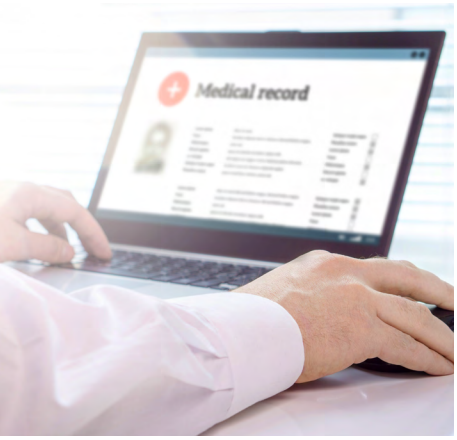
Health Information: Patient Rights and Provider Obligations



Federal and state law provides patients with the right to access their health information, obtain copies, and share it with other providers and third parties. Healthcare entities have obligations to share patients' health records and must have patient consent before legally sharing information, with some exceptions. It is essential for providers to understand the laws related to record sharing for multiple reasons, including the potential of negative impacts on a patient's care. Purposeful withholding of patient information when it should be shared is called information blocking.

What Information Blocking Means

The 21st Century Cures Act defined information blocking as, "a practice that interferes with, prevents, or materially discourages access, exchange, or use of electronic health information," except as required by law or covered by an exception defined by the Secretary of the U.S. Department of Health and Human Services.[1] There are exceptions to this law, such as when it will cause harm. States also have specific laws that might require providers to withhold a patient's access to certain results from an electronic medical record or patient portal for a short period unless certain requirements are met.[2]

Information blocking applies to healthcare providers, health information networks and/or health information exchanges, and developers of certified health information technology. Information blocking applies to products that are certified under the Office of the National Coordinator for Health Information Technology's (ONC) certification of health information technology program, as well as non-certified products.[3] Examples of information blocking could be:

1. Patient Costs Associated with Information Sharing

Entities can require patients to pay a fee but only within specific limits. The cost to provide the individual (or the individual's personal representative) with a copy of their record or to direct the copy to a designated third party must be reasonable. Some states have laws that require entities to provide one free copy.

2. Physicians' Interfering with Information Exchange

There are situations where the release of information or a delay in the release may be appropriate. Examples include when a teen's parent or legal guardian has access to confidential information, in cases of child abuse, and when state and federal laws require it.[4] Providers must consider and document why their actions were reasonable in that situation.[5]

If concerns exist about an individual inappropriately being able to access a patient's electronic health information or if the provider knows that a patient is being coerced into sharing their information, it may be appropriate for a physician to interfere with the exchange of information. A provider may be able to claim a "Privacy Exception," which allows information blocking in order to protect the privacy of the patient.[6] After the information is shared with the entity, the sender is not responsible for what happens once the receiver has that information.

continued on page two

Telehealth Providers: Unique Considerations

Telehealth plays an important role in delivering care across the continuum and the rules and ethics regarding privacy, recordkeeping, and record sharing apply. Examples are below.

- A few state telemedicine laws require that, with the patient consent or upon patient request, the patient's medical records from a telemedicine visit are sent to their primary care physician within a set amount of time.
- As telehealth providers can practice exclusively virtually and without a "physical office," efforts should make sure providers, patients, and outside third parties have a way to contact the provider or agency to request records.
- Many state statutes and codes require telehealth documentation to be retained in the medical record, and it must be comparable to an in-person office visit. For example, Texas Administrative Code states that in order to be reimbursed for telemedicine services, "documentation in the patient's medical record for a telemedicine medical service or a telehealth service must be the same as for a comparable in-person evaluation."[7]

Providers Balance Between Continuity of Care and Patient Privacy

To enhance continuity of care, actors are required to request and document consent to share pertinent data with other providers involved in the patient's care. Information blocking requires the health information to be shared unless an exception applies. Under information blocking, if a request to access, exchange, or use electronic health information is made, actors – i.e., healthcare providers, health information networks (HINs) and/or health information exchanges (HIEs) – must respond to the request in a timely manner.

Tips for Helping to Prevent Information Blocking

1. The Blue Button symbol signifies that a site has functionality for customers to download health records. Including this icon can assist patients with accessing their information. The words "Blue Button," the Blue Button logo, the Blue Button combined logo and the slogan "Download My Data" are what consumers should look for when they want electronic access to their health data.[8] There are guidelines for using the Blue Button symbol; click **here** for those guidelines.

2. Compliance documents and policies should include facts about information blocking and other related laws, such as HIPAA.
3. Virtual health providers should take steps to ensure that all relevant staff are aware of and document staff training. Educate staff about information blocking, the legal and ethical obligations of sharing information, the process, related policies, where to go if they have any questions, and how and where to document the actions taken.

References

1 American College of Surgeons. (n.d.). New Information Blocking Rules. https://www.facs.org/advocacy/advocacy-quality/new-information-blocking-rules/

2 Mast, J. & Thole, G. (2022, June). Health Care Operations & Compliance, Professional Perspective – HIPAA & Information Blocking Compliance. Bloomberg Law. https://www.bloomberglaw.com/external/document/X8DOPGUO000000/health-care-operations-compliance-professional-perspective-hipaa

3 ibid.

4 American Medical Association. (2021, May). How do I comply with information blocking? https://www.ama-assn.org/system/files/2020-11/info-blocking-compliance.pdf

5 ibid.

6 American College of Physicians. (n.d.). FAQ on Information Blocking: Patient Access. https://www.acponline.org/practice-resources/business-resources/health-information-technology/interoperability-and-information-blocking-regulations/faq-on-information-blocking-patient-access

7 Friedberg, R. & Daniel, K. (2013, July 30). Telehealth, Remote Monitoring & Medical Records: What Data Must Providers Include in a Patient Medical Record? https://www.healthlawadvisor.com/2013/07/30/telehealth-remote-monitoring-medical-records-what-data-must-providers-include-in-a-patient-medical-record/

8 The Office of the National Coordinator for Health Information Technology. (2018, June 25). Logo and Usage. https://www.healthit.gov/topic/health-it-initiatives/blue-button/logo-and-usage

ata®

Health.
Virtually.
Everywhere.

American Telemedicine Association®
601 13th St NW • 12th Floor • Washington, DC 20005
info@americantelemed.org