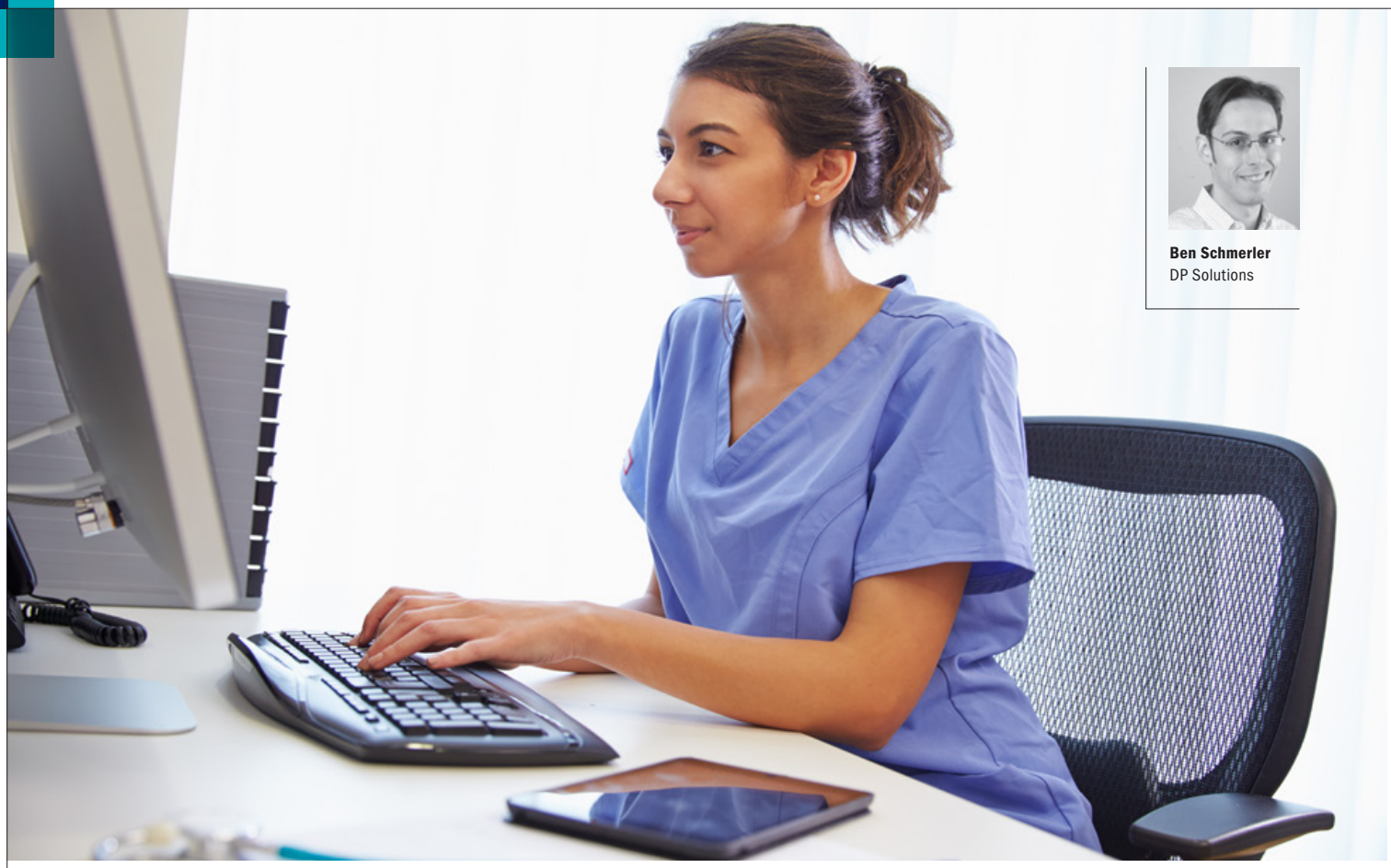

Ben Schmerler
DP Solutions

How to Maintain IT Security & Compliance During the On-boarding and Off-boarding Process

JUST LIKE EVERY other business on the planet, Medical Practices and other organizations controlling personal health records (PHI) have to deal with personnel changes on a regular basis. New people come in and, for whatever reason, others move on. Many organizations undergo significant shifts. Perhaps the practice expands or contracts. These are all normal things that any manager would anticipate.

However, in the case of medical practices, these events can either strengthen data security, or make the investment you made in security technology and risk management worthless.

Technology can only do so much. An authorized user going into an EMR and accessing data is going to be seen by any monitoring tool as business as usual. However, if that "authorized user" is someone who was terminated, and their account still has significant access rights, then everything they do within your system is a HIPAA violation and data breach.

This is why it is important to recognize that there must be strong management and control of onboarding and off-boarding of staff. In this article, I will touch on a few important points on both ends.

ONBOARDING

So you've found the perfect fit for your practice. Your new billing person is extremely qualified, has a robust background and experience, they answered all of the questions perfectly during the interview and hiring process, and passed appropriate background checks. That's great. However, once they come on board, you can't just give them the keys to the car and let them drive off with your patient information.

First, it is important to establish what level of familiarity they have with things like HIPAA/HITECH. Just because they came from an environment that supposedly had compliance management and regulated patient data, does not mean they have been given a proper education. Many health care workers I have met lack the basic grasp that really should be the standard. While you don't need to create a staff of HIPAA auditors, it is important that your staff understand the basic ideas of what HIPAA looks to accomplish when it comes to protecting the privacy, integrity, and availability of PHI. The good thing about having a grasp of that basic understanding is that these principles can be applied logically to the tasks that staff members perform every day. It also empowers them to approach new challenges to compliance in a logical way.

Beyond a simple understanding of compliance, this kind of training or teaching should apply to HOW they do their jobs. Is the staff member in any way, shape or form responsible for the transmission of sensitive data to a third party? Their training should keep that in mind. Is the staff member located near an area where PHI could be accessed, and potentially seen by visitors to the office? If so, that staff member should understand how they

should work to block that kind of unwanted, incidental contact with sensitive information. This is why basic principles of HIPAA are important. Once that baseline is established, staff can apply these ideas to practical scenarios, or at least be aware that they should work with management if something seems relevant to meeting HIPAA compliance and they aren't sure how to handle it.

Additionally, practices have to establish the proper level of access to data across the board, not just ePHI. Your practice has plenty of information that you want to protect. Using the "minimum necessary" standard is a good way to think of access rights, regardless of the data you are looking to protect. What is this employee's role? How much PHI should they have access to? Do they even need access to it? What kind of equipment and security tools should be in place based on the level of touch with sensitive data? While I can appreciate the idea of giving staff the freedom to have flexibility to do their jobs, it does not mean that you need to give unfettered access to everything in the system. Furthermore, some staff may need elevated system rights for things like software installations, updates, etc., that other staff members simply don't need. Don't forget that the more elevated access accounts that exist on your system, the greater your risk of exploitation.

Finally, you need to consider the general idea of Acceptable Use. Regardless of roles and responsibilities, there should be some basic rules of engagement with technology. What websites are staff allowed to visit, and under what conditions? What kind of data is allowed to be transmitted, and what is not (or stored on portable media)? What is the relationship between personal devices (BYOD) and organizational data? When is remote work allowed and under what circumstances? Generally, you don't want to be too restrictive as to limit productivity, but at the same time a line has to be drawn so that you can limit risk exposure of a data breach.

While this is not entirely extensive, when looking at the big picture of staff onboarding, your focus should be on a) compliance and security awareness training b) determining access rights and c) defining the terms of use for system utilization and organizational data. Once these items are addressed to the satisfaction of management (and documented for records), then you should be much more comfortable allowing a new staff member access into the system and allow them to do their work.

OFFBOARDING

Every organization is going to have staff turnover. In my experience, many organizations have loose governance over access and management for terminated staff. I have seen dozens of accounts for former staff that are still active, and sometimes those accounts don't even have things like forced password resets which could at least restrict access to these lapsed accounts. I can't stress enough how important it is to have an off-boarding procedure, especially when IT and data access is concerned. Not only is off-boarding important for restricting former employees, but those lapsed accounts could also be potential points of entry for outsiders.

Fortunately, off-boarding should be a much more streamlined and simplified process, and the most important. Unlike onboarding, where you have to perform several exercises before allowing someone access into sensitive assets, off-boarding is about lock down. The same documentation used to outline what was done to determine user rights, training, etc., should be referred back to so tech support can reverse the process. Passwords should be immediately changed, EMR access should be locked out, and so on.

However, there are a few additional things to consider. Was this a privileged account, and as such do you need to simply transfer rights to someone else as opposed to completely disabling or removing the account? What kind of termination was it? If it was due to violations and perhaps not the most pleasant termination, then there should be much more focus and urgency on a quick off-boarding. If these changes are part of broader changes across the board (perhaps the result of something like major layoffs) then these sort of off-boarding considerations should be brought up much earlier than they might be in the case of a more casual end–of-employment scenario.

If I were to leave the reader with any particular message about off-boarding, it would be: diligence and discipline. Tech support can only respond to the requests of management, and it cannot be solely the IT Department's responsibility to manage this process. Proper cohesion between HR departments, tech support, and other management is critical during off-boarding.

CONCLUSION

It is difficult to write a one-size-fits-all approach to managing the onboarding and off-boarding process as it pertains to IT. This article cannot possibly address all considerations and the unique nature of each organization that has ePHI. However, if you can focus on building an environment where you only provide access to system assets after careful vetting and consideration, and conversely, use discipline when off-boarding employees, then you can create an environment where risks from orphaned and mismanaged users are dramatically minimized. Like other security concerns, this kind of risk isn't something you can just buy and fix. It requires consistent management and focus from your team. ■

Ben Schmerler is a Senior IT Risk Advisor at DP Solutions, an award-winning managed service providers (MSP) servicing medical practices throughout the Mid-Atlantic region. Ben works with clients to develop a consistent strategy not only for technical security, but also policy/compliance management, system design, integration planning, and for other business-level technology concerns. You can follow DP Solutions updates on LinkedIn or their website: www.dpsolutions.com.