

## Tip #1: Maintaining Patient Confidentiality

**The Risk:** Patient confidentiality breaches pose a significant risk in the healthcare setting. HIPAA and New York State laws govern your obligation to maintain the confidentiality of protected health information (PHI). Staff and providers must be aware that routine office practices, including telephone contact, verbal discussions, and computer use, inherently carry the risk of patient confidentiality breaches.

### Recommendations:

1. Staff should be educated, at a minimum annually, regarding HIPAA and patient confidentiality. This should be documented and maintained in their personnel files.
2. Confidentiality agreements should be signed by all staff members.
3. Staff conversations regarding patient care should not be audible to patients and visitors in the waiting area.
4. The staff should be advised to never discuss patients outside the office, including the use of social media.
5. Assess the flow of patients through the office to determine how best to maintain the privacy of PHI.
6. Computer screens should not be visible to patients or visitors.
7. Computers in exam rooms should not be left on or active when staff or providers are not present.
8. Any electronic device that is used for the transmission of PHI must be encrypted and have regular software updates installed.
9. The practice can leave messages on patient answering machines (e.g., regarding appointments) only if contained in your Notice of Privacy Practices. Patients must be offered the option of opting out.
10. Business Associate Agreements must be obtained and maintained for all vendors who have access to PHI.