Healthcare & Public Health Sector Coordinating Councils
PUBLIC PRIVATE PARTNERSHIP

Protecting the Healthcare Digital Infrastructure: Cybersecurity Checklist

The Healthcare and Public Health (HPH) Sector's ability to coordinate facility operations and provide life-saving health services are influenced by the computer networks, databases, and wireless systems that make up the digital infrastructure within a healthcare organization. This equipment and information is unfortunately prone to attack from individuals who seek to cause catastrophic harm to the HPH Sector and other entities that are critical to our nation's people, economy, and national security.[i] In order to mitigate cyber threats and strengthen cybersecurity in the HPH Sector, potential vulnerabilities must be identified and addressed. The following introductory checklist outlines several hardware, software, and cybersecurity educational items organizations should consider and implement to protect their digital infrastructure.[ii,iii,iv,v,vi]

How do you protect computer hardware and other technological equipment?

- ☐ Secure all computer equipment and servers in a locked storage area with specific individual access permissions
- ☐ Identify lost or stolen laptops and devices immediately; establish appropriate procedures to report lost items for employees
- ☐ Develop and implement procedures to prevent unauthorized data transfer via USB drives and other portable devices
- ☐ Wipe content on all devices before they are discarded or transferred to others
- ☐ Establish policies and procedures to disable inactive accounts, including those of transferred or terminated employees, after a set time period
- ☐ Set automatic timeouts for all computers following a period of inactivity
- ☐ Monitor, log, and report all intrusions to the appropriate authorities
- ☐ Review manufacturer technical safeguards, standards, and incident reports of all medical devices that are issued to patients to reduce malware and other security risks
- ☐ Develop and implement a detailed plan of how to address potential cybersecurity vulnerabilities with medical devices

[i] The White House National Security Council. Cybersecurity. http://www.whitehouse.gov/cybersecurity
[ii] National Cybersecurity Alliance. http://www.staysafeonline.org/
[iii] U.S. Department of Health and Human Services. Office of the National Coordinator for Health Information Technology. http://www.healthit.gov/providers-professionals/ehr-privacy-security/10-step-plan
[iv] U.S. Department of Homeland Security. U.S. Computer Emergency Readiness Team. Cyber Security Guidance. http://www.us-cert.gov/reading_room/poster_1.pdf.
[v] U.S. Department of Commerce. National Institute of Standards and Technology. Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53). http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800_53_r4_draft_fpd.pdf.
[vi] U.S. Department of Health and Human Services. U.S. Food and Drug Administration. Medical Devices. http://www.fda.gov/MedicalDevices/default.htm.

How do you protect local networks and other computer software?

- Conduct a computer network assessment to obtain the information you need to develop a cybersecurity plan to reduce cyber attacks and address breaches
- Encrypt all computers and mobile devices issued by the organization; preapprove the use of any devices not issued by the organization
- Implement role-based access to any systems to ensure employees only have access to any programs and applications necessary to perform the functions of their job
- Prevent the installation of any peer-to-peer software applications
- Perform regular desktop audits for the entire organization to ensure unauthorized software applications are not installed
- Install and regularly update anti-virus software on all network computers
- Conduct anti-virus scans on all incoming and outgoing files
- Research and build the necessary firewalls to protect against intruders
- Develop security policies for the use of virtual private network or remote connections
- Configure any electronic health records (EHR) system or database to require specific access permissions for each user; inquire with the EHR vendor to determine how they provide updates and technical support
- Backup data regularly and develop a plan to access information quickly in case of a natural or manmade disaster

How do you encourage safe computer & cyber practices from employees & staff?

- Define policies and procedures for employee use of your organization's information technologies
- Employ a system use notification banner before granting employees access to the system that informs them of applicable regulations and federal laws (i.e. system usage may be monitored, recorded, and subject to audit and unauthorized use of the system is prohibited and subject to criminal and civil penalties)
- Conduct information and cyber security awareness trainings and brown bag workshops to educate employees about phishing scams, spyware, and identity theft on initial hire and on annual basis; employees should also be aware of how to report and respond to suspicious cyber events
- Require employees and staff to utilize strong passwords for networks and systems with a combination of letters, numbers, and special characters
- Require frequent password resets for all systems
- Implement multiple authentication methods for computers and networks
- Establish policies prohibiting the transmittal of protected health information using unencrypted public networks (i.e. free Wi-Fi hotspots)