MLMIC
MLMIC Insurance Company
a Berkshire Hathaway company

Two Park Avenue, New York, NY 10016
(212) 576-9800 | (800) 275-6564 | MLMIC.com
New York City | Latham | Syracuse | Long Island | Buffalo

Tip# 24: Security of Patient Information and Health Information Technology

The Risk: With virtually all medical offices and healthcare facilities connected to the internet and using computer systems for the practice of medicine, maintaining the security of computers and other electronic devices, as well as the privacy of patients' protected health information (PHI), has become critical.

The following are tips for staff and providers on securing this technology and information.

Recommendations:

1. Require that staff and providers have strong and unique passwords:
    a. Passwords should have a minimum number of 12 characters and include upper and lower-case letters, numbers and symbols.
    b. Passwords should be changed at set intervals.[1]

2. Do not share passwords:
    a. Do not allow others to document in an electronic health record (EHR) under your password, while you are logged on.

3. Grant staff access to an EH only on a "need to know" basis:
    a. Individuals should be granted access only to the information necessary to perform his/her job.
    b. If an employee transfers to a different job function, have a process in place to reduce or increase their access based on the new job functions.

4. Educate staff regarding not:
    a. plugging in their personal devices to USB ports on the system's computers;
    b. installing software on their work computers without prior approval;
    c. clicking on suspicious links in emails; and
    d. allowing USB devices to leave the facility unencrypted.

5. Position computers and printers away from patient and visitor traffic:
    a. Consider the use of screen filters to prevent visualization of PHI by others.

[1] Current guidelines suggest that if the password length is set to 16 characters, it should be changed annually at a minimum.

6. Encrypt all computer hard drives. At a minimum, all laptops and tablets should be encrypted, especially if they are to leave the facility.

7. Provide frequent and ongoing cybersecurity education and training.

8. Policies and procedures should clearly define the disciplinary actions to be taken for the inappropriate use of the computer system.

9. Develop a cybersecurity incident response process to address a security breach or cyberattack, and test it at least annually to confirm that there is:
    a. a defined procedure for reporting any suspected information security incident;
    b. an obligation for employees to report any suspected incident immediately upon discovery; and
    c. an individual(s) with clearly assigned responsibilities for managing incidents.

10. Promptly disable an individual's access to the computer system upon their leaving employment:
    a. For involuntary dismissal, disable access prior to the notification of termination.
    b. If access to the employee's emails, voicemail, etc. is necessary, assign another qualified individual to address any information that requires review or action.

11. Maintain inventory control of all computerized devices including laptops, thumb drives, handheld devices, etc.

12. Install appropriate anti-virus software and update devices frequently to protect the computer system from security vulnerabilities.

13. Perform system back-ups of files and data routinely:
    a. Test back-up restoration semi-annually, at a minimum.

14. Perform audits to assure compliance with health information technology policies and any applicable regulations.