October 2018 OCR Cybersecurity Newsletter

National Cybersecurity Awareness Month

Every October, the federal government and its partners celebrate National Cybersecurity Awareness Month. This is a coordinated effort between government and industry organizations to promote the importance of cybersecurity and increase awareness of the threats to the confidentiality, integrity, and availability of sensitive electronic data. Within the healthcare industry, such data includes electronic protected health information (ePHI).

Because ePHI identifies individuals and includes information regarding an individual's health, treatment, or treatment payment information, it presents a tempting target for bad actors – especially identity thieves. On the black market, ePHI is often more valuable than other types of personal data because it can be used to steal identities and commit healthcare fraud.

However, there are many basic cybersecurity safeguards that HIPAA covered entities and business associates can deploy to greatly reduce the impact of attempted cyberattacks. National Cybersecurity Awareness Month is an opportunity to review some of these safeguards.

Cybersecurity Safeguards

- **Encryption**: Encryptions is the conversion of electronic data into an unreadable or coded form that is unreadable without a decryption key. The proper use of encryption can prevent unauthorized users from viewing encrypted data in a usable form and may substantially reduce the risk of compromising ePHI. HIPAA covered entities and business associates are required to assess whether encryption is a reasonable and appropriate safeguard as a means of protecting ePHI at rest (i.e., ePHI that is stored such as on a computer's hard drive or on electronic media) and ePHI that is electronically transmitted. See 45 CFR §§164.312(a)(2)(iv), 164.312(e)(2)(ii).
- **Social Engineering**: Phishing remains one of the most common and effective social engineering tactics for stealing user credentials and other sensitive information. Malicious actors send deceptive emails to users, enticing them to disclose login credentials or click links that may install malware (malicious software). The effectiveness of phishing attacks can be greatly reduced with proper training to keep information system users aware of the threats of phishing attacks and helps users identify suspicious emails. The Security Rule requires covered entities and business associates to implement security awareness and training programs for all workforce members including management. See 45 CFR § 164.308(a)(5)(i).
- **Audit Logs**: Network and system activity can be recorded and monitored with logs, which are a record of events and information pertaining to whatever device, system, or software they are monitoring. Audit logs are an important security tool that allows organizations to detect suspicious activities as they are occurring and can be used to reconstruct events that happened

in the past. In order to be effective, the information contained in logs should be reviewed on a regular basis. The HIPAA Security Rule requires the implementation of audit controls, i.e., safeguards to record and examine activity on information systems that contain or use ePHI (see 45 CFR § 164.312(b)) and to regularly review records of information system activity, such as audit logs. See 45 CFR § 164.308(a)(1)(ii)(D).

- **Secure Configurations**: Proper configuration of network devices and software will reduce the attack surface for bad actors and greatly improve an organization's cybersecurity defenses. The aforementioned tools – encryption, anti-malware, and audit logs – require appropriate settings in order to function as intended. If encryption safeguards are not implemented correctly and do not use the latest versions, the encryption solution may be compromised or bypassed. Anti-malware software settings determine what files or devices are scanned and how often. Maintenance and updating of malware definitions will ensure that the software is providing maximum protection. Proper log configuration is also essential to effective network defense. If logs do not collect and retain the correct data, suspicious activity may go unnoticed. Furthermore, logs should be protected against unauthorized manipulation or deletion, which is a common tactic malicious actors use to cover their tracks. These are just a few examples of network components that require proper configuration to provide effective cybersecurity defense. The configuration of firewalls, workstations, routers, servers, and other components all play an important role in minimizing the chance of security incidents. See 45 CFR §§ 164.306(e), 164.308(a)(8), 164.312(a)(1), 164.312(a)(2)(iv), 164.312(b), 164.312(c), and 164.312(e)(2)(ii).

References

- *Encryption Basics* from the National Institute of Standards and Technology (NIST) https://www.nist.gov/publications/encryption-basics
- HHS OCR *Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals* https://www.hhs.gov/hipaa/for-professionals/breach-notification/guidance/index.html
- NIST Special Publication (SP) 800-128: *Guide for Security-Focused Configuration Management of Information Systems* https://csrc.nist.gov/publications/detail/sp/800-128/final

* *This document is not a final agency action, does not legally bind persons or entities outside the Federal government, and may be rescinded or modified in the Department's discretion. Noncompliance with any voluntary standards (e.g., recommended practices) contained in this document will not, in itself, result in any enforcement action.*