

# PROVIDERS BE AWARE: INFORMATION BLOCKING RULES TO EXTEND TO ALL EHI AS OF OCT. 6

## BACKGROUND

In 2016, the 21st Century Cures Act (Cures Act) was passed, governing the sharing of electronic health information (EHI) and authorizing the Secretary of Health and Human Services (HHS) to identify "reasonable and necessary activities that do not constitute information blocking."

Information blocking is a practice by an "actor" that is likely to interfere with the access, exchange, or use of EHI, except as required by law or specified in an information blocking exception. The Cures Act applied the law to health care providers, health IT developers of certified health IT, and health information exchanges (HIEs)/health information networks (HINs).

Notably, too, the Cures Act established two different "knowledge" standards for actors' practices within the statute's definition of "information blocking." **For health IT developers of certified health IT, as well as HIEs/HINs, the law applies the standard of whether they know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI. For health care providers, the law applies the standard of whether they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.** Thus, the exceptions are divided into two categories: exceptions that involve not fulfilling requests to access, exchange, or use EHI, and exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI.

## EXCEPTIONS

Eight information blocking exceptions were established in the 2020 Cures Act Final Rule. When an actor's practice meets the condition(s) of an exception, it is not considered information blocking. Importantly, the information blocking exceptions are voluntary and offer actors certainty, but it is also worth noting that even in cases where a practice does not meet any of the exceptions it does not automatically mean that information blocking has occurred. Instead, such practices are evaluated on a case-by-case basis to determine whether information blocking has occurred.

## PEOPLE

Steven E. Pozaric

## SERVICES AND INDUSTRIES

Health Care and Life Sciences

The eight exceptions include:

- the Preventing Harm Exception, which recognizes that the public interest in protecting patients and other persons against unreasonable risks of harm can justify practices that are likely to interfere with access, exchange or use of EHI;
- the Privacy Exception, which recognizes that if an actor is permitted to provide access, exchange or use of EHI under a privacy law, then the actor should provide that access, exchange or use. However, an actor *should not* be required to use or disclose EHI in a way that is prohibited under state or federal privacy laws;
- the Security Exception, which is intended to cover all legitimate security practices by actors, but does not prescribe a maximum level of security or dictate a one-size-fits-all approach;
- the Infeasibility Exception, which recognizes that legitimate practical challenges may limit an actor's ability to comply with requests for access, exchange or use of EHI. An actor may not have—and may be unable to obtain—the requisite technological capabilities, legal rights or other means necessary to enable access, exchange, or use;
- the Health IT Performance Exception, which recognizes that for health IT to perform properly and efficiently, it must be maintained and, in some instances, improved, which may require that health IT be taken offline temporarily. Under this exception, actors should not be deterred from taking reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of health IT;
- the Content and Manner Exception, which provides clarity and flexibility to actors concerning the required content (i.e., scope of EHI) of an actor's response to a request to access, exchange or use EHI and the way the actor may fulfill the request;
- the Fees Exception, which enables actors to charge fees related to the development of technologies and provision of services that enhance interoperability, while not protecting rent-seeking, opportunistic fees and exclusionary practices that interfere with access, exchange or use of EHI; and
- the Licensing Exception, which allows actors to protect the value of their innovations and charge reasonable royalties to earn returns on the investments they have made to develop, maintain, and update those innovations.

Each of the eight exceptions have multiple conditions which must be satisfied for the exception to apply.

## LOOMING CHANGES

Currently, the scope of EHI subject to the Information Blocking Rule is limited to the data elements listed in the United States Core Data for Interoperability (USCDI v1) data classes. Such data includes patient demographics, assessment and plan of treatment, clinical notes, health concerns, laboratory tests and results, medications, and procedures.

Health care providers, health IT developers of certified health IT and HIEs/HINs should be aware that effective Oct. 6, 2022, however, the EHI that is applicable will expand beyond the USCDI v1 to include **all** electronic protected health information (ePHI) to the extent that such information is a part of a designated record set, regardless of whether the records are used, maintained by, or for a covered entity, as defined by the Health Insurance Portability and Accountability Act (HIPAA).

Electronic records will soon include the following information:

- medical;
- billing;
- enrollment;
- payment;
- claims adjudication;
- case or medical management; and
- any other records used, whether in whole or in part, to make decisions about individuals.

Information that is excluded from EHI for purposes of the Information Blocking Rule includes:

- psychotherapy notes;
- information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;
- employment records;
- education records;
- records regarding a person who has been deceased for more than 50 years; and
- de-identified data.

Providers want to proactively adopt policies and procedures to ensure they are not engaging in practices that may inhibit the appropriate exchange, access, and use of EHI. Notably, and as indicated above, applicable providers should also be aware of the dual and different knowledge standards for actors to be at risk of enforcement action. Health care providers meet the knowledge standard



Armstrong  
Teasdale

if they know the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI. Health IT developers of certified health IT and HIEs/HINs meet the knowledge standard if they know, or should know, that a practice is likely to interfere with the access, exchange, or use of EHI,

For questions or for more information on this pending change, contact your AT lawyer, or any of the authors listed below.