MediQuant®

INFORMATION BLOCKING:

Is Your Healthcare System Compliant?

A 21st Century Cures Act Overview for Healthcare Executives

A MediQuant White Paper

©Copyright 2024

CONTENTS

Introduction

It's no surprise that preparations for the 21st Century Cures Act took a backseat to COVID-19. Now, not only are healthcare providers battling declining revenues and unprecedented labor shortages, but they also must adhere to new information blocking regulations. Otherwise, they could face steep fines and public scrutiny.

Several Cures Act regulation deadlines have passed, and more are fast approaching, leaving much of the healthcare industry unprepared.

This white paper serves as a 21st Century Cures Act compliance reference tool for providers to understand the new regulations and how best to prepare their organizations to achieve information blocking compliance.

Background

The 21st Century Cures Act1 was signed into law on December 13, 2016. This law included provisions to streamline the drug and medical device supply chain, prevent and treat opioid abuse, and accelerate treatment for serious illnesses.

This legislation also aimed to drive the electronic access, exchange, and use of health information. It required organizations to remove bureaucratic burdens associated with the use of electronic health records (EHR) and health information technology (health IT). To be compliant, organizations adopted interoperability requirements to prevent "information blocking."

To implement the Cures Act's electronic health information provisions, the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS) wrote two sets of rules that focus on health information access, increased innovation, and the elimination of information blocking.
In 2020, the U.S. Department of Health and Human Services (HHS) finalized the two sets of rules and announced the next phase of the Cures Act.

The HHS announced that these ONC Cures Act Final Rules require "both public and private entities to share health information between patients and other parties while keeping that information private and secure."[2]

The ONC Cures Act Final Rule puts patients at the center.

The ONC's Cures Act Final Rule aims to provide patients with complete transparency regarding the cost and outcomes of their care.[3] The Final Rule is designed to ensure patients and providers have easier access to electronic medical records at no additional cost.

The Final Rule implements the Cures Act's interoperability provisions to give patients more control over their own information. It achieves this through the prevention of information blocking practices by providers, health IT developers, health information exchanges (HIEs), and health information networks.[4]

These regulations apply not only to healthcare organizations but also to IT vendors. For example, an IT vendor can't use proprietary technology to encrypt data and prevent a hospital or organization from sharing that data.

The End Game: Patient-Centered Health IT for All Americans

The success of the Cures Act centers on the seamless exchange of EHI and patient use of smartphone applications. Once all stakeholders comply with the Cures Act regulations, all U.S. healthcare system participants will have access to their electronic health information when, where, and how they want it.

This will be a seismic shift in the patient-provider paradigm. It will further democratize the access, exchange, and use of EHI. Patients will have the ability to easily switch providers, seek second opinions, and gather legal documentation.

But, many providers and health IT vendors find themselves unprepared from a procedural and technological standpoint. They're still recuperating from a global pandemic, severe labor shortages, and an ever-changing competitive landscape.

The time is now for healthcare providers to incorporate the Cures Act regulations into their digital strategy.

The success of the Cures Act centers on the seamless exchange of EHI and patient use of smartphone applications

Information Blocking - What Every Provider Should Know

The Office of the National Coordinator for Health Information Technology (ONC) considers information blocking a "serious problem because it can prevent timely access to information needed to manage patients' health conditions and coordinate their care."[5]

The ONC defines information blocking, or data blocking, as occurring when individuals or entities – such as healthcare providers or IT vendors – knowingly or unreasonably interfere with the exchange or use of electronic health information (EHI).[6]

Put simply, any action that interferes with the access, exchange, or use of a patient's EHI is considered information blocking. But not all actions that prevent the exchange or use of electronic health information qualify as a Cures Act violation. Sometimes, information is withheld for a patient's privacy or security.

When does information blocking violate the Cures Act?

- The person(s) or entity interfering with the access, exchange, or use of the EHI is a designated "Actor".
- The blocked data qualifies as EHI that must be shared with patients quickly and affordably.

The Cures Act established three "Actor" categories.

Healthcare Provider
This includes hospitals, physician offices, skilled nursing facilities, and ambulatory surgical centers. (a full definition is in the Public Health Service Act (42 U.S.S. 300jj))

Health Information Network (HIN) or Health Information Exchange (HIE)
These entities do not provide healthcare services. Instead, they serve as a method for disparate healthcare providers to share patient medical records securely and electronically. This applies to treatment, payment, or health care operations purposes. (a full list of covered entities is defined in 45 CFR 164.501)

Health IT Developer of Certified Health IT
This includes any individual or entity (other than a provider) that self-develops health IT for its own use or offers it as a product or service (as defined in 42 U.S.C. 300jj).

These "Actors" can be directly or indirectly involved with the violation. Information blocking can be an overt action, like withholding electronic health information from a patient, or more subtle situations like organizational policies or technical constraints that prevent a patient from accessing their EHI in a timely manner.

What kind of data must be shared?

Initially, the Cures Act did not define "EHI" as it relates to information blocking. The ONC Final Rule clarified the definition and included a two-phase approach implementation.

Phase 1

Timeline: First 24 months after the Final Rule's publication.

Definition: For the purposes of information blocking, EHI was limited to the data elements represented in the US Core Data for Interoperability (USCDI).[7]

The USCDI is a standardized set of data classifications that enable nationwide, interoperable health information exchange.

When the Final Rule was published, the USCDI v1 served as the information blocking data requirement template.

USCDI v1 Data Classes[8]	
Allergies and Intolerances	Medication
Assessment and Plan of Treatment	Patient Demographics
Care Team Members	Problems
Clinical Notes	Procedures
Goals	Provenance
Health Concerns	Smoking Status
Immunizations	Unique Device Identifier(s) for a Patient's Implantable Device(s)
Laboratory	Vital Signs

Phase 2

Timeline: On or after October 6, 2022.

Definition: The electronic protected health information (ePHI) in a designated record set per the Health Insurance Portability and Accountability Act (HIPAA) regulations regardless of whether the records are used or maintained by or for a covered entity.[9]

The second phase of the 21st Century Cures Act dramatically expands the definition of EHI scope for the purposes of information blocking.

As a result, **50 new data classes are now considered EHI.**

Noteworthy New EHI Data Classes	
CLINICAL	**MEDICATION**
Exposure/Contact Information	**ADT Events**
Medical Device or Equipment	**Prior Authorizations**
Orders	**Claims**
Data from Durable Medical Equipment	**Billing Codes**
Provider to provider emails/chats with PHI	**Collection Information**
Provider to patient messages/chats	**Patient Relationships**
	Oncology Outcomes

Providers will be required to share all EHI within a patient's designated record except for psychotherapy notes and certain other documents.

This changes the game from a data retrieval standpoint. Now, all providers are required to make their patients' ePHI available for access, exchange, and use.

Unfortunately, many providers aren't prepared. They're confused about the provisions, penalties, and processes tied to October 6th compliance date.

In September 2022, a group of hospitals, medical groups, and long-term care organizations banded together and urged the HHS to push back its Oct. 6 deadline another calendar year.[10] With or without a deadline extension, many providers will struggle to achieve compliance.

Common Information Blocking Practices

Information blocking is any practice that interferes with the access, exchange, or use of EHI. Some can be blatant violations, while others are more subtle. And not all instances are considered an information blocking violation. It's often situational and depends on the "Actor's" knowledge and intent.

Here are some examples of how information blocking may show up in a healthcare provider's organization:

- Patient unable to log into a portal and view EHI due to lack of standards within health IT
- Physician refuses to register software application that enables patients to access their EHI
- Lack of standard process for patients to request EHI resulting in a slow or no response for requests
- Patient waits a week to see lab test results due to a system requirement for physician approval prior to being available to patient
- Medical record policy requires all medical record release requests, including EHI, to be made in person

These are just a few examples of how information blocking can occur in a healthcare organization. Not only do these infractions negatively affect healthcare organizations' reputations, but "Actors" will face steep fines if they aren't information blocking compliant.

Information blocking penalties could cost health IT vendors millions.

The Health and Human Services (HHS) of the Office of the Inspector General (OIG) finalized information blocking penalties of up to $1,000,000 per violation for HINs, HIEs, and certified developers of health information technology.11 However, the civil monetary penalties for provider organizations haven't been finalized–yet.

In March 2022, the HHS vowed to make these penalties a top priority to close the "provider enforcement gap".[13]

A recent ONC report revealed that

77% **of information blocking complaints were against healthcare providers.[12]**

Getting Compliant. Challenges, Assessments & Best Practices

Challenges: To get compliant, providers must overcome several hurdles.

The 21st Century Cures act includes many new regulations and adhering to them won't be easy.

Faster Turnaround Times

The Cures Act Final Rule stipulates how fast organizations must complete patient information requests and how much they can (or can't) charge to retrieve the data.

To achieve these rigorous turnaround times and minimize costs, providers need to better leverage their portals and get patients to use them.

The good news is that 90% of healthcare providers have a patient portal.[14] Unfortunately, most patients (69%) prefer to interact directly with their provider rather than access the portal.15 Improving patient portal use is two-fold. First, the physicians must have buy-in, knowledge, and experience with the portal. They need to understand how and when their notes, orders, and test results appear for the patient. Once physicians see the value, they'll help direct patients to the portal.

Slow adoption of Fast Healthcare Interoperability Resources (FHIR).

The Cures Act requires certain health IT developers to provide a certified FHIR Application Programming Interface (API) by December 31, 2022.

The goal of FHIR is to make healthcare data flow like the Internet and be searchable, traceable, and usable.16 It also defines how healthcare data should be exchanged between different computer systems, regardless of how that data is stored within the systems.

But, for interoperability to reach its full potential, all healthcare providers and health IT vendors need to adopt FHIR.

Many organizations haven't adopted FHIR due to the nuances involved and required extensive testing. Yet, it's inevitable–healthcare data will be expected to flow through FHIR.

It's important for providers to partner with vendors that already leverage FHIR technology to meet Cures Act requirements. Otherwise, they may be left behind in the market and at risk of information blocking.

Vendor Readiness

Many healthcare organizations are delayed because their IT vendors haven't adopted the necessary technology. Their compliance is contingent on their vendors' readiness which is behind schedule.

There are also deadline inconsistencies between providers and certified vendors. Providers are expected to be compliant by Oct. 6 while the vendors have later cutoffs. This has contributed to confusion and interoperability limitations.

The need for unique patient identifiers.

Increased merger and acquisition activity along with changing regulations underscore the need for unique patient identifiers.

These identifiers ensure the right person is accessing the right record—a critical element to staying compliant with HIPAA and the Cures Act.
What's more, if a healthcare organization sends a patient record through an interoperability component, a unique identifier must be in place to transfer that data.

Slow adoption of Fast Healthcare Interoperability Resources (FHIR).

The Cures Act requires certain health IT developers to provide a certified FHIR Application Programming Interface (API) by December 31, 2022.

The goal of FHIR is to make healthcare data flow like the Internet and be searchable, traceable, and usable.16 It also defines how healthcare data should be exchanged between different computer systems, regardless of how that data is stored within the systems.

But, for interoperability to reach its full potential, all healthcare providers and health IT vendors need to adopt FHIR.

Many organizations haven't adopted FHIR due to the nuances involved and required extensive testing. Yet, it's inevitable–healthcare data will be expected to flow through FHIR.

It's important for providers to partner with vendors that already leverage FHIR technology to meet Cures Act requirements. Otherwise, they may be left behind in the market and at risk of information blocking.

Definition and Regulation Confusion

Providers already struggled with information blocking compliance during the Cures Act's first phase. Now they face an even wider set of EHI that is open to interpretation.

Part of the 10 healthcare organizations' requests to extend the October 6, 2022, deadline centered on the need to clarify the eight information blocking exceptions and how to balance the privacy of sensitive health records.18

Assessments: Evaluate your data retention, retrieval, and recovery processes.

Before you start fixing things, you need to know what's broken. That's why an in-depth assessment is always the first step for any compliance initiative.

Healthcare organizations should evaluate their existing patient information retrieval capabilities and identify potential gaps as well as strategies for addressing those areas. It's also important to analyze the data retrieval and recovery process for EHI, especially the newly added 50 data classes.

Perform an IT and Medical Records policy and procedure deep dive.

Data retention, retrieval, and sharing policies and procedures should be reviewed and updated to reflect Cures Act regulations.

Policies and procedures to consider for review:

- Data Retention & Purging
- Medical Record Retrieval of Information
- Data Recovery & Back-up
- Patient Portal
  - New User Set Up
  - Access Requests
  - Available EHI
  - Troubleshooting
- PHI and Data Privacy
- Data Sharing Governance

Evaluate your existing archive.

Assess how quickly you are able to shift infrequently accessed or older data into a low-cost storage system.

The ability to retrieve data at the point of care and make corrections as needed is important to patient care.

An active archive provides staff with a complete view of the patient record and prevents the need to scroll through multiple records to find the right person. This capability is critical when considering HIPAA compliance and meeting new Cures Act requirements.

Revisit your Cures Act strategy and implementation plan.

The sooner healthcare organizations work on a plan to meet the new Cures Act requirements, the better. The plan needs to define all necessary processes, steps, technologies, and staff members who need to be evolved to comply with the changes.

It's also important to consider the benefits of adopting unique identifiers to help you meet inter-operability requirements and safely allow the patient's the ability to access their own records.

If necessary, get outside help.

To kickstart your Cures Act compliance initiative, attend a boot camp or training program that helps organizations conduct internal assessments of where their organizations are today, and what action needs to be taken for their organizations to get compliant.

Organizations also need clearly written policies and procedures, especially around exceptions. A data compliance expert can help you draft policies and procedures and assess your organization's performance and risk areas.

A data compliance expert can help you draft policies and procedures and assess your organization's performance and risk areas.

Identify your interoperability strengths and weaknesses.

Eventually, all healthcare organizations will be expected to securely share information across IT systems. It's critical to understand where your organization stands from a data interoperability standpoint.

Data interoperability requires sophisticated levels of data architecture exchange, interfaces, and applications.

Healthcare Information and Management Systems Society (HIMSS) recommends using the following categories to assess your interoperability capabilities[19]:

Foundational
individual data that is accessible across clinical, social, and community institutions.

Structural
measures the levels of data integrity and automated data flow across systems. It focuses on data formatting, syntax, and organization.

Semantic
parameters that employ standard definitions of data elements and coding terminology that are available to the public.

Organizational
takes into consideration governance, policy, social, legal, and organizational structures. When achieved, it enables integrated processes and workflows for end users that establish trust.

Interoperability will continue to impact an organization's ability to achieve data compliance, especially with information blocking.

Best Practices for Cures Act Compliance

Healthcare organizations should be actively working on getting compliant with the Cures Act. This starts with assessing existing capabilities, identifying gaps, and implementing best practices. Here's where to start:

Review, update, and enforce your data retention policy.

You must have an updated, relevant, and compliant policy. Even the simplest policy should include the following components:

Formatting
Define how medical records and data should be formatted when they're stored. This should include standards for paper and electronic information.

Timeline
Establish your organization's data retention timelines and validate that your timeline meets several requirements:

- **Federal** - HIPAA requires a minimum of six years from the time of creation or when the record was last in effect.
- **State** - Each state establishes its medical record retention timeline requirement. This also can vary based on patient age and provider type.
- **Insurance Contracts** - Some Payors have documentation retention requirements built into their hospital and physician practice agreements.

Storage System
Designate the storage system(s) or devices that will store your data. Depending on the type of data use case, you may select various storage systems. Keep in mind the cost of storing and retrieving data when selecting storage systems.

Data Back-up
Describe the method for backing up your data. Be sure to designate the backup process for different types of data. This will also play a role in the type of storage system you select.

Data Archive
Describe the type of archive system you will use and how to retrieve data.

Data Purge
Describe when data will be purged and how the process will be executed. It's critical to hold on to data but it's also important to purge it. Not only does this save in storage costs, but it minimizes risk with unnecessary data sitting on your servers or hardware.

In healthcare, it's important when possible, to de-identify and store data and to purge any discoverable data to stay in line with privacy regulations.

Monitoring
Define the method that you will use to monitor your data retention procedures. This should include reviewing, updating, and auditing your procedures. It's important to outline the steps you will follow if a data retention violation occurs.

Assess your data storage strategy

Now more than ever, it's important for healthcare organizations to take their data archive process seriously. To stay compliant with the Cures Act, organizations will need to archive more data elements in their storage systems.

However, more is not always better with data archiving–be sure to assess the time and cost of storing and retrieving data in potential archive systems.

Often, healthcare organizations have far more legacy systems than they realize. Once they start to dig into their data records, they realize the financial and operational burdens associated with buying and maintaining legacy systems.

Archiving data is a popular method, but it may not meet the needs of healthcare organizations anymore.

Traditionally, healthcare companies archived data to tape or cloud-based cold storage. As a result, retrieving old, inactive files was time-consuming for IT administrators. With the Cures Act's patient data request regulations, healthcare organizations can't afford to waste time accessing cheaper cold-tier data storage systems.

Active archiving solutions can help healthcare organizations achieve Cures Act compliance without burdening their IT departments.

Active archiving creates a multi-vendor ecosystem that accommodates various storage systems and platforms–like disk, tape, on-premises, and cloud–depending on client needs. It also enables healthcare organizations to consolidate patient records from multiple providers.

Clinicians use a single sign-on to launch the patient's complete digitized historical record to provide continuity of care. The active archive system also satisfies regulatory requirements with strong user access, activity logging, and integrity protection[20].

Healthcare providers should consider an active archiving solution when building their Cures Act data retention strategy. Active archiving solutions offer flexible integration tools that save money and time–something healthcare providers desperately need currently.

Conclusion

The 21st Century Cures Act is the latest and most significant regulatory compliance issue facing healthcare organizations and their archived data today. The Cures Act is designed to give patients greater access to, and more control over, their healthcare information.

The prevention of information blocking ensures patients receive their healthcare data from their healthcare providers. This data could live in a primary HIS system or as a designated record set in an archiving system.

Information blocking fines are already mounting at an alarming rate. Understanding what to expect and preventing potential hurdles can help your organization avoid massive penalties and fees.

As the Cures Act's regulatory milestones go into effect, organizations will face new challenges to deliver patient data quickly and securely at the individual and organizational levels. Effective interoperability, data retention, and archiving strategies will enable healthcare organizations to achieve information blocking compliance.

About MediQuant

Founded in 1999 and headquartered in Brecksville, Ohio, MediQuant is the leader in enterprise active archiving solutions for hospitals and health systems. The Company's flagship product, DataArk®, assists hospitals in retiring legacy clinical, patient accounting and ERP platforms while maintaining access to critical data via a cloud-based software platform.

MediQuant®

Endnotes

1. Thune, Senator. “H.R.34 - 114th Congress (2015-2016): 21st Century Cures Act | Congress.gov | Library of Congress.” Congress.gov, U.S. Congress, December 2016, https://www.congress.gov/bill/114th-congress/house-bill/34. Accessed 28 September 2022.

2. Department of Health and Human Services. “HHS Finalizes Historic Rules to Provide Patients More Control of Their Health Data.” www.hhs.gov, Archived HHS Content, 9 March 2020, https://public3.pagefreezer.com/browse/HHS%20–%C2%A0About%20News/20-01-2021T12:29/https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html. Accessed 28 September 2022.

3. Official Website of The Office of the National Coordinator for Health Information Technology (ONC), 5 December 2018, https://www.healthit.gov/sites/default/files/page2/2020-03/TheONCCuresActFinalRule.pdf. Accessed 28 September 2022.

4. American Medical Association. “What is Information Blocking? Part 1.” American Medical Association, https://www.ama-assn.org/system/files/2021-01/information-blocking-part-1.pdf. Accessed 29 September 2022.

5. Office of the National Coordinator for Health Information Technology. “Help Us Stop Information Blocking.” HealthIT.gov, Office of the National Coordinator for Health Information Technology, https://www.healthit.gov/sites/default/files/information_blocking_complaints_flyer.pdf. Accessed 1 October 2022.

6. Office of the National Coordinator for Health Information Technology. “HealthIT.gov Topics Information Blocking.” HealthIT.gov, 19 August 2022, https://www.healthit.gov/topic/information-blocking. Accessed 28 September 2022.

7. The Office of the National Coordinator for Health Information Technology. “United States Core Data for Interoperability (USCDI) | Interoperability Standards Advisory (ISA).” HealthIT.gov, https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi. Accessed 2 October 2022.

8. Office of the National Coordinator of Health Information Technology. “The United States Core Data for Interoperability.” HealthIT.gov, Office of the National Coordinator of Health Information Technology, July 2020, https://www.healthit.gov/isa/sites/isa/files/2020-10/USCDI-Version-1-July-2020-Errata-Final_0.pdf. Accessed 1 October 2022.

9. Office of National Coordination of Health Information Technology. “Changes and Clarifications from the Proposed Rule to the Final Rule.” Organization, Office of National Coordination of Health Information Technology, 2022, www.healthit.gov. Accessed 1 October 2022.

10. Muoio, Dave. “Providers petition HHS for more time on info blocking.” Fierce Healthcare, 27 September 2022, https://www.fiercehealthcare.com/providers/providers-say-they-need-extra-year-clearer-guidance-meet-hhs-looming-info-blocking. Accessed 1 October 2022.

11. The Daily Register of the United States Government. “Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; Office of Inspector General's Civil Money Penalty Rules.” Federal Register, The Daily Register of the United States Government, 24 April 2020, https://www.federalregister.gov/documents/2020/04/24/2020-08451/grants-contracts-and-other-agreements-fraud-and-abuse-information-blocking-office-of-inspector. Accessed 1 October 2022.

12. Office of National Coordinator of Health Information Technology. “Information Blocking Claims: By the Numbers.” HealthIT.gov, Office of National Coordinator of Health Information Technology, September 2022, https://www.healthit.gov/data/quickstats/information-blocking-claims-numbers. Accessed 1 October 2022.

13. Muoio, Dave. “HIMSS 2022: Becerra, Brooks-LaSure say provider info blocking penalties, revamped interoperability rule on the horizon.” Fierce Healthcare, Fierce Healthcare, 15 March 2022, https://www.fiercehealthcare.com/health-tech/becerra-brooks-lasure-himss-2022-info-blocking-interoperability-civil-monetary. Accessed 1 October 2022.

14. Lyles, Courtney, and Matthew Krasowski. “Quantifying Patient Portal Use: Systematic Review of Utilization Metrics.” NCBI, National Library of Medicine, 25 February 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7952240/. Accessed 1 October 2022.

15. Office of the National Coordinator of Health Information Technology. “Individuals’ Access and Use of Patient Portals and Smartphone Health Apps, 2020.” HealthIT.gov, September 2021, https://www.healthit.gov/data/data-briefs/individuals-access-and-use-patient-portals-and-smartphone-health-apps-2020. Accessed 3 October 2022.

16. Agnew, James. “The Urgent Need for HL7 FHIR Adoption.” Smile CDR, Smile Digital Health, 10 March 2022, https://www.smilecdr.com/our-blog/hl7-fhir-adoption-urgency. Accessed 7 October 2022.

17. Muoio, Dave. “Providers petition HHS for more time on info blocking.” Fierce Healthcare, 27 September 2022, https://www.fiercehealthcare.com/providers/providers-say-they-need-extra-year-clearer-guidance-meet-hhs-looming-info-blocking. Accessed 1 October 2022.

18. Muoio, Dave. “Providers petition HHS for more time on info blocking.” Fierce Healthcare, 27 September 2022, https://www.fiercehealthcare.com/providers/providers-say-they-need-extra-year-clearer-guidance-meet-hhs-looming-info-blocking. Accessed 1 October 2022.

19. HIMSS. “Interoperability: How to Measure Data Interoperability and Communication Across Health Systems.” HIMSS, 22 February 2021, https://www.himss.org/resources/interoperability-how-measure-data-interoperability-and-communication-across-health. Accessed 16 October 2022.

20. Active Archive Alliance. The Active Archiving Ecosystem, Building a Flexible Archive Repository Your Way. Active Archive Alliance, July 2022, https://activearchive.com/wp-content/uploads/2022/07/AAA-Annual-Report-2022-Final.pdf. Accessed 22 October 2022.