Is your PHI protected in compliance with HIPAA?

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. When implementing a system to help protect sensitive PHI in compliance with HIPAA, 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 manner (within 30 days)?

Is your PHI protected with encryption?
- ☐ 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?

Do you create and monitor PHI access logs?
- ☐ Do you know when and how records were retrieved and accessed with 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 the following annual audits/assessments required by HIPAA compliance been completed?
- ☐ Security Risk Assessment
- ☐ Security Standards Audit
- ☐ Physical Site Audit
- ☐ Privacy Assessment
- ☐ Asset and Device Audit
- ☐ HITECH Subtitle D Audit

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 supposed to keep the specific medical documents according to regulations?

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 procedues 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?

Want to make HIPAA compliance a breeze? **Contact us today if you need help protecting your PHI.**
www.digitechsystems.com