Insights

HIPAA Assessments... Here's Looking at You!

August 22, 2018

By: Susan E. Ziel and Stacy Walton Long

Whether you are the Privacy Officer, the Security Officer, or both, the question remains the same. When was the last time you scheduled a "walk through" of your work space for the sole purpose of looking into the "eyeballs" of your personnel and finding out what they are really doing (or not doing) to protect the privacy and security of your customers' health information?

No, this is not the annual HIPAA security risk assessment. No, this is not a surprise, mock survey in preparation for some third party visit. Instead, you are simply showing up and letting your personnel know, first hand, that you really are interested in what they are actually doing to safeguard your customers' protected health information or "PHI." Nothing more.

In working with our HIPAA clients, we always recommend an annual HIPAA assessment calendar that sets out a series of compliance "questions" that will be reviewed -- one for each of the 12 months -- as part of an ongoing assessment process. The calendar can always be updated (or supplemented) as new questions or issues arise through the year.

For example, if this is January, then you may be in the HR department with the education coordinator reviewing a sample of personnel files to confirm that documentation exists to confirm completion of all new hire and annual HIPAA training. In March, you may join a supervisor and walk through their department work space at the end of the business day to look for any printed copies of PHI that may have been left on a counter or on a fax machine or in a "shred" bucket under their desk, all for easy "view" by the after-hours cleaning staff, or otherwise.

In April, you may make rounds with the medical records staff to query them about how they work through their checklist for subpoenas and other third party requests for records. In August, you may meet with the CFO's contract manager to review a sample of vendor agreements that should include a fully executed Business Associate Agreement. In June, you may seat yourself in a public waiting area with one of the admissions staff and listen for any "incidental" disclosures that could be overheard by other customers and their family members who are seated nearby.

During September, you may request a current copy of your organization's "workstation" inventory and confirm whether its up-to-date by conducting an assessment of all computing devices - whether owned by the organization or workforce, including desktops, laptops, tablets, smartphones and "any other devices that perform similar functions" and which are used on (or off) premises. According to a May 2018 OCR Cyber Security Newsletter, the physical security of all such "workstations" requires a complete inventory, rigorous policies and ongoing training programs that communicate the reasonable safeguards necessary to protect these "workstations" - encryption, strong passwords, secure use in public areas and secure storage when not

in use. These safeguards are especially important for those "workstations" that are mobile and used off-premises.

Of course, HIPAA assessment worksheets can be used to score and report your observations to create a paper trail and to keep your leadership apprised, but it is the "eyeball" connection with your workforce that is truly the bottom line here.

Raise the bar, raise the awareness and show up. It only takes an hour once a month to get this done. Here's looking at you -- in your hallways and offices -- very soon!

Please contact Susan E. Ziel at sziel@ihsconsultinggroup.com, Stacy Walton Long at slong@kdlegal.com or your regular Krieg DeVault attorney regarding HIPAA assessments or compliance issues.