September 2017

National Cybersecurity Awareness Month

Are you getting ready for National Cybersecurity Awareness Month? Every October, the federal government and its industry partners celebrate National Cybersecurity Awareness Month (NCSAM). The security of electronic health information is more critical than ever, and it is the responsibility of all in the regulated community to ensure the confidentiality, integrity, and availability of electronic protected health information (e-PHI). NCSAM provides an opportunity to review cybersecurity tips, both generally and related specifically to e-PHI; and to review the obligations of HIPAA covered entities and business associates to protect e-PHI.

Next month, in celebration of NCSAM, consider going "back to basics," and strengthening your cybersecurity for e-PHI!

Back to Basics (Basic Cybersecurity Tips)

- **Have a Strong Password.** Make sure you use a strong password (i.e. usually 10 characters or more and includes uppercase and lowercase letters, numbers, and special characters like #$&*). Recent research suggests users could also consider using "passphrases," which are sentences that may be easier to remember than a very complex password (e.g. "I got a pony for my 8th birthday!")[1]. Do not use passwords or phrases that would be easy to guess, such as a pet's name or your birthdate.[2]
- **Training**. Train your staff regularly on important cyber security issues, such as how to spot phishing e-mails and when/who to report possible cyber incidents to in your business. For more on phishing e-mails look back at Newsletter #16.
- **Multi-factor Authentication.** A username and password may not be adequate to protect sensitive information, privileged accounts, or information accessed remotely. As part of its risk analysis, an entity should determine what authentication schemes to use to protect its systems and sensitive information (e.g. e-PHI). Multi-factor authentication typically includes a password and additional security measures, such as a thumbprint or key card.
- **Updates and Patching.** You should update and patch your systems and applications regularly, because updates and patches often fix critical security vulnerabilities.

[1] For more information, please see *Appendix A-Strength of Memorized Secrets* from *NIST Special Publication 800-63B Digital Identity Guidelines* available at: https://pages.nist.gov/800-63-3/sp800-63b.html.
[2] For additional tips on creating strong passwords visit: https://www.stopthinkconnect.org/tips-advice/general-tips-and-advice.

- **Lock Devices.** Limit physical access to devices and lock devices when not in use.
- **Portable Devices**. Be cautious plugging a phone, USB, or other portable device into a secure computer or network. Portable storage devices may not be as secure and may contain malicious software that could corrupt your secure network. If the device is needed, be sure to follow your organization's policies on the use of such devices, which could include prohibitions on the use of personal devices or having IT personnel review such devices to ensure they do not contain malicious software.
- **Do Not Wait.** Do not wait to report possible cybersecurity threats to the right people in your organization. Time is often critical during a cyber-incident, so if you suspect a cyber-threat, report it right away.

For more tips, visit Department of Homeland Security and National Cyber Security Alliance. Both DHS and NCSA provide additional information on securing computers and networks.

Cyber Security and e-PHI

- **Be Aware.** Be aware of your responsibilities as a covered entity or business associate under HIPAA. *See* 45 C.F.R. Parts160 and164. Also, be aware of current threats and trends in cyber security, so you can take action and update security measures as needed.[3]
- **Plan.** Covered entities and business associates are required to have security incident procedures and response plans in place, as well as contingency plans to ensure effective, concentrated, and coordinated means to respond to and recover from security incidents. These policies, procedures, and plans should provide a roadmap for response and recovery activities, be approved by management, and be reviewed and tested regularly.[4]
- **Respond.** Once a security incident is detected, the entity should immediately take steps to analyze the incident in order to contain its impact and propagation, eradicate the incident, remediate vulnerabilities that permitted the incident, recover from the incident and conduct post-incident activities.[5] You should also take steps to mitigate any impermissible disclosure of protected health information.
- **Report.** Breaches of e-PHI affecting more than 500 individuals must be reported to OCR, affected individuals, and the media as soon as possible, but no later than 60 days after the discovery of the breach. Breaches affecting fewer than 500 individuals must be reported to the affected individuals as soon as possible, but no later than 60 days after the discovery of the breach, and to OCR no later than 60 days following the calendar year the breach was discovered. Entities may delay its reporting of a breach if such a delay is requested by a law enforcement official. OCR encourages entities to report all cyber threat indicators to federal information-sharing and analysis organizations (ISAOs), such

[3] For more information on reporting and monitoring, review Newsletter #13.
[4] *See* 45 C.F.R. § 164.308(a)(7), *see also* Security 101 for Covered Entities, *see also* Newsletter #15.
[5] For more information on responding to a cybersecurity incidents review Cyber Attack Checklist and OCR's Ransomware Guidance.

as those maintained by the Department of Homeland Security and HHS Assistant Secretary for Preparedness and Response, as well as to private-sector cyber threat ISAOs. **Do not include PHI in these reports. OCR does not receive such reports from its federal or HHS partners.**

The HHS Office for Civil Rights (OCR) web site provides guidance on the HIPAA Security Rule as well as guidance on specific cybersecurity topics. We recommend you bookmark these pages so you can refer to them easily whenever you have a question or need some guidance.