HIPAA COMPLIANCE CHECKLIST

The HHS Office for Civil Rights has identified the following area to be essential elements of an effective HIPAA compliance program. How does your organization fare? Use this checklist to self-evaluate HIPAA compliance at your organization.

- ☐ Have you meet these six annual audits/assessments requirements for HIPAA compliance?
    a. Security Risk Assessment
    b. Privacy Assessment (only for covered entities)
    c. HITECH Subtitle D Audit
    d. Security Standards Audit
    e. Asset and Device Audit
    f. Physical Site Audit
- ☐ Do you have documentation showing that the above audits/assessments have been performed going back six years?
- ☐ Have you identified the gaps discovered in the audits above?
    - ○ Have you documented all deficiencies?
- ☐ Have you made remediation plans to address deficiencies found in all six audits?
    - ○ Are these remediation plans fully documented in writing?
    - ○ Do you update and review remediation plans annually?
    - ○ Are annually documented remediation plans retained in your records for six years?
- ☐ Have all staff members undergone annual HIPAA training?
    - ○ Is there documentation showing that each employee has completed annual training?
    - ○ Is there a designated HIPAA Compliance, Privacy, and/or Security Officer?
- ☐ Have all staff members completed Security Awareness training?
    - ○ Is there documentation showing that each staff member completed this training?
    - ○ Are there regular reminders supporting security awareness training?
- ☐ Is there a contingency plan in place?
    - ○ Are there written policies and procedures for emergency situations?
    - ○ Is all ePHI backed up to ensure an exact copy is available for disaster recovery?
    - ○ Are there written procedures to maintain critical business processes in case of an emergency?
    - ○ Are contingency plans regularly updated and tested?
- ☐ Has a risk analysis been performed to determine if ePHI encryption is appropriate?
    - ○ If it's not appropriate, are there alternative measures in place to secure the confidentiality, integrity, and availability of ePHI?
    - ○ Are there controls to guard against unauthorized access of ePHI that is transmitted electronically?
    - ○ Is there written documentation about the decision the use of encryption?

- [ ] Are identity management and access controls implemented?
    - Are unique usernames or numbers used for everyone needing access to ePHI?
    - Is access to ePHI restricted to users that need access in order to perform work duties?
    - Are there policies and procedures in place to check the appropriateness of employees' access to ePHI?
    - Are there policies and procedures in place for terminating access to ePHI when an employee leaves the organization or his/her role changes?
    - Are there policies for recovering all electronic devices containing ePHI when an employee leaves the organization?
    - Does your system automatically logout users after a period of inactivity?

- [ ] Are ePHI access logs regularly produced and reviewed?
    - Are there ePHI access logs tracking login attempts that can be audited?
    - Are ePHI access logs regularly reviewed to spot unauthorized access of ePHI?
    - Are controls in place to ensure that ePHI is not altered or destroyed in an unauthorized manner?

- [ ] Are there measures in place to limit the use of PHI to the minimum needed?

- [ ] Are there policies and procedures about how to securely dispose of PHI and ePHI?
    - Are there policies and procedures about how to make physical PHI unreadable and impossible to reconstruct?
    - Are there policies and procedures about erasing ePHI from electronic devices when no longer required or used?
    - Are electronic devices containing ePHI and physical PHI stored securely until they are disposed of properly?

- [ ] Have you developed policies and procedures for providing patients with access to their health information?
    - Does your organization give individuals access to their PHI or copies of it on request?
    - Does your organization give copies of PHI in the format requested by the individual?
    - Does your organization give copies of their PHI within 30 days?
    - If fees are charged, are they reasonable and cost-based?

- [ ] Does your organization obtain and store HIPAA authorizations and disclosures of PHI not otherwise permitted by the HIPAA Privacy Rule?
    - Do your authorizations clearly explain the specific uses and disclosures of PHI and are they written in plain language?
    - Do your authorizations state the classes of people to whom PHI will be disclosed?
    - Do the authorizations include an expiry date or event?
    - Do the authorizations contain the individual's signature and date of signature?

- [ ] Have you created a Notice of Privacy Practices (NPP)?
    - Do you provide periodic reminders to reinforce security awareness training?
    - Have you provided your notice of privacy practices to all patients?
    - Has every patient stated in writing that they have received the notice of privacy practices?
    - Has your notice of privacy practices been published in a prominent location and on your website?
    - Have you developed procedures for dealing with complaints about failures to comply with the NPP?

- ☐ Do you have policies and procedures relevant to the annual HIPAA Privacy, Security, and Breach Notification Rules?
  - ○ Have all staff members read and legally attested to the HIPAA policies and procedures?
  - ○ Do you have documentation of their legal attestation?
  - ○ Do you have documentation for annual reviews of your policies and procedures?

- ☐ Have you identified all of your vendors and business associates?
  - ○ Do you have Business Associate Agreements (BAAs) in place with all business associates?
  - ○ Have you performed due diligence on your business associates to assess their HIPAA compliance?
  - ○ Are you tracking and reviewing your Business Associate Agreements annually?
  - ○ Do you have Confidentiality Agreements with non-business associate vendors?

- ☐ Do you have a defined process for security incidents and data breaches?
  - ○ Do you have the ability to track and manage the investigations of all incidents?
  - ○ Are you able to provide the required reporting of minor or meaningful breaches or incidents?
  - ○ Do your staff members have the ability to anonymously report a privacy/security incident or potential HIPAA violation?

Disclaimer - Always consult an expert. Contact I.S. Partners for guidance on HIPAA/HITECH compliance.