HIPAA Privacy & Security Officer's Guide

HIPAA requires every Covered Entity and Business Associate to designate a Privacy Officer and a Security Officer. In private healthcare practices, it is most common to designate one person, a HIPAA Coordinator, to assume both roles. The HIPAA Coordinator oversees all ongoing activities related to the development, implementation, and maintenance of the organization's Privacy Policies and Procedures in accordance with the law.

HIPAA Privacy Rule

- **Written Programs** – Your practice must have up-to-date, written HIPAA policies and procedures to prevent unauthorized persons from accessing patients' Protected Health Information (PHI).
- **Statement of Privacy Practices** – You must develop a Statement of Privacy Practices that tells patients what PHI you will collect, how you will use their PHI, how you will protect their PHI, and what the patients' HIPAA rights are. Display your HIPAA Statement of Privacy Practices where it is visible to patients, publish it on your website and offer each patient a copy on their initial visit to the practice.
- **Acknowledgement of Receipt** of your Statement of Privacy Practices. You must make a good faith effort to get each patient's written acknowledgement that they have received your Statement of Privacy Practices. Patients are not required to sign. We recommend asking each patient, on their initial visit, for their authorization to speak with their family members or others.
- **Confidentiality Agreement** – All workforce members must sign a HIPAA Confidentiality Agreement prior to allowing them to access PHI. Workforce members include full and part-time employees, temporary employees, work-study students, interns, volunteers, etc.
- **Business Associates** – Prior to disclosing PHI to any business that is not a HIPAA Covered Entity, you must have in place a Business Associate Agreement. Business Associates include software companies, I.T. service providers, collection agencies, etc.
- **Training** - HIPAA requires you to provide training for all new workforce members, and training as often as needed to perform their duties. Annual training is considered to be a best practice.

HIPAA Security Rule

- **Access Level Determination** – Prior to allowing a workforce member to access electronic Protected Health Information (ePHI), you must determine the minimum information necessary to perform their duties.
- **Passwords** – Each workforce member must have a unique password. When logging into your system, the password authenticates the identity of the workforce member and limits access to only authorized ePHI.
- **Encryption** – All ePHI must be encrypted. This includes data at rest, such as your network server, and data in motion such as your system backup and emails that contain ePHI.
- **Firewall** – Your network must be protected by an effective firewall to protect from unauthorized access and unwanted content.
- **Malware Detection Software** – You must have up-to-date malware detection software to identify malicious software and prevent it from infecting your network.
- **Information System Activity Review** – Most healthcare software has audit reports that confirm activity within the system. You are required to "regularly" review such activity.
- **Annual Risk Assessment** – You are required to perform a risk assessment annually to reveal any weaknesses in your systems that could potentially place ePHI at risk.