

A woman with long brown hair, wearing a black blazer over a white top and black trousers, is walking through a modern office hallway. She is holding a tablet in her right hand and looking out of a large window. The hallway has a blue carpet and large windows that reflect the city outside. In the background, other office furniture and a person are visible.

5

Steps to Prepare for Information Blocking Regulations

verato

Executive Summary

As healthcare data – and the number of systems and organizations housing it – continue to grow at an accelerating pace, the timely and secure flow of electronic health information (EHI) has never been more important.

The drive to healthcare interoperability began nearly 20 years ago, starting with the executive order from President George W. Bush, the establishment of the Office of the National Coordinator (ONC) and the appointment of Dr. David Brailer as the nation's first "Health Information Technology Czar". The Meaningful Use program, developed by Centers for Medicare & Medicaid Services (CMS) to incentivize the use of EHRs was then born out of the HITECH Act and Merit-Based Incentive Payment System.

In 2016, Congress signed the 21st Century Cures Act into law that stated that sharing electronic health information is the expected norm in healthcare.

The U.S. Department of Health and Human Services (HHS) has established Information Blocking rules and regulations in the Final Rule. Information blocking occurs when organizations interfere with the access, exchange, or use of EHI. Not only does the practice have the potential to impede patient care, but it can also lead to a range of penalties and disincentives.

Fortunately, healthcare organizations can take steps to prepare for information blocking regulations and ensure optimal interoperability.



1. Establish a data governance framework

As a first step to meeting Information Blocking rules, organizations should lay the groundwork for clean, well-managed data by establishing a clear governance structure.

Putting this foundation in place is especially important as information blocking regulations will trigger an influx of data flowing between organizations. While 98% of healthcare executives expect an increase in data requests from other organizations, only 43% said their organizations are fully compliant in this area. Executives are feeling similarly about the other side of the coin: 97% predict an increase of external data entering their organization, but only 43% feel confident their organization is compliant. A solid data governance structure helps organizations prepare data for sharing with other entities and integrate data coming from external sources, even if the data quality is unknown.

1. Establish a data governance framework

A data governance framework is a set of principles, processes, and practices for effectively managing and protecting data, including sensitive patient, provider, and consumer information. The framework typically covers areas such as security and privacy, data accuracy and integrity, access control, data sharing and exchange, data retention policies, data quality, data architecture, and audit trails.

Such an enterprise-wide framework helps keep data accessible and secure, which in turn facilitates interoperability across healthcare organizations. It is much easier for entities to run afoul of information blocking rules when it is not clear who owns the requested data, whether it is accurate and complete, and who has access to the information.



Tip

A master data management solution built for healthcare (hMDM) can help organizations implement a data governance strategy. As the enterprise-wide single source of truth, hMDM is designed to improve the accuracy, consistency, and security of patient, provider, and consumer information. This ensures that healthcare providers and other stakeholders have access to up-to-date, reliable information for optimal patient care. Additionally, hMDM can be used to streamline the data exchange process by creating and maintaining a central repository of patient data, thus reducing duplication and manual errors.

2. Ensure compliance

Once a holistic data governance structure is in place, healthcare organizations should turn their focus to the specific compliance requirements for meeting all aspects of information blocking rules. If a dedicated project team is not already in place to oversee compliance, now is a good time to establish one.

First, the compliance team should familiarize itself with the ONC Information Blocking Rule and understand the responsibilities of healthcare organizations. This is especially important as there are nuanced rules exceptions, and penalties for healthcare providers, health IT developers, and health information exchanges (HIEs)/ health information networks (HINs).

Then, it is time for the team to take action and establish a compliance plan. A compliance plan should take stock of current ways the organization does or doesn't meet aspects of the information blocking rule, what necessary steps need to be taken to remedy the situation, who owns individual projects, and include a proposed timeline.



Tip

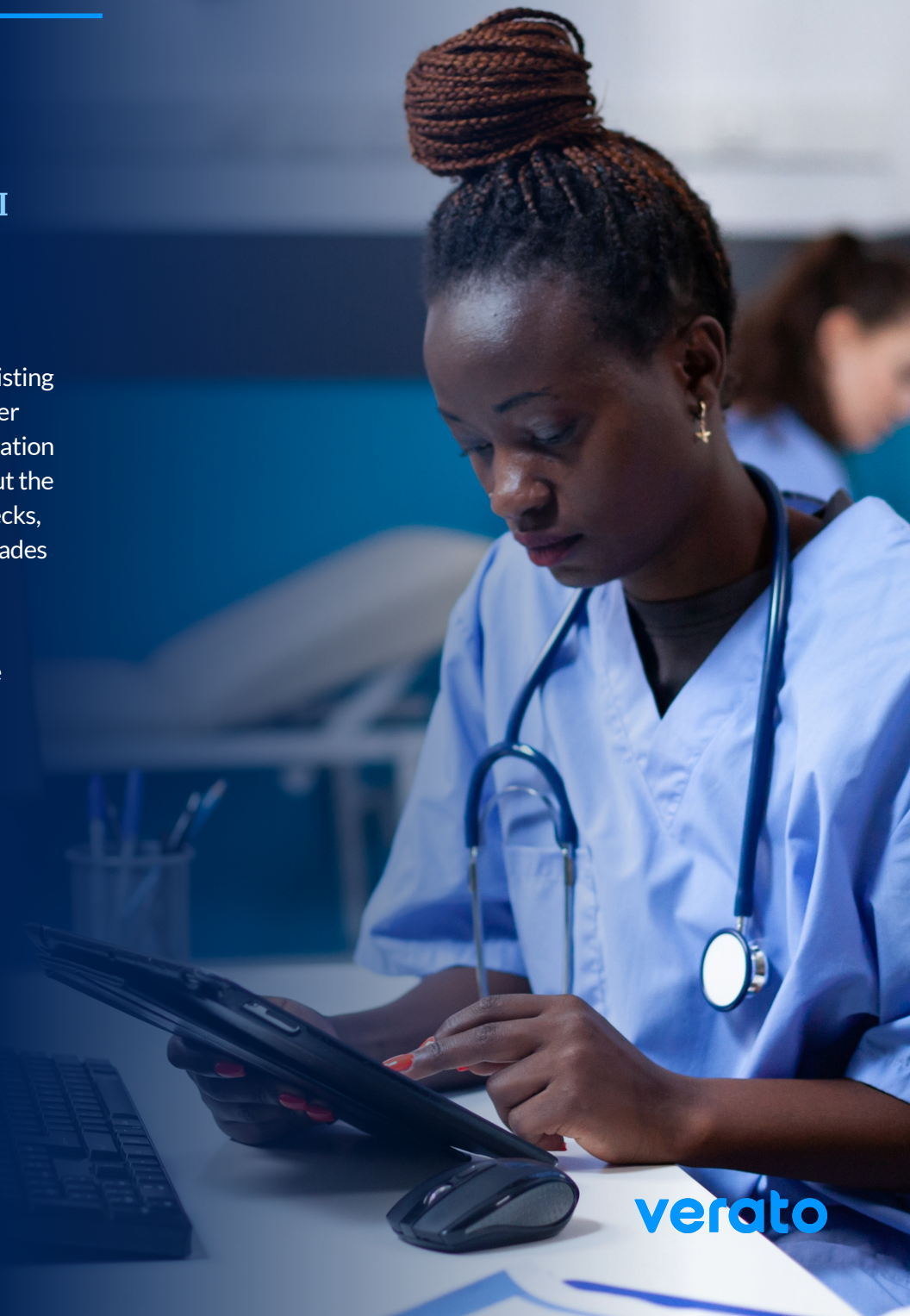
Encourage open communication channels where employees feel comfortable seeking guidance and reporting potential issues and establish feedback mechanisms to gather insights from staff on the effectiveness of compliance measures, allowing for continuous improvement.

3. Identify and connect systems

Identifying all systems that will be involved in EHI sharing requests is a critical step in preparing to comply with information blocking regulations.

Healthcare organizations should conduct a thorough inventory of their existing health information systems, electronic health records (EHRs), and any other systems that handle patient data. This includes systems within the organization as well as those used in collaboration with external entities. By mapping out the entire ecosystem, healthcare organizations can identify potential bottlenecks, interoperability challenges, and areas that may require technological upgrades or integration solutions.

Such an assessment also helps in establishing a clear understanding of how information flows within and outside the organization, facilitating the development of streamlined and standardized processes for handling EHI sharing requests.



3. Identify and connect systems

After compiling an inventory of all systems that contain information pertaining to EHI requests, organizations should look toward building infrastructure to support the access, sharing, and exchange of information between EHRs and other systems containing health information. But accessibility does not look the same for every requestor. Organizations may consider a patient portal to give patients easy access to data, while other, API-based solutions may be more appropriate for provider-to-provider sharing.

Once organizations have considered how data will be shared, it is time to ensure all necessary information will be available. Patient data is often housed in diverse and siloed sources, making it difficult to retrieve complete and current information in a timely manner. By connecting all relevant systems, organizations ensure efficient compliance with information blocking regulations.



Tip

An identity management solution like the Verato hMDM platform allows you to connect disparate data sources and systems, manage data to deliver the right information, and enables interoperability across your digital health ecosystem. The platform makes it easy to not only see the flow of information but also feel confident knowing patient data is complete, accurate, and up to date before answering EHI requests.

4. Institute a clearly defined process

In order for healthcare organizations to comply with the information blocking rule at all times, the compliance team should define clear and easy-to-understand processes for managing information sharing requests.

While every organization's processes will look different depending on individual needs, the following list serves as a starting point for the items the process should define:

- Which team is accountable overall
- Defining steps of the process and ownership of each step
- Proposed timelines for completion of each step
- Steps needed to document compliance and enable reporting
- Identifying dependencies and risks



Tip

Regularly review and update these processes to adapt to evolving regulatory requirements and technological advancements and evaluate the efficiency and effectiveness of existing protocols.

4. Institute a clearly defined process

Information needs to be accurate, complete and a timely response is expected according to the rules. If patient information resides in different systems, it is critical that infrastructure is put in place to connect data from these different systems.

As ONC defines information blocking as any practice that is likely to interfere with the access, exchange, or use of EHI, including unreasonable delays in providing patient records or charging exorbitant fees for data access, it is of the utmost importance that standardized processes are in place to avoid unintentional information blocking. Organizations should consider utilizing a technological solution for answering EHI requests in a timely manner. Not only does this reduce time spent on manually preparing and sharing data, it reduces the potential for errors and enables accountability and reporting. These processes should also include provisions for the eight exceptions to the information blocking rule as established by ONC.

The info blocking Final Rule defines “access,” “exchange,” and “use” as follows:

- “Access” is the ability or means necessary to make EHI available for exchange, use, or both.
- “Exchange” is the ability for EHI to be transmitted between and among different technologies, systems, platforms, or networks; and is inclusive of all forms of transmission such as bidirectional and network-based transmission.
- “Use” is the ability for EHI to be understood and acted upon once accessed or exchanged. “Acted upon” includes the ability to read and write and is also bidirectional.

4. Institute a clearly defined process: 8 exceptions

ONC has defined eight exceptions to the information blocking regulations:

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

- Preventing Harm Exception
- Privacy Exception
- Security Exception
- Infeasibility Exception
- Health IT Performance Exception

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

- Content and Manner Exception
- Fees Exception
- Licensing Exception

5. Prepare staff members

To ensure established processes are followed, healthcare organizations should identify staff members responsible for monitoring and, when necessary, auditing incoming and outgoing EHI requests.

In addition to dedicated staff members, all employees who will be affected by EHI requests should receive regular training on information blocking regulations. Training should cover the following topics:

- The importance of information sharing for patient care
- Defined exceptions
- Internal processes
- Applicable penalties
- The legal aspects of compliance.

Encouraging a culture of collaboration and emphasizing the significance of patient-centric care is essential in fostering a proactive approach to information sharing and compliance. Regular updates and refresher courses should be instituted to keep staff members informed of any changes or amendments to the regulations to ensure sustained compliance.



Tip

Offer practical scenarios and case studies to enhance your staff's understanding of transparency, interoperability, and timely patient data access. By combining legal knowledge with practical skills and a culture of collaboration, your staff will be well-prepared to navigate the complexities of information blocking regulations in the healthcare landscape.

How Verato can help you prepare

Verato is by your side as you prepare for increasing expectations around interoperability. In order to comply with information blocking regulations, your systems need to be able to assemble, ingest, match, and share a growing rate of information across data sources. As the industry's only master data management solution built for healthcare, Verato hMDM can help you get ready for the tasks ahead and support your interoperability strategies.

To see Verato in action and learn how we can support your initiatives,

[Book a demo.](#)



verato

Verato enables digital engagement, clinical interoperability, cloud migration, and provider data integrity by solving the problem that drives everything else—knowing who is who. The Verato hMDM platform, the industry's first purpose-built healthcare master data management solution, enables a complete and trusted 360-degree view of patients, consumers, members, providers, and communities. Over 90 of the most respected brands in healthcare rely on Verato to connect, identify, enrich, manage, and activate person and provider data across the complex digital health ecosystem with unprecedented accuracy, ease, and time-to-value. With a secure enterprise-wide single source of truth for identity, Verato ensures that you get identity right from the start.

For more information, visit verato.com

© 2024 Verato, Inc. All rights reserved.

The Verato logo is displayed in a bold, lowercase, sans-serif font. The letters are a light blue color, contrasting with the dark blue background. The 'v' is particularly prominent, starting with a long horizontal stroke that extends to the left.