HIPAA Required Officers

The two **"gotta have's"** for getting HIPAA compliant: your office's HIPAA Privacy Officer and Security Officer. They're a key component for compliance and one of HIPAA's major **"must-do's."** I want to review the unique role each officer plays in the compliance process. But first let's take a look at what these two positions have in common

According to HIPAA, the responsibilities of each officer revolve around keeping Protected Health Information (PHI) safe. The Privacy Officer and the Security Officer both have a role in developing the practice's policies and procedures, training the staff in HIPAA's requirements, and working to establish and maintain a culture of compliance within the practice.

And because the Privacy Officer and Security Officer share these responsibilities, in smaller practices it's not uncommon for one person — say, the office manager or the doctor — to wear both hats.

But in organizations where two people take on these different roles, who does what, exactly?

The Privacy Officer and Confidentiality of PHI

A Privacy Officer deals mainly with issues surrounding this question: Who has the right to see a patient's records or be included in conversations about a patient's health or care? "Who" is the operative word here. Think of this role as the one that's more people-focused — with the Privacy Officer fielding calls and assessing requests for patient information, as well as making sure that the staff respects every patient's right to privacy and has received training in what that means within the office and outside of it.

The Security Officer and the Integrity of PHI

The responsibilities of a practice's Security Officer, on the other hand, center on the PHI itself — the data and the physical records. A Security Officer's duties include:

- Understanding the HIPAA Security Rule and keeping up-to-date with any and all changes to the law.
- Developing and implementing policies and procedures to safeguard PHI
- Identifying and evaluating threats to the integrity of PHI
- Developing and implementing action plans for addressing risks to PHI

In other words, it's up to the Security Officer to make sure no one messes with the practice's PHI; that the information can't be tampered with, viewed illegally, or stolen.

To that end, it's the Security Officer's job to put in place appropriate administrative, physical and technical safeguards — everything from privacy screens for computer monitors to data encryption, firewalls, and virus protection.

It's a huge plus for a practice, then, if the Security Officer is a whiz with computers. But let's be real — not every office has someone on staff with that kind of expertise. In those cases, the Security Officer may choose to seek outside help from trusted technicians or specialists in information technology. In fact, in such instances, that's a very good idea. (And when that course of action is taken, it's also the Security Officer's responsibility to get signed Business Associate Agreements from those contractors.)

The dynamic duo of HIPAA compliance

A practice's Privacy Officer and Security Officer are a team, working together to safeguard patient info. For instance, while it falls to the Privacy Officer to authenticate requests for PHI, it's the Security Officer's job to ensure that those patient records won't get compromised, whether they're zipping through Internet or sitting in a file on a shelf, in the cloud, or on a front-desk computer.

It's in everyone's the best interest — a practice's and its patients' — for the Privacy and Security Officers to see themselves as Co-Protectors of PHI, kind of like the Batman and Robin of HIPAA compliance. Super heroes in a world of medical records. And a practice's best defense against breaches, fines, and ending up on the Wall of Shame on the Health & Human Services website.

If at all possible we would recommend having two different people in the roles.