology reports, etc. What is the process to ensure data quality? Remember, this begins with USCDI data elements until standards are accepted.

As new players enter the app market for EHI using the new rules on API's, one of the primary risks will be around security for the data. In most cases, HIPAA won't apply to these app developers, and there is the possibility that security practices will not be as stringent for all those new apps, opening up new avenues of attack for malicious actors who can now target these fledgling app companies for purposes of stealing medical records. These types of attacks will only be facilitated by the standardization of the API's, since the same parameters can be used for attacking any app in the ecosystem which is an advantage to certified App Developers but also for black hat hackers.

Addressing the Issues

Combating the complex privacy and security issues raised by the ONC Final Rule will take time and effort. Provider organizations will have to clearly define their designated and legal health record-sets to answer fulfillment and access questions. Will patients have access to all of their records under the definitions? Most hospitals have multiple EHR systems, and many times do not upload all information into the primary EHR systems, raising important questions. For example, if the information that is not uploaded is used for patient care, will this secondary EHR data be discoverable, maintained, and is it customarily released when requested? Is the HIM department aware of all the systems that collect PHI? A defined designated record set (DRS) removes confusion and inconsistency in the process in regard to what should be released and where to find it. Lack of this clarification can have legal consequences as well as have an impact on patient care. Remember that the DRS is made available only for patient and patient-directed situations. For legal situations, a legal heath record would be required.

Patients will also have a right to the United States Core Data for Interoperability (USCDI) data set. Health care providers need to look at what they currently have available on their patient portals and provide the USCDI data set within nine months (six months plus three months from May 1, 2020). As third party apps are developed and made available to patients, the USCDI data set must be made available within the same timeline as noted above. After the 24 months plus the additional three months, the "full" EHI per the designated record set needs to be available to the patient.

Data exchanged from Provider A to Provider B creates additional ambiguity that will need to be addressed as it creates definition challenges related to the legal record set. Is the combined information expected to become part of the legal patient record that is released for legal requests? Will this new data be combined, or will the imported data be stored under "imported" or "miscellaneous" in the chart to designate different sources? Will the imported data be used by Provider B to make medical decisions, and if so, would it then be part of the legal record as well? Each organization has many questions to answer, and the conversation should include the providers, those who perform HIM functions as well as IT.

Tracking is another area that needs further evaluation and discussion with HIM representation.

As apps are offered, what education will be provided by the health care organization to assist patients in understanding the privacy and security risks associated with the apps they use? How do we envision patients sharing their information in these apps with other third parties? Do the information blocking provisions apply when patient information is being released with assistance from ROI staff or only when patients access their EHI directly with no assistance through an app or a health care organization's portal.

As the patient will be able to view their entire medical record, this will likely result in organizations experiencing an increase in addendum requests. Healthcare organizations will need to determine the best way to correct records or communicate to a patient that the record is accurate as is. On the other side of the coin, how will practices address information that is incorrect? With full interoperability nationwide, who owns the original source of information, and who must find it and change it and disseminate the correction? Keep in mind that anyone can point out or suggest an error, but the original author still has the control for changes and the amendment rules of HIPAA still apply.

Finally, it is important to note that penalties by the Office of the Inspector General (OIG) will come into play, though specifics are to be determined.

Summary & Conclusion

The ONC Final Rule enables the health care delivery system to deliver an “app economy” that provides patients, physicians, hospitals, payers, and employers with innovation and choice. Through the delivery of modern smartphone and software apps, patients and providers will see benefits in accessing electronic health information (EHI). Patients will have more convenient and easier options to gain on-demand access to their EHI whenever and wherever they need it.

While the ONC Final Rule provides for some of the most sweeping enhancements to patient access, it also raises significant concerns about patient privacy and security.

It is critical for healthcare providers to understand the many privacy and security issues raised by the final rule and develop strategies and plans to address them. New technology tools (APIs, apps, etc.) need to be vetted and discussed by healthcare privacy officers, HIM departments, and IT to determine how patient access can be enhanced without compromising privacy. Provider organizations should integrate the implementation of their operational and business responses to the final rules into their compliance plan.

The May 9, 2020 ONC Final Rule provides a framework for innovating and significantly increasing patient access. Provider organizations need to put plans in place that ensure patient privacy and security are not compromised as the industry ramps up patient access.

Additional Resources

The CMS Interoperability and Patient Access Final Rule

The Interoperability and Patient Access Fact Sheet

Disclaimer: This white paper is for informational purposes only and does not constitute legal advice. You should contact your attorney to obtain advice with respect to your specific issue or problem.

About the Association of Health Information Outsourcing Services

Established in 1996, AHIOS promotes, strengthens and enhances the health information management outsourcing industry while ensuring excellence in managing risk and compliance issues associated with the disclosure of Protected Health Information. Its goals are to increase awareness of the value, importance and complexity of the industry’s services; establish standards of excellence for the industry of health information management outsourcing; pursue fair and equitable treatment of the industry through legislative, regulatory and legal processes; and create educational and networking opportunities for members. For more information, visit AHIOS.org