By Jennifer Vessels, JD, CHC, CHPC

- linkedin.com/in/jennifer-vessels-jd-chc-chpc-1a310176/

In the classic 1979 horror film *When a Stranger Calls*, a babysitter phones the police to report a series of increasingly threatening and frightening prank calls. The police manage to trace the calls (via the wonders of 1970s technology), resulting in the chilling and memorable line: "The calls are coming from inside the house!" While deranged callers are probably not at the top of most compliance professionals' lists of concerns, internal sources of data and, more importantly, a lack of clarity about the risks posed by that data are frightening enough to keep one up at night. In preparation for the next phase of implementation of the Information Blocking Rule, it will be critical for organizations to have a clear view of the data lurking outside of electronic health record (EHR) systems.

Background

In 2016, passage of the 21st Century Cures Act put the healthcare industry on notice of a coming sea change in how electronic health information (EHI) is to be used and shared, with the end goal of full interoperability, "allow[ing] for complete access, exchange, and use of all electronically accessible health information for authorized use."[1] To this end, the final rule, published in May 2020,[2] prohibits engaging in "information blocking," or any practices likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

April 2021 ushered in the first phase of requirements related to information blocking, focusing on 52 data elements within 16 data classes specified in the United States Core Data for Interoperability version 1.[3] A survey of 4,000 clinical, technical, and administrative stakeholders across the industry found a large percentage were unprepared for the new requirements.[4] While 70% of the respondents indicated they were aware of the rules going into effect, nearly half reported either making no changes in anticipation of the requirements or being unaware of how to ensure compliance for their facilities. Given this, it was perhaps unsurprising that the same number were unfamiliar with the term "information blocking" and/or were unaware of any practices or policies that might constitute it.

While enforcement penalties against providers have yet to be announced in the first year of implementation, the Office of the National Coordinator for Health Information Technology (ONC) received 364 claims of possible information blocking via its Report Information Blocking Portal. Over 225 of these were submitted by patients, and more than 300 were against providers.[5] This would indicate that patient claims against providers are likely to far outstrip those against health IT developers, information networks, or information exchanges. This should be a wake-up call to any organization that has not yet taken concrete steps to address the information blocking requirements.

Barring further extensions by ONC, the next phase of the requirements will go into effect October 6, 2022, and

will expand the subject data to include all EHI within the designated record set, which for providers would include all medical and billing records about individuals or any other record maintained by a provider and used to make decisions about the individual. Many organizations worked hard to expand availability, use, and exchange of the data within the EHR in anticipation of the first phase of the information blocking requirements, and the October 2022 deadline may require an even deeper dive.

This document is only available to members. Please log in or become a member.

Become a Member Login