People. Trust. Results.
Since 1960

Put Your Lab's HIPAA Compliance Policies Under the Microscope

By now we all know the importance of safeguarding personal health information (PHI) data in keeping with current HIPAA requirements, but did you know that employees themselves are frequently the cause of PHI breaches?

While there are significant technological resources available today that work to secure systems and data, they must be successfully combined with the actions of staff and employees to work as intended. With human error accounting for a good chunk of PHI breaches, it's important to maintain policies and strategies to reduce the risk of breaches stemming from basic employee mistakes and omissions. For example, consider these basics:

Policies related to employee computer use should define:

- Appropriate and inappropriate use of computers, laptops and other digital equipment in the lab
- Strong password creation and the schedule of required password updates
- Proper use of email including rules for forwarding, and replying to, emails containing PHI as well as encryption requirements
- Expectation to lock the system/screen when the desk is unattended
- Zero tolerance policy for installation of unauthorized software

Desks and office areas can house a treasure trove of PHI that can build up if clear policies don't exist, to require:

- Limiting access to authorized personnel
- Erasing white boards after use
- Locking file drawers
- Storing hard copy documents out of sight
- Removing documents from copy and fax machines immediately after use
- Shredding documents rather than disposing of them in trash cans

And not to be overlooked when developing your policies, the use of mobile devices containing PHI presents obvious risk that definitive actions, such as encryption, effectively work to mitigate.

Educating employees on security awareness is a must if you want to keep the risk of PHI breaches to a minimum. One needs only to view the Office for Civil Rights' (OCR) "Wall of Shame" to see that the root cause of many large-scale (affecting 500 or more individuals) breaches begins with the employees, themselves.

Effective policies & procedures and ongoing employee education, combined with consistent monitoring, will provide a sound framework for guarding the privacy of your patients' personal health information. Visit HHS.gov for additional guidance, facts and FAQs for Covered Entities.

Information provided by APS Medical Billing, August 2018