Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Proposed Regulations

4/30/2024

On April 4, 2024, the U.S. Department of Homeland Security published a proposed rule to implement the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). CIRCIA requires any critical infrastructure company (a covered entity under the statute) to report to the Cybersecurity and Infrastructure Security Agency (CISA) within certain prescribed timeframes any substantial cyber incident (a covered event), ransom payment made in response to a ransomware attack, and any substantial new or different information discovered related to a previously submitted report.

CISA estimates that the proposed rule will apply to approximately 316,000 covered entities, whom are in one of 16 enumerated Critical Infrastructure sectors and either (i) do not qualify as a small business as defined by the Small Business Administration, or (ii) meet a sector-based criterion. According to CISA under the Healthcare and Public Health (HPH) Sector-Specific Plan, the "HPH Sector is large, diverse, and open, spanning both the public and private sectors. It includes publicly accessible healthcare facilities, research centers, suppliers, manufacturers, and other physical assets and vast, complex public-private information technology systems required for care delivery and to support the rapid, secure transmission and storage of large amounts of HPH data."

CISA's summary of the rule proposal may be found here and Critical Infrastructure Sector information may be found here.

Click Here to read the entire April 2024 Healthcare Law Update now!

For additional information or for assistance with your organization's privacy and security program, contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com