CISA's CIRCIA NPRM Advances the March Toward Heightened Reporting – Yet the Jury Still Is Out on How CIRCIA Will Affect Healthcare

Remember CIRCIA? The Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA") – intended to beef up reporting requirements across industries following cyber incursions – is moving along the pathway from concept to final rule. In early 2023, we wrote about CIRCIA's potential fundamentally to change reporting requirements concerning compromise of healthcare data. Fast forward to April 2024: now the Cybersecurity and Infrastructure Security Agency ("CISA") has published its Notice of Proposed Rulemaking (NPRM) for CIRCIA in the Federal Register, and CIRCIA's likely effects on the healthcare industry are coming into finer focus.

As a reminder – in 2022 President Biden signed CIRCIA into law, tasking CISA with developing and implementing regulations requiring Covered Entities ("CEs") to report certain cyber incidents and ransomware payments to CISA. At the time, CISA signaled that some of these CEs would be in healthcare (among other wide-ranging 'critical' industries). CISA issued a Request for Information ("RFI") intended to inform its development of regulations.

Within our earlier piece that summarized the RFI, we signaled that CIRCIA could result in changes in the content and frequency of reporting for healthcare entities by requiring covered 'critical infrastructure' sectors to report cyber incidents within 72 hours, and ransomware payments within 24 hours. We flagged that there may be some bumpiness as between CIRCIA and standards like the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which has its own definitions for CEs and attendant reporting standards, all which may not neatly overlay with CIRCIA.

The recently issued NPRM includes guidance surrounding the developing definition of CEs under CIRCIA, covered cyber incidents, reporting requirements and enforcement mechanisms. Details from the NPRM relevant to the healthcare sector are below:

Covered Entities

CIRCIA defines a CE as "an entity in a critical infrastructure sector, as defined in Presidential Policy Directive 21", within which one will find the health and public health industries.[1] Under the NPRM, CISA proposes two additional requirements: (1) a sized-based criterion; and (2) a sector-based criterion. The sized-based criterion derives from U.S. Small Business Administration ("SBA") definitions, and CISA envisions small businesses generally to be excluded from CIRCIA responsibilities. That noted, CISA included sector-based criteria that overlay and hale in some healthcare providers, e.g., certain entities that provide direct patient care, manufacturers of certain essential drugs and manufacturers of certain medical devices.

Drilling down, CISA specifies that in its vision, direct care would be synonymous with healthcare entities operating: (1) hospitals with one hundred or more beds; or (2) critical access hospitals. As for drug manufacturers, the NPRM signals that manufacturers listed in Appendix A of the Essential Medicines Supply Chain and Manufacturing Resilience Assessment would be haled into CIRCIA, while device manufacturers would

1 This directive will be retired and replaced by directive 22.

include Class II and III devices as defined in 21 U.S.C. 360c.

Covered Cyber Incidents

The NPRM signals CISA's interest only in receiving reporting on "substantial" cyber incidents. Under the NPRM, substantiality is defined as:

1. Substantial loss of confidentiality, integrity, or availability of information;
2. Serious impact on safety and resiliency of operational systems and processes;
3. Disruption of ability to engage in business or industrial operations, or deliver goods or services; or
4. Unauthorized access facilitated through or caused by a: (1) compromise of a cloud service provider, managed service provider, or other third-party data hosting provider; or (2) supply chain compromise.

Supplemental reports would be due to CISA when: (1) substantially new or different information becomes available; or (2) the CE makes a ransomware payment in connection with a previously reported incident.

Enforcement

Under the NPRM, CISA would have three enforcement mechanisms to drive CE compliance with the reporting requirements: (1) a request for information (RFI) from CISA to the provider in question; (2) subpoena power; and (3) the power to refer for suspensions, debarment, and contracting actions.

Where the Rubber Will Meet the Road with Healthcare

The NPRM also includes a limited set of exceptions to the reporting requirements, including one envisioned when a CE is required to submit substantially similar information within a substantially similar timeframe to another federal agency that has an information sharing agreement and mechanism with CISA. It remains to be seen whether HIPAA reporting requirements both will meet the substantial similarity standard and if HHS will establish an information sharing agreement with CISA. We will be watching closely as substantiality is better defined by CISA through its rulemaking process, as are the standards for agency information sharing.

Next Steps

Public comment on the NPRM is expected to end on June 3, 2024, and in 2025 the final rule is likely to be published, following CISA's integration of public comment and its implementation of adjustments to the proposed rule. More information on the process may be found here, including a CISA slide deck, here. In the interim, Bond will watch the development of the proposed rule closely, including by leveraging knowledge gleaned through the Federal 405d task group, of which Mr. Oberfield is a member.[2] We recommend that healthcare organizations continue to evaluate their cybersecurity policies and procedures with the expectation that CIRCIA will result in new or otherwise modified reporting requirements, once implemented.

For more information regarding healthcare and data privacy, contact Gabriel Oberfield, Victoria Okraszewski, CIPP/US or any attorney in Bond's cybersecurity and data privacy practice or in the firm's health care and long

2 This piece is informed by materials Mr. Oberfield gleaned earlier in April while attending a function tied to the 405d working group's activities, at which CISA leadership presented on CIRCIA.