New Reporting Requirements for Cyber Incidents and Ransomware Payments under the Strengthening American Cybersecurity Act of 2022

On March 15, 2022, President Biden signed into law the Strengthening American Cybersecurity Act of 2022, which, among other things, seeks to improve cybersecurity disclosures and protections by operators of federal infrastructure and federal civilian agencies. The new law requires critical infrastructure sectors, defined under Presidential Policy Directive 21 (PPD-21) to include healthcare and public health, to:

- Report to the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) any substantial cyber incidents within 72 hours and ransomware payments within 24 hours.
- Submit follow-up reports to CISA.
- Preserve, and possibly produce to CISA, certain data related to the cyber incident or ransomware payment.

Reports may be designated as proprietary and will be treated accordingly, cannot be used for enforcement or other regulatory actions, and are not subject to disclosure under the Freedom of Information Act. The new reporting requirements will become effective once CISA promulgates its final regulations, including what specific entities within each critical infrastructure sector must report and what specific types of cyber incidents and payments must be reported.

Stakeholders will need to update their cybersecurity compliance programs to ensure compliance with these new reporting requirements once the final regulations are promulgated by CISA.

Click Here to read the full April 2022 Healthcare Law Update now!

For more information, contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com
Joseph M. Gorrell | 973.403.3112 | jgorrell@bracheichler.com
Edward J. Yun | 973.364.5229 | eyun@bracheichler.com