COSMOS
Navigate the Compliance Universe

Compliance Today - November 2023

Kelly McLendon (kmclendon@complianceprosolutions.com, linkedin.com/in/kelly-mclendon-rhia-chps-1855686/) is Senior Vice President, Compliance and Regulatory Affairs, at CompliancePro Solutions, Titusville, FL.

OIG information blocking: CMP final rule takes the stage

by Kelly McLendon, RHIA, CHPS

In June 2023, a new final rule was issued by the U.S. Department of Health and Human Services (HHS) Office of Inspector General (OIG) entitled: Grants, Contracts, and Other Agreements: Fraud and Abuse; Information Blocking; OIG's Civil Money Penalty Rules.[1] The effective date of this new rule is September 1, 2023, with no look-back period. In other words, the rules are in effect now, so there is urgency in the preparation, operation, and administration of compliance for the areas impacted within actors that are subject to the rules.

Rule overview

This final rule from one of the most powerful enforcement arms of the federal government is important for several reasons, but primarily because it establishes an infrastructure for enforcing portions of the 21st Cures Act that has previously not been enforced. And the penalties it proscribes are potentially in the seven to eight figure range ($1 million *per violation*), which adds an entirely new element of risk to organizations that may fall under its purview.

This final rule amends the civil monetary penalty (CMP) OIG regulations to incorporate new CMP authority for information blocking; incorporate new authorities for CMPs, assessments, and exclusions related to HHS grants, contracts, other agreements; and increase the maximum penalties for certain CMP violations.

Section 4004 of the Cures Act added section 3022 to the Public Health Service Act (42 U.S.C. § 300jj-52),[2] which, among other provisions, provides OIG the authority to investigate claims of information blocking and authorizes the secretary to impose CMPs against a defined set of individuals and entities that OIG determines committed information blocking. Information blocking poses a threat to patient safety and undermines efforts by providers, payers, and others to make the health system more efficient and effective. Information blocking may also constitute an element of a fraud scheme, such as forcing unnecessary tests or conditioning information exchange on referrals.

The Office of the National Coordinator for Health Information Technology (ONC) Final Rule implements certain Cures Act information blocking provisions, including defining terms and establishing reasonable and necessary activities that do not constitute information blocking or "exceptions" to the definition of information blocking. OIG and ONC have coordinated extensively on the ONC Final Rule and this final rule to align both sets of regulations.

Why and what is the OIG CMP final rule about? [3]

ONC's information blocking regulations at 45 C.F.R. Part 171 and the OIG CMP regulation at 42 C.F.R. § 1003,

subpart N, are designed to work in tandem. As a result, parties should read this OIG CMP final rule together with the ONC Final Rule. The ONC Final Rule defined "information blocking"—and specific terms related to information blocking—as well as implemented exceptions to the definition of information blocking. This final rule describes the parameters and procedures applicable to the CMP for information blocking. Using the definition from the Cures Act—which defines conduct that constitutes information blocking—is practice by an actor likely to interfere with the access, exchange, or use of electronic health information (EHI), except as required by law or specified in an information blocking exception.

A healthcare provider must provide a clear explanation for any limitations they impose on access to EHI and must make a good faith effort to provide access to as much EHI as possible. Healthcare providers are also required to make available any information blocking policies or procedures that they have in place, and provide patients with information on how to file a complaint if they believe their access to EHI has been improperly limited or blocked. This should be added into your Notice of Privacy Practices. It has not been answered at this point if and when an invoked information exception must or even should be notified to the requesting party.