Prevent Information Blocking and Ensure Cures Act Compliance

The Cures Act took effect in April 2021. However, many organizations have yet to fully understand and comply with the law's provisions. The information blocking rule in this legislation has far-reaching implications regarding healthcare data sharing. By taking proactive steps, including information governance, organizations can simplify regulatory compliance.

The Cures Act affects virtually every organization with access to electronic health information (EHI). A key purpose of the act involves facilitating the access and exchange of EHI among authorized parties. These parties include entities such as healthcare providers, patients, and health IT developers.

Many of these entities already fall under HIPAA regulations, which aim to protect the privacy and security of EHI. Together, HIPAA and the Cures Act work to empower patients with their own health information and improve the quality and efficiency of healthcare delivery.

Information Blocking Rule and Exceptions

A significant provision of the Cures Act prohibits information blocking by various "actors." The actors specified include healthcare providers, health information technology (IT) developers and health information networks or exchanges (HIN and HIE). These parties must not engage in practices that are likely to inhibit the access, exchange, or use of EHI.

For example, a hospital that refuses to share necessary health information with another provider, even though the patient has given consent, engages in information blocking. Likewise, a health IT vendor that charges excessive fees for interfacing with other systems creates unacceptable barriers to data exchange.

Information blocking can include a wide range of activities. Consequently, instead of defining specific activities that constitute information blocking, the regulation specifies eight exceptions to the rule. These are circumstances under which an entity may legally restrict the access, exchange, or use of EHI. They include the following:

- Preventing harm – An entity may interfere with EHI if it is necessary to protect patients or other persons from physical harm.
- Privacy – An entity may protect the privacy of EHI by complying with state and federal laws and regulations, or by honoring the requests or preferences of individuals.
- Security – An entity may protect the security of EHI by implementing reasonable safeguards and best practices to prevent unauthorized or malicious access or disclosure.
- Infeasibility – An entity may decline to provide EHI if it is not technically feasible or if it imposes an unreasonable burden or cost.
- Health IT performance – An entity may limit the availability of EHI temporarily for maintenance, improvement, or testing of health IT systems or services.
- Content and manner – An entity may limit the content or the manner of providing EHI if it meets certain conditions and offers an alternative method of access.
- Fees – An entity may charge fees for accessing or exchanging EHI if they are reasonable, cost-based, and transparent.
- Licensing – An entity may require a license for the use of interoperability elements (such as software or data standards) if they are non-discriminatory and fair.

Best Practices to Simplify Cures Act Compliance

Healthcare entities that fail to comply with these standards face significant monetary penalties and other disincentives. Therefore, proactive organizations will follow best practices to ensure that patients can access their own data and that data flows where it needs to go.

Begin by conducting a gap analysis to identify any practices, current or potential, that might be considered information blocking. Include all stakeholders, including the legal team and IT, in the process. This process will involve reviewing policies and procedures related to accessing, exchanging, or using EHI to ensure they align with information blocking guidelines.

Educate both staff and stakeholders about the implications of the information blocking rule. For instance, this will include teaching staff how to respond to EHI requests in a timely manner. It will also include continued security awareness training to ensure the protection of regulated data.

Information governance also plays a key role in compliance by establishing procedures to ensure the availability, integrity, and security of EHI. For instance, organizations should:

- Conduct a data inventory to identify where EHI is stored, who has access to it and how it is shared.
- Implement data quality practices to ensure the accuracy of EHI.
- Adopt comprehensive data security and privacy measures to protect EHI from unauthorized access or use.
- Develop data exchange standards to facilitate the interoperability and portability of EHI.

For help building and implementing an effective information governance strategy, contact the information governance experts at Messaging Architects.