MLMIC
MLMIC Insurance Company
a Berkshire Hathaway company

(800) 275-6564 | MLMIC.com
New York City | Latham | Syracuse | Long Island | Buffalo

USE OF TECHNOLOGY CHECKLIST #4

SECURITY OF PATIENT INFORMATION AND HEALTH INFORMATION TECHNOLOGY

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.

	YES	NO
1. Staff and providers are required to have strong and unique passwords: • Passwords have a minimum number of 12 characters and include upper and lower-case letters, numbers and symbols. • Passwords are changed at set intervals.	□	□
2. Passwords are not shared: • Others are not allowed to document in an electronic health record (EHR) under another person's password, while they are logged on.	□	□
3. Staff are granted access to an EHR only on a "need to know" basis: • Individuals are granted access only to the information necessary to perform his/her job. • If an employee transfers to a different job function, a process is in place to reduce or increase access based on the new job functions.	□	□
4. Staff have been educated regarding not: • plugging in their personal devices to USB ports on the system's computers; • installing software on their work computers without prior approval; • clicking on suspicious links in emails; and • allowing USB devices to leave the facility unencrypted.	□	□
5. Computers and printers are positioned away from patient and visitor traffic: • The use of screen filters to prevent visualization of PHI by others has been considered.	□	□
6. All computer hard drives are encrypted. At a minimum, all laptops and tablets are encrypted, especially if they leave the facility.	□	□
7. Frequent and ongoing cybersecurity education and training are provided.	□	□
8. Policies and procedures clearly define the disciplinary actions to be taken for the inappropriate use of the computer system.	□	□

SECURITY OF PATIENT INFORMATION AND HEALTH INFORMATION TECHNOLOGY(continued)	YES	NO
9. A cybersecurity incident response process has been developed to address a security breach or cyberattack, and it is tested at least annually to confirm that there is: • a defined procedure for reporting any suspected information security incident; • an obligation for employees to report any suspected incident immediately upon discovery; and • an individual(s) with clearly assigned responsibilities for managing incidents.	□	□
10. An individual's access to the computer system is promptly disabled upon their leaving employment: • For involuntary dismissal, access is disabled prior to the notification of termination. • If access to the employee's emails, voicemail, etc. is necessary, another qualified individual is assigned to address any information that requires review or action.	□	□
11. Inventory control is maintained for all computerized devices including laptops, thumb drives, handheld devices, etc.	□	□
12. Appropriate anti-virus software has been installed and devices are updated frequently to protect the computer system from security vulnerabilities.	□	□
13. System back-ups of files and data are performed routinely: • Back-up restoration is tested semi-annually, at a minimum.	□	□
14. Audits are performed to assure compliance with health information technology policies and any applicable regulations.	□	□