Articles + Publications | September 5, 2023

The Risks and Rewards of Value-Based Care in Health Care IT

WRITTEN BY

Erin S. Whaley | Emma E. Trivax

Reprinted with permission from Healthcare Business Today*.*

As value-based care models have evolved, so too have the health care information technology (IT) tools designed to support them. There are now a plethora of health care IT applications and platforms that aggregate and analyze data to inform care at the bedside, enhance patient engagement, identify gaps in care, and streamline care management, among other things. While these platforms bring value to patients, providers, and payors, the vendors of these platforms should be aware of potential liabilities under current regulatory rules.

On May 1, 2020, the Centers for Medicare and Medicaid Services (CMS) and the Office of National Coordinator for Health Information Technology (ONC) each published a final rule (Information Blocking Rules) that are intended to improve patient access to health information, with new standards for application programming interfaces (APIs) that will reduce "information blocking." "Information blocking" is defined as "a practice that interferes with, prevents, or materially discourages access, exchange, or use of electronic health information" that is not otherwise protected or prohibited by other laws, such as the Health Insurance Portability and Accountability Act (HIPAA).

The original Information Blocking Rules did not contain defined penalties for health IT developers of certified health IT, health information exchanges (HIEs), or health information networks (HINs); therefore, while some of these actors tried to comply with the Information Blocking Rules, others did not dedicate resources to compliance. On June 27, 2023, the Department of Health and Human Services Office of Inspector General (OIG) published its final rule implementing information blocking penalties. Under this final rule, enforcement will begin on September 1, 2023. As a result, health IT developers of certified health IT, HIEs, and HINs will now be at risk for engaging in information blocking and should take immediate steps to come into compliance if they have not already done so.

Data Exchange Promotes Value-Based Care

The legal developments since 2020 have created a regulatory environment that lends itself to promoting value-based care. Value-based care is a form of delivering health care that rewards providers for higher quality of care, rather than the number of services provided. At its core, value-based care requires unhindered and quick access to the appropriate data and patient information, so providers can deliver the most effective and essential health services to patients.

Health IT vendors have responded to providers' needs for access to actionable data with a wide variety of

innovative products and services. Many of these new products and services leverage APIs which enable interoperability and aggregation of health care records from a variety of sources. Currently, many of these innovative software platforms that are used by providers in value-based care initiatives are not certified under the ONC Certification Program. As a result, these health IT vendors may not think that they are subject to the Information Blocking Rules.

Applicability Of Information Blocking Rules To Health IT Developers, HIEs, And HINs

There are three regulated actors under the Information Blocking Rules: health IT developers of certified health IT, HIEs, and HINs. Health IT developers of certified health IT are entities that "self-develop health IT for its own use, that develops or offers health information technology (as that term is defined in 42 U.S.C. 300jj(5)) and which has, at the time it engages in a practice that is the subject of an information blocking claim, one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the National Coordinator pursuant to 42 U.S.C. 300jj–11(c)(5) (ONC Health IT Certification Program)."

An HIE or HIN is an entity that "determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information:

"(1) Among more than two unaffiliated individuals or entities (other than the individual or entity to which this definition might apply) that are enabled to exchange with each other; and

"(2) That is for a treatment, payment, or health care operations purpose, as such terms are defined in 45 CFR 164.501 regardless of whether such individuals or entities are subject to the requirements of 45 CFR parts 160 and 164."

If a health IT vendor is providing services to its provider or payor customers that aggregate information from various sources, it should consult counsel to discuss whether its services would qualify it as a health IT developer of certified IT, HIE or HIN for purposes of information blocking. If the health IT vendor determines that it is or is likely to be considered a health IT developer of certified health IT, HIN or HIE under the Information Blocking Rules, the vendor may now be penalized if it knows, or should know, that a practice it implements is likely to interfere with the access, exchange, or use of electronic health information. This could be a technical, administrative, or business practice. While there are certain exceptions to the Information Blocking Rules, these exceptions tend to be fairly narrow and must be applied through established policies. These policies can only be established by investing the resources to develop an information blocking compliance program.

Penalties For Non-Compliance

Under the new enforcement rule, HIEs, HINs, and health IT developers of certified health IT face steep penalties per instance of information blocking. For each information blocking violation, the HIE, HIN, or health IT developer of certified health IT faces up to a $1,000,000 penalty. In investigating violations, the OIG prioritizes cases that: (1) resulted in, caused, or had the potential to cause patient harm; (2) significantly impacted a provider's ability to deliver patient care; (3) were of long duration; (4) caused a financial loss to a Federal healthcare program,

government entity, or private entity; or (5) was performed with actual knowledge.

Ensuring Compliance To Avoid Significant Penalties

Because of the significant financial penalties that can result from an information blocking violation, vendors who fall into the HIE, HIN, or health IT developer of certified health IT categories should ensure that they remain compliant with the Information Blocking Rules. If they have not done so already, they should review existing technical, administrative, and business practices to identify any potential practices that are not compliant with the Information Blocking Rules; modify those practices to come into compliance; develop and deploy a training program for personnel who may be faced with information blocking issues; adopt policies that describe how the exceptions to the Information Blocking Rules will be applied; and, adopt a policy that sets forth how the developer will respond to information blocking complaints. While these activities will require a significant investment of time and resources, it is advisable in light of the potential for a $1,000,000 penalty per violation.

---

1. The 21st Century Cures Act, 42 U.S.C. 300jj-52.

2. 45 CFR 171.102

3. 45 CFR 171.102

RELATED INDUSTRIES + PRACTICES

- Digital Health
- Health Care + Life Sciences