Ben Schmerler
Virtual CIO Consultant,
DP Solutions

Organizing Your Team to Make IT Risk Management a Priority

EVERY PRACTICE, REGARDLESS of size and complexity, is responsible for protecting patient data. While it is important to deploy security solutions to avoid the breach or loss of data, technical controls are only half of the overall risk management solution. This article will highlight several themes you will want to consider when designing your organizational roles and responsibilities for protecting patient information.

THE ROLE OF A HIPAA PRIVACY CONTACT

When it comes to managing data, it is inevitable that incidents will arise that require staff communication and ownership in order to avoid data breaches and loss. These occurrences can be extremely stressful, as the people responsible for incident management are often not very technical. HIPAA Privacy Contacts usually understand the incident from an outcome perspective, rather than understanding why and how an incident occurred in the first place.

In light of this, it is important to structure organizational roles based on staff competencies. It is not a problem if the HIPAA Privacy Contact is not the most technical individual, but if they decide to take technical actions to remediate a security incident themselves, they will most likely only make matters worse.

Rather than being a technical expert, the HIPAA Privacy Contact should be the "champion" for compliance and incident management. This person should understand the serious nature of their role, as well as make it clear to staff that they are responsible for reporting incidents directly to the Privacy Contact. From there, the Privacy Contact needs to manage the communication to staff and any third parties responsible for technical incident response, documentation of all details related to the incident, and ultimately longer term follow up to determine if the incident could occur again, and what can be done to limit risks in the future.

EDUCATING YOUR STAFF

Risk management is not only a reactive exercise, but also an exercise in putting staff in a position to avoid dangerous behaviors that could lead to significant incidents. Starting from the top of the organization going down to individual staff members, it is important that a risk management plan includes regular education for security awareness. Often times, we find that staff does not totally grasp the risks that are out there, leading to honest mistakes that cause problems. Ensuring that your staff is consistently educated on IT security best practices is key to a successful risk management strategy.

ORGANIZING YOUR RISK MANAGEMENT TEAM

When organizing your risk management team, you should start with identifying (at each office location) who you trust to manage the process as a HIPAA Privacy Contact. This individual will be responsible for establishing education plans, reporting security incidents to IT support (internally or externally), and holding staff accountable for their adherence to security policies. Additionally, these contacts should have a broad responsibility for communicating with upper level management as risks evolve and change, as well as be comfortable dealing with subject matter experts when a risk is identified for additional management. Remember, it's not about having all of the knowledge to mitigate risks, but having personal awareness and responsibility for those risks so that the subject matter experts can deal with the actual issue.

The risk management team at any particular office should include both a managerial type as well as users who may not be high-level managers. That way, risk management strategies will represent both the goals of management as well as the daily challenges of end users who are often the first to be aware of peculiar incidents or other risks such as connectivity and accessibility challenges or patient feedback. These users can also provide input for effective communication strategies and policies. In general, end users should be encouraged to communicate risk management challenges to the leader of the risk management team, and from there the concern can be resolved with management or subject matter experts.

MAINTAINING YOUR RISK MANAGEMENT STRATEGY

As you may be able to tell by now, documentation and communication are essential for proper risk management. A good risk management strategy will unify communications. Every staff member will know who to report to when dealing with issues. Incidents will be centrally managed, with single points of contact for remediation so efforts are not duplicated or conflicting. And of course, all policies regarding communication of risk related issues should be reviewed on a regular basis. Part of the risk management process is revisiting policies regularly, especially as organizational changes may make existing policies moot or ineffective.

Another responsibility of the risk management team, in particular the HIPAA Privacy Contact, is making sure that technical controls are evaluated, including vulnerability testing and risk assessments by third parties. While most of the team likely lacks the expertise to evaluate technical risks, they can be responsible for ensuring that a regular risk assessment takes place to make sure the practice's data is properly protected. It should also be up to the Privacy Contact to make sure that remediation efforts to fix technical shortcomings are completed and documented. While your technical support may or may not be internal, they are essentially part of your risk management team. It's important that you document their role in this process and make sure your support team has bought into your risk management strategy.

GETTING STARTED

So how do you build this team? How many people belong on the team? This can be tricky, since there is no one-size-fits-all risk management solution. Smaller practices may get by simply with a single Privacy Contact responsible for all risk management. However, larger practices should have risk management teams for each office location with their own documented policies and education sessions. In general, the size of the team is going to be representative of the number of staff at the location as well as the actual assets that staff can touch. For example, an environment where several servers are in place locally requires an entirely different risk management team and plan than one where data processing and storage is hosted elsewhere.

Remember, none of this is a one-size-fits-all solution; it's up to you and your staff to take the time to consider the various risk factors to which your practice is exposed. Upper level management (along with third parties) is responsible for identifying risk factors to the practice. The organization of your risk management and ultimately your incident response team will depend on what those risk factors are. ■

Ben Schmerler is a Virtual CIO Consultant at DP Solutions, a leading IT managed service providers (MSP) in the Mid-Atlantic region specializing in Security & Compliance, Managed Services, Cloud Technology and Virtual CIO Consulting. Ben works with his 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. For assistance with any of your compliance needs, contact Ben at bschmerler@dpsolutions.com *or follow DP Solutions updates on LinkedIn at* www.dpsolutions.com.

New Member Corner

Please join us in welcoming the following new Maryland MGMA member who joined between December 9, 2016 and January 15, 2017.

Lisa Lockhart
Metropolitan Medical
Specialists, LLC

CALLING ALL MEMBERS

Refer a New Member for Your Chance to Win a $100 Gift Card

Do you have colleagues who would benefit from Maryland MGMA's educational programs and benefits? Please encourage them to join as a member. During each quarter of 2017, we will hold a drawing for a $100 gift card from those who referred at least one member during that quarter. Simply instruct the person to enter your name on the application as the person who made the referral.

Direct your referrals to the Membership tab at *www.marylandmgma.com*. Membership questions may be directed to Jennifer Thornton at the Maryland MGMA office – 443.966.3875.