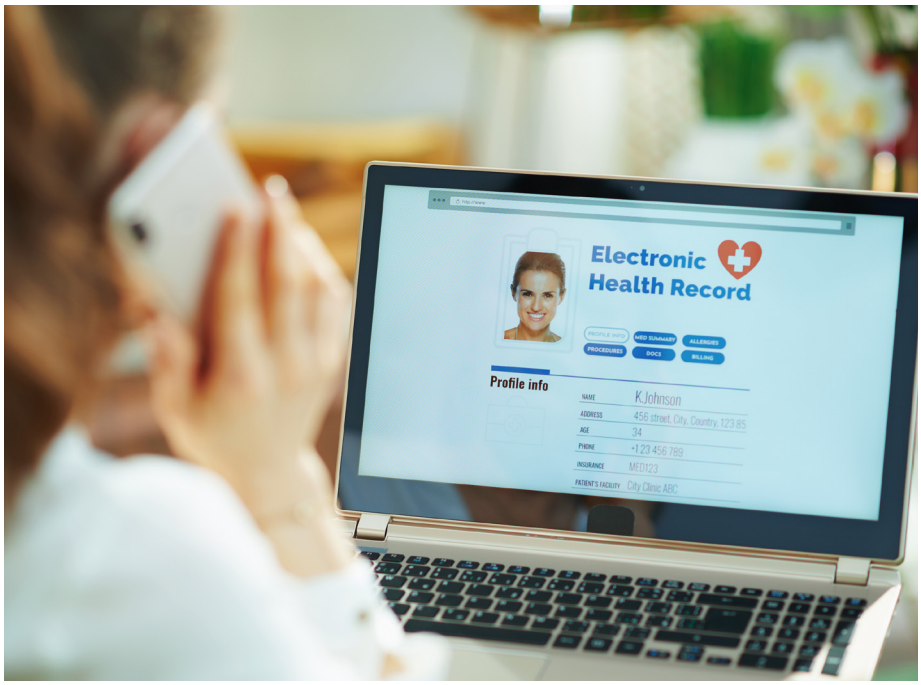
Rethinking Patient Privacy: Information Blocking



Jenna Bickford is a partner at MacDonald Illig Attorneys and is a member of the firm's Business Transactions, Real Estate and Finance, and Healthcare Practice Groups.

Over the last two decades, the federal government has made several attempts, through regulations and financial incentives, to expand the use of electronic health records (EHRs) and make EHRs more compatible and interoperable. EHR compatibility and interoperability allows health-care providers, payors, and health information exchanges to share and access health information data across systems in order to better facilitate health-care delivery.

In 2016, Congress continued these efforts by passing the 21st Century Cures Act, which included provisions aimed to promote electronic health information interoperability, promote patient access to records, and prohibit "information blocking." Final rules took effect on April 5, 2021.

Information Blocking

Information blocking is any practice that is likely to interfere with, or discourage access, exchange, or use of, electronic health information. To constitute information blocking, a health-care provider must *know* that the practice is unreasonable and is likely to interfere with, or discourage access, exchange, or use of, electronic health information. Additionally, a health IT developer, exchange, or network engages in information blocking if it knew, or *should have known*, that a practice was unreasonable and was likely to interfere with, or discourage access, exchange, or use of, electronic health information.

A study by the U.S. Department of Health and Human Services found anti-competitive uses of information blocking, such as an EHR developer who intentionally makes exportation of an EHR more difficult than necessary to discourage switching the EHR to a different developer. A health-care provider may engage in anti-competitive information blocking by refusing to interface its EHR technology with another provider who is a competitor.

However, not all information blocking is anti-competitive. Conduct that has historically been considered not only legal, but good privacy practices, may now constitute information blocking. For example, a health-care provider's privacy policies may be considered information blocking if the policies result in the provider declining to share electronic health information when other applicable law would permit the disclosure.

A Shift in Thinking About Patient Privacy

Information blocking requires health-care providers to rethink patient privacy. Since the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted, health-care providers have been rightfully cautious about disclosing patient information. HIPAA *requires* providers to disclose patient information only in limited circumstances. In many situations, HIPAA permits, but does not require, a provider to disclose patient information. Accordingly, many health-care providers disclose patient health information only when required.

Now, health-care providers who decline to disclose electronic health information may run afoul of the information blocking rules if HIPAA would *permit* the disclosure. The question is no longer whether the provider is *required* to make the disclosure, but whether the provider is *permitted* to do so. If the provider is permitted to disclose, the information blocking rules may require the disclosure.

Information blocking rules may also require proactive steps to facilitate a disclosure, such as working with a patient to obtain a valid HIPAA Authorization form in order to permit a requested disclosure.

Compliance Steps

To implement these changes, a health-care provider should consider the following compliance steps:

- Reevaluate privacy practices and identify areas in which information blocking may exist.
- Review EHR vendor and other data sharing agreements to ensure the contractual terms prohibit information blocking and promote interoperability between EHRs.
- Review the Notice of Privacy Practices, and other HIPAA policies and procedures, to *require* appropriate access, exchange, and use of electronic health information in situations where HIPAA *permits* such use or disclosure.
- Review Business Associate Agreements for consistency with updated HIPAA policies and procedures.
- Review fees charged in connection with EHR interfaces or connections.
- Communicate and train employees about these changes. ■

For more information, contact Attorney Jenna Bickford at 814/870-7762 or jbickford@mijb.com.