HIPAA Compliance checklist for IT admins

“This checklist covers the key strategies an IT admin must adopt to maintain HIPAA compliance in the industry”

TRACK AND MONITOR ePHI

□ Do you keep track of all the folders and files that contain ePHI* (Electronically Protected Health Information) in your organization?

□ Have you maintained detailed records of who accesses protected patient information, including the time and location of access?

□ Do you monitor the real-time location of work devices that contain protected health information?

MANAGE ACCESS TO ePHI

□ Do you restrict employees’ access to ePHI such that only those with the right privileges may access and edit it?

□ Do you authenticate employees with MFA/passwords/biometrics, before granting them access to a patient's ePHI?

□ Do you ensure that staff members do not use personal accounts to send or receive protected patient information?

*Examples of Electronically Protected Health Information (ePHI) can range from MRI scans to blood test results, and may also include a name, social security number, or phone number. Oftentimes, it may also include a home address or credit card information as well

PROTECT AND SAFEGUARD ePHI

- □ Is it mandatory in your company to connect to a VPN before accessing a patient's protected health information?
- □ Have you ensured that your business associates appropriately safeguard the patient’s protected health information entrusted to them?
- □ Does your company provide training on HIPAA policies to ensure that employees stay in compliance with HIPAA rules and regulations?
- □ Do you ensure that your policies are verified by notable HIPAA compliance professionals?
- □ For employees who use personal devices to access protected health information, have you enforced BYOD policies to secure ePHI?
- □ Do you dispose of outdated and inessential ePHI in a safe and secure manner?

SECURE DEVICES THAT STORE ePHI

- □ Do you enforce restrictions and security configurations on devices that store ePHI?
- □ Do you ensure devices that store ePHI have encryption turned on and are secured with strong passwords?
- □ If required, do you possess the ability to remotely lock, or in worst cases wipe the protected health information stored on company devices?
- □ Do you ensure your work devices are updated to the latest patches and operating systems?

□ Have you enabled firewall and installed antivirus software on work devices?

□ Have you blocked your employees from accessing suspicious apps and websites on devices that contain ePHI?

□ If required, do you possess the ability to lock down devices that wander outside the specified operation zones?

AUDITING AND REPORTING

□ Do you regularly review your data security measures and perform organization-wide risk analysis to detect faulty processes or loopholes?

□ Do you perform regular checks to verify that employees adhere to HIPAA policies?

□ Do you document your HIPAA compliance policies and lay out proper remedial plans to counter any potential gaps in compliance?

□ Do you regularly monitor the health and status of devices that contain ePHI?

□ Do you keep a record of the applications installed on work devices that contain ePHI?

□ Do you maintain and manage a history of the location details of work devices that store your patient's ePHI?