Healthcare and Cybersecurity: CIRCIA's Potential Effect on Healthcare Entities

Welcome to 2023. As in 2022, we are likely to see continuing escalation of cyber intrusion threats to healthcare entities – and their data. Healthcare data breach already is far from a trivial matter – according to one expert, there have been more than 4,400 breaches during the span of 2009 to 2021 involving 500 or more records, and disclosure of healthcare records topping 300 million in number. At Bond, we will be tracking how our federal cybersecurity structure changes and adapts to these increased risks, what that means for healthcare providers and the regulations that apply to them, and how these changes aim to protect healthcare data integrity.

In March of 2022, President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), which requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. Covered entities under CIRCIA include some healthcare entities. As part of its rulemaking process, CISA issued a Request for Information last fall intended to inform its development of regulations that fundamentally may change the regulatory landscape. Review of the Request for Information is underway – and the implications of the results could be vast.

At a high level, CIRCIA ups the ante by indicating companies operating in the healthcare space and in other 'critical infrastructure' sectors report cyber incidents within 72 hours – and ransomware payments within 24 hours. In addition, by CIRCIA giving CISA the authority to develop those regulations, CISA may potentially include further compliance requirements beyond that what is currently required of healthcare entities. This important rulemaking development will continue throughout 2023, but it will not be implemented until after CISA's rulemaking becomes final.

How does CIRCIA mesh with HIPAA and the various reporting requirements within? For instance, although CIRCIA seems to provide some allowance for avoidance of duplicative reporting if there already is a functionally similar reporting requirement in place (e.g., HIPAA), it may end up that the existing reporting requirements under HIPAA, (e.g., concerning breach notification, as enforced by HHS's Office for Civil Rights), will fall below the bar and CIRCIA will require more. CISA will have a lot of say on that, and this is the first major rulemaking that this relatively new agency is taking on.

The public comments that were submitted on CIRCIA by healthcare entities are particularly telling. Organizations spell out concerns about duplication and unnecessary confusion; a number stressed the importance of cleanly implementing the CIRCIA provision that precludes CISA from requiring duplicative reporting (see CIRCIA at Section 2242(a)(5)(B)). Others emphasized that required reporting only should comprise data absolutely necessary for governmental operations, so as to protect data integrity wherever possible and to, where necessary, allow ongoing 'ransom' negotiations to continue out of the limelight when that benefits data retrieval efforts.

As CISA develops CIRCIA regulations during 2023, Bond will be watching closely. In the meantime, we encourage readers to avail themselves of useful healthcare cybersecurity resources, including those of the '405(d)' task group (of which this author is a member), and for those readers in New York State, the New York Healthcare Cyber Alliance (which this author co-chairs) continues its work of linking healthcare delivery organizations to the resources that can improve their cyber posture.

For more information regarding healthcare and data privacy, contact Gabriel Oberfield or any attorney in Bond's cybersecurity and data privacy practice.

BOND SCHOENECK & KING ATTORNEYS