# Is your PHI securely protected in compliance with HIPAA?


Can your organization ensure that your medical records and patient information are being protected? The Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires anyone who handles medical information such as healthcare providers and insurance companies, to secure Protected Health Information (PHI), exchange data electronically, and protect patient information. Risks of noncompliance can include fines as much as $1.5 million per violation.[1] When implementing a system to help safely protect sensitive PHI use this checklist to make sure your bases are covered:

## HAVE YOU DEVELOPED POLICIES AND PROCEDURES FOR PROVIDING PATIENTS WITH ACCESS TO THEIR HEALTH INFORMATION?

- ☐ Are you providing individuals with access to their health information on request?
- ☐ Are you providing individuals copies of their health information in a timely matter and within 30 days?

## DO YOU CREATE AND MONITOR PHI ACCESS LOGS?

- ☐ Do you know when and how records were retrieved and accessed with detailed audit trails to ensure documents are being protected?
- ☐ Are access logs routinely monitored to identify unauthorized access?
- ☐ Does your organization restrict access to medical records with strong security settings to ensure PHI privacy and confidentiality?

## HAVE YOU DEVELOPED POLICIES AND PROCEDURES COVERING DISPOSAL OF PHI?

- ☐ Have you developed policies and procedures for permanently erasing PHI after a minimum of 6 years or recommended 21 years?
  - ☐ Paper Documents
  - ☐ Electronic Documents
- ☐ Do you know how long you are suppose to keep the specific medical documents according to regulations?

## IS YOUR PHI PROTECTED WITH ENCRYPTIONS?

- ☐ Are you able to ensure the confidentiality, integrity and availability of PHI?
- ☐ Have you implemented controls to guard against unauthorized access of PHI during electronic transmission and at rest?

## HAVE THE FOLLOWING ANNUAL AUDITS/ ASSESSMENTS REQUIRED BY HIPAA COMPLIANCE BEEN COMPLETED?

- ☐ Security Risk Assessment
- ☐ Privacy Assessment
- ☐ Security Standards Audit
- ☐ Asset and Device Audit
- ☐ Physical Site Audit
- ☐ HITECH Subtitle D Audit

## HAVE ALL EMPLOYEES GONE THROUGH HIPAA TRAINING?

- ☐ Do you have documentation to confirm each employee has completed their annual training?
- ☐ Is there a staff member designated as the HIPAA Compliance, Privacy, and/or Security Officer?

## DO YOU HAVE POLICIES AND PROCEDURES IN ACCORDANCE WITH HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULES?

- ☐ Have all your employees read and legally attested to HIPAA policies and procedures?
- ☐ Do you have documentation of their legal attestation?
- ☐ Do you have documentation for annual reviews of your policies and procedures?

[1] https://www.ama-assn.org/practice-management/hipaa-violations-enforcement



DIGITECH SYSTEMS

**Now that you know what questions you need to answer, ensuring that you are in compliance with HIPAA will be a breeze.**
Contact us if you need help protecting your information! • www.digitechsystems.com/hc