BRACH | EICHLER LLC 973.228.5700 www.bracheichler.com

Guidance on Multi-Factor Authentication and Smishing

9/30/2023

The U.S. Department of Health & Human Services, Office of Information Security and the Health Sector Cybersecurity Coordination Center have issued joint guidance on Multi-Factor Authentication and Smishing. Multi-factor authentication (MFA) requires computer system users to go through multiple authentication steps in order to use the system or software within the system. MFA provides another layer of access protection over single-factor authentication. Smishing is a form of phishing in which an attacker uses a compelling text message to trick targeted recipients into clicking a link, which sends the attacker private information or downloads malicious programs to a smartphone or smart device. The guidance is intended to assist health care organizations in addressing the top five cyber threats in health care: (i) phishing/smishing, (ii) ransomware attacks, (iii) data breaches, (iv) distributed denial of service (DDoS) attack, and (v) info-stealing malware.

Click Here to read the entire September 2023 Healthcare Law Update now!

If you need assistance with your HIPAA compliance program, an OCR investigation, or a data breach incident, please contact:
Lani M. Dornfeld, CHPC | 973.403.3136 | ldornfeld@bracheichler.com