Health Information Compliance Alert

Clip And Save: Cybersecurity: Update Your Health IT Glossary with These 10 Additions

As hackers push the healthcare envelope, HIT needs more terms to address issues.

With many of this year's large-scale HIPAA breaches attributed to hackers and cyber criminals, it's a great time to look at the ever-evolving list of cybersecurity terminology to get ready for 2018. Keeping in sync with the hot topics in health IT allows your practice to prepare for and be part of healthcare's security conversation - and protect your practice in the process.

Bulk up your office's digital dictionary with these ten cybersecurity must-knows:

1. Brute Force: A cyber-hijack that involves brute force breaks systems by repeatedly trying different passwords until finding one that finally works. Once the encryption is compromised, the hackers can take down the system. Find a great overview of brute force attacks on healthcare and how to combat them by the Department of Homeland Security's at: www.dhs.gov/sites/default/files/publications/Encryption-Software-TN_0913-508.pdf.

2. Cloud Computing: This type of health IT is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service-provider interaction," instructs the National Institute of Standards and Technology (NIST). Cloud computing remains a popular, cost-saving technology in healthcare with a plethora of certified vendors, but recent HHS Office for Civil Rights data attributes some common breach issues to problems with poorly configured systems with the culprit - cloud computing technologies. (See Health Information Compliance Alert, Vol. 17, No. 7.)

3. DDoS Attack: Distributed Denial of Service attacks wiggle into your systems and attack your resources, literally stopping your ability to do business. "Hackers accomplish a DDoS attack by literally sending so much web traffic at a target that it is unable to function," notes the Department of Homeland Security's fact sheet on DDoS attacks. A famous DDoS healthcare case involved the takedown of Boston Children's Hospital's servers in 2014 by hackers from the group Anonymous.

4. Handshake Traffic: This back-and-forth greeting centers on the agreement of two systems to do business. Technically speaking, it refers to the "protocol dialogue between two systems for identifying and authenticating themselves to each other, or for synchronizing their operations with each other," the NIST guidance says.

5. Internet of Things: Also known as the IoT, the Internet of Things concerns the connection of devices, systems, objects, and more to the Internet. This coordination supports the idea that connecting everything in your office and life will make practicing medicine more efficient and easier - but, that's not always the case. With each new hook up, the opportunity for the loss of electronic protected health information (ePHI) rises.

6. Jailbreak: This is a slang term that concerns the override of restrictions, usually on mobile devices like cellphones and tablets, in order to decrypt and install malware, illegal software, and/or other barred applications. For this reason, it is critical to keep all your practice devices locked with multi-factor authentication and at-rest protocols as hackers may attempt to jailbreak a mobile unit when you leave these tools unattended.

7. KRACK: Key Reinstallation Attacks, or KRACKs, happen when a hacker uses weaknesses in Wi-Fi systems. "An attacker within the wireless communications range of an affected [access point] AP and client may leverage these vulnerabilities to conduct attacks that are dependent on the data confidentiality protocol being used," says the United States Computer Emergency Readiness Team (CERT) in vulnerability report VU #228519 on the problem. The only way

to eradicate KRACK issues is to consistently install updates to impacted products. See the US-CERT report at: www.kb.cert.org/vuls/id/228519/.

8. Mobile Device Management: Often referred to under its acronym MDM, mobile device management covers the administration of a practice's mobile devices, and also the security, updates and upgrades, implementation, and protection of these devices. MDM software helps with the organization of your office cellphones, tablets, and laptops to ensure the protection of ePHI.

9. 2FA: Formerly known as two-factor authentication, this type of encryption increases the protection of your devices by requiring both a password and another security measure. This adds another layer of user authentication for covered entities to protect electronic protected health information (ePHI). (For more a more in-depth study of this topic, See Health Information Compliance Alert, Vol. 16, No.12.)

10. Virtual Private Network: Though many remote users know this term under its acronym VPN, they often don't know what it means. A VPN allows you to securely share your health data in a public network through the utilization of a private and secure network. The VPN offers you online protection virtually, and the utilization of a secure VPN remains a top tip to "help secure and protect PHI on mobile devices," according to the October 2017 edition of the HHS Office for Civil Rights Cybersecurity Newsletter.