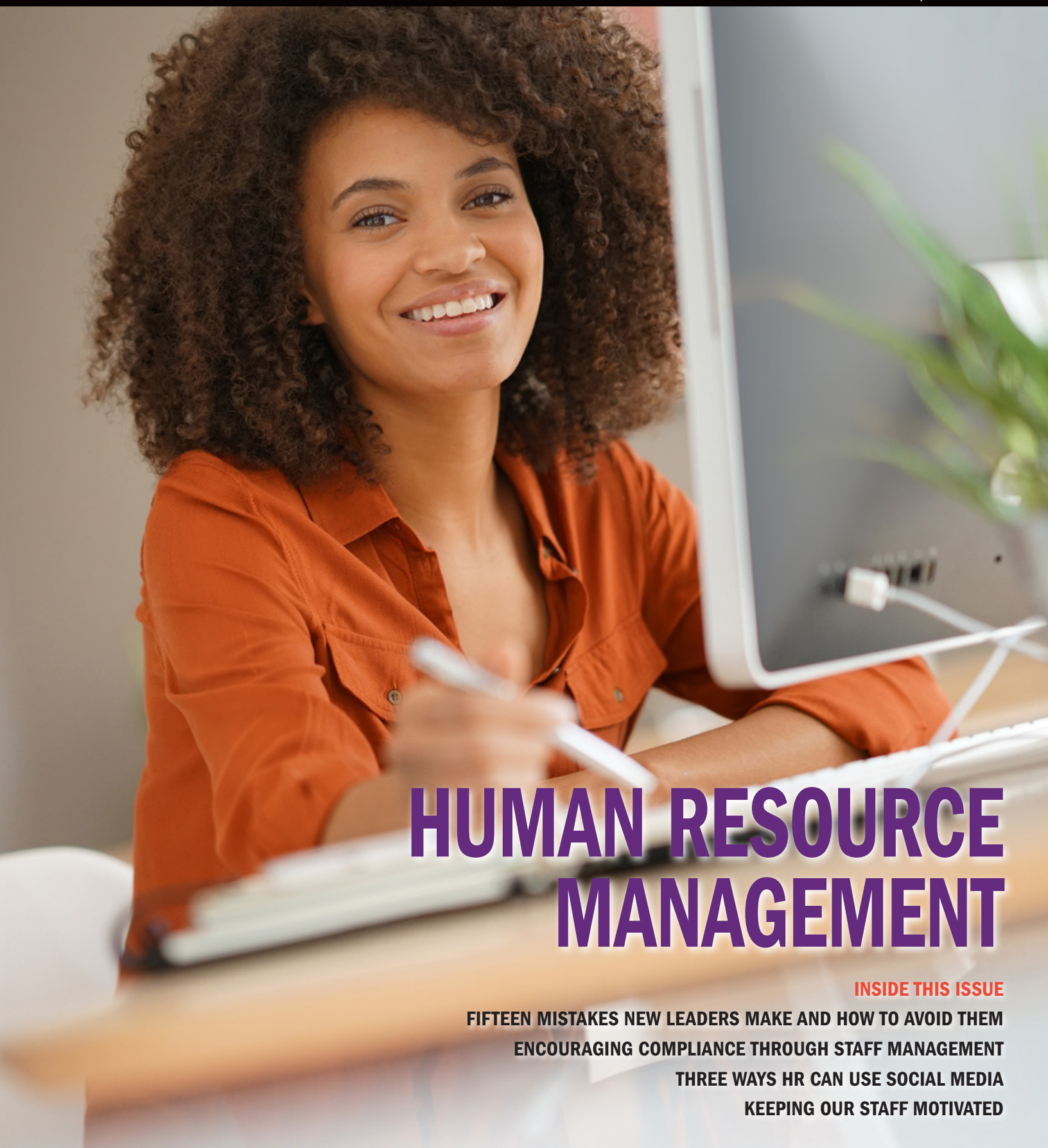
A PUBLICATION PROVIDED BY
MGMA
Medical Group Management Association
Maryland

MediNews

MARCH/APRIL 2017



HUMAN RESOURCE MANAGEMENT

INSIDE THIS ISSUE

Ben Schmerler,
DP Solutions

Encouraging Compliance through Staff Management

EVERYONE WHO MANAGES staff in a medical environment immediately becomes a key decision maker when it comes to HIPAA compliance, whether they realize it or not. Many data breaches do not occur because of technical failures that come from a conscious attack on security systems, but by the failures of personnel to properly control the access to patient health information. Practice managers hand the keys to the vault of patient data to staff members every day. Just like money in your bank account, sensitive data has a real value, and anyone with access to it holds a serious responsibility.

As such, establishing proper rules and expectations to staff and management is paramount to a proper risk management strategy for HIPAA IT Compliance.

Here are some concepts and key points that anyone who manages staff in a medical practice should keep in mind to foster HIPAA IT compliance.

KNOW WHO ACTUALLY HAS ACCESS TO THE SYSTEM

Just the other day I read a post on a popular IT security blog about a former IT administrator who was a 14-year employee of a company in Oregon, and upon leaving left backdoor access into his former employer's systems. This went on for a few years, and he exploited information that he was not entitled to in order to give competitive information to his new employer. Eventually, this was discovered, but not until multiple parties were involved, including the FBI. While this story is troubling, this sort of thing is very common.

Without getting into too many details, there are a few obvious lessons to be learned from this kind of security incident. First of all, in this situation there was clearly no oversight regarding this rogue former employee's rights at the time he left the original company. He was able to create an account with suitable rights to give himself access whenever he wanted. There should have been some kind of sign off upon his termination that another IT administrator had reviewed the entire access situation to make sure no unauthorized accounts were enabled, and this should have been directed by Human Resources.

There is also the broader question of oversight and system review. Simply put, there was no policy instituted by management requiring review of rights on a regular basis, regardless of new or terminated employees. While this example is about a former employee, there could be third party vendors or hackers who have accounts that are enabled. Oftentimes during system audits, I find accounts that have been enabled for years that nobody knows about, and even more troubling, these accounts are often ones with significant system privileges. Anyone with ample knowledge and bad intentions could easily take advantage of these oversights to cause major losses to organizations with sloppy access rights such as these.

ESTABLISH DEFINED PROCEDURES FOR NEW AND TERMINATED STAFF ACCESS INTO THE SYSTEM

This may sound simple, but I often find that in reality these rules are not universally followed. When a new staff member is brought on, the first step should be for management to ask a series of questions, such as:

- What is this person's role within the organization?
- Based on that role, what information are they required access to?

(Remember the "minimum necessary" standard, which states that users should access only the PHI that they need, and nothing else whenever possible.)

- Where do they need to access this data? Is it just in the main office or remotely as well?
- Who do they need to share sensitive data with?
- What familiarity do they have with HIPAA, and what additional training do they need before gaining access to ePHI?

While this list is not exclusive, it gives you an idea of what to think about prior to adding a new user. Once you answer these kinds of questions, someone in management will need to work with an IT support representative to get that user added based on their role. This process should be documented from the beginning all the way until that user is completely added. HR should be aware of who determined the user rights and when the decisions were made. There also should be specific documentation outlining who from IT implemented the user creation in the system.

Of course, it is inevitable that people will leave the organization, and you are going to have to take similar steps to remove them. Consider the following:

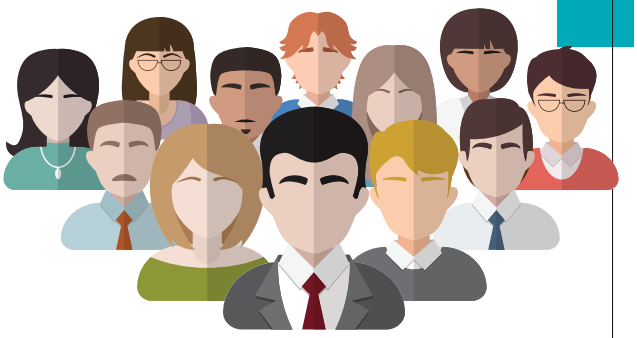
- When is the person actually leaving (or have they already been terminated)? As soon as their rights are no longer needed, that person should be removed.
- What information do you need to get from that user before they leave? Did they control some kind of information or access that a current staff member will need (and perhaps have their rights adjusted accordingly)?
- What personal devices did they use to access organizational data? Are you certain that your procedures for removing the user considers this?
- Would this user have any way of taking data with them prior to losing access (such as copying files to a flash drive)?

The truth is that most of the time terminations are quite amicable and most former employees just move on, but that doesn't mean we can forget about proper procedures before contacting IT support to have their rights revoked. Needless to say, once that user is ready to be removed, the entire process of removal should be documented for future reference if needed.

ACCEPTABLE USE AND SECURITY INCIDENT EDUCATION AND POLICIES

Even after we have come up with processes to add and remove users, as well as consider what rights and responsibilities they have within the system, it is important that staff understand the sensitive nature of the information they will have access to. They should know what it means once you give them credentials and let them do work for which the organization will ultimately be responsible. Both an Acceptable Use and a Security Incident policy should be created, communicated, and agreed to by any user before they begin working in the system.

An Acceptable Use policy is a set of rules that a user must follow when using company technology. A good Acceptable Use policy should include rules regarding what web sites users are allowed to visit (if any), proper use of company email, mobile device usage (both personal and company owned), any system configuration or changes that the user is or is not allowed to make on their own, and so on. Consider how much self-regulating you want your staff to have over their behavior as well. If you aren't using sophisticated tools that forcibly limit their access, then your Acceptable



New Member Corner

Please join us in welcoming the following new Maryland MGMA member who joined between January 15, 2017 and March 31, 2017.

Durbin Vido
SunTrust

Michael Thibault
Potomac Physicians Associates

Tasia Powers
Medstar Medical Group

Shawntel Gray
Aruna Nathan, MD PA

Korey Cobb
Mid-Maryland Muskuloskeletal Institute

Julia Konovalov
Medical Business Partners

Hemik Patel
RS&F Healthcare Advisors

Lauren Gross
Anne Arundel Healthcare Enterprises, LLC

Drenary Gwynn
Anne Arundel Healthcare Enterprises, LLC

Anna Fink, CPA
Ellis & Associates, CPA's, P.A.

Brillia Perez
MedStar Health- MedStar Medical Group

Jenna Tucker
Curtis Bay Medical Waste Services

Peggy Candore
Anne Arundel Rheumatology

Kevin Friedel
UM Community Medical Group - Pediatrics Easton

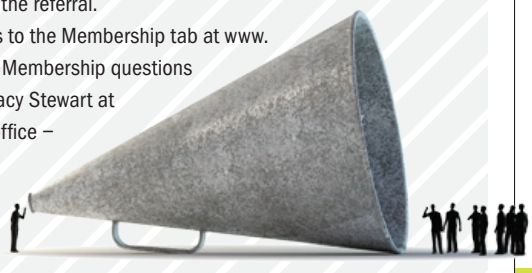
Amy Smiley
Diamond Healthcare Corporation

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 Stacy Stewart at the Maryland MGMA office – 443.966.3875 x131.



Use policy will need to put more responsibility back on the end user. Remember, this isn't just about protecting your data assets, but also limiting liability if possible by forcing staff to agree to rules, and holding them accountable with real consequences should they violate the policy.

A Security Incident policy focuses more on the actions of users if and when an actual security challenge occurs. These kinds of incidents could be as simple as a basic virus preventing a computer from proper operation, to a significant data breach. While a robust Security Incident policy will speak to what IT support may do, reporting to various entities regarding the nature of a breach, or other technical details, I'd like to just focus on the internal behavioral rules as a part of this policy. Most medical practices will be utilizing an IT department for the actual resolution of a security incident.

From the end user's perspective, a good Security Incident policy will inform the end user:

- What is defined as a significant incident
- Who is covered by the policy
- Roles and responsibilities of staff for response
- Who an end user will need to report to in management
- Who an end user needs to report to from IT support (if in fact the issue is reported to IT support by the user, which is not always the case)
- Post-remediation efforts to determine ways to avoid these kinds of incidents in the future, among other things.

For both of these policies, there are ample resources online to learn more, as well as consultants like myself who can help advise as to what a specific policy should look like based on your organizational needs.

COMMON MISTAKES OR MISCONCEPTIONS

A few common scenarios amongst practice administrators or HR direct seem to emerge that, while done with good intentions, do not always contribute to HIPAA compliance:

- Storing passwords for end users. There is simply no reason to keep these passwords. This normally occurs because of a lack of trust in staff, and a manager wishes to have access into their account, or because there is a fear that a password is lost and someone will be locked out. The truth is that there are alternative solutions for either of these that don't create uncertainty as to who is logging into an account, or open a treasure trove of passwords that someone could exploit.
- Lack of accountability for personal devices accessing company data. Most organizations allow people to connect and touch sensitive data on home PCs or personally owned mobile devices with little oversight or care. They look at this as a productivity boost, which of course it is. But managers need to make sure that they know what devices are touching sensitive data, and ensure that these devices are taking proper measures to ensure HIPAA compliance.
- Too many network administrators. In an effort to try and prevent lock outs, or because of distrust of IT, managers set up too many people with high level system rights. This moves against the minimum necessary standard, and also creates highly valuable accounts that are the most exploitable.
- Overly restrictive rules. Creating a reasonably secure environment, strong user policies, and being productive are not mutually exclusive. Particularly in small organizations, users need to feel empowered to solve problems. While of course staff shouldn't be allowed to visit adult web sites, or download any application they want to their PC, completely locking down web traffic for example stifles creativity and productivity. You want to create an environment where security compliments your workflow, and doesn't hinder it. There is a middle ground.

These are only some of the things management should consider when creating a culture of HIPAA compliance. Whenever focusing on HIPAA compliance, or any other standard, always remember what you are trying to protect, and who has access to it. By starting at this point, many of the answers for risk management become much more obvious. ■

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.