COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 1. January 13, 2022
Security Experts' Checklists for 2022

By Jane Anderson

Security experts listed several top strategies for covered entities (CEs) and business associates (BAs) to prioritize this year.[1]

Chuck Everette, director of cybersecurity advocacy at cybersecurity company Deep Instinct, offered 10 must-do items for health care entities to address in 2022:

1. Plan for security threats in advance by having an incident response plan ready to go at a moment's notice.
2. Have a prevention-first mentality, and test annually.
3. Enforce multifactor authentication on all systems and don't allow the use of a single password on multiple systems.
4. Patch vulnerabilities and stay up to date on operating systems, software and firmware on all devices.
5. Limit your "attack blast zone" by employing network segmentation and limiting administrator rights with a strategy of least privilege.
6. Have a solid backup plan, such as an off-site, air gap solution that includes frequent and comprehensive backups, and don't depend on local backup or rollback features, since these are often the first targets of an attack.
7. Enable strong spam filters to prevent phishing emails from reaching end users.
8. Require annual security awareness training for all employees.
9. Limit false positives in order to reduce alert fatigue.
10. Consider cyber insurance coverage.