MAY 2020

Magnolia minutes

A PUBLICATION OF MGMA OF MISSISSIPPI

MGMA MISSISSIPPI

A Word From Our President

President

Pam Franck

Regional Director,
North Mississippi
Medical Clinics, Inc.

As you are reading this message, I hope we have "flattened the curve" and are on the other side of COVID-19. What a time to be a leader in Healthcare! At no other time in my medical management profession have I felt so supported. MGMA and MGMA MS have served as valuable resources to me as I have worked with my team to navigate these uncharted waters. I hope you, too, have taken advantage of MGMA's COVID-19 Action Center and COVID-19 Community, multiple web-ex opportunities, and have talked with your fellow MGMA MS members to see what is working in their clinics.

Thanks to all of you who were able to attend our Insurance Forum on February 13, 2020. We had 58 attendees with 4 payers (Molina, UHC, Aetna, Magnolia) presenting and answering your questions. I would like to say a special thanks to Bob Williams, Director of Life and Health Actuarial with the Insurance Commissioner's office, for participating as well as Harold Ingram for serving as our Moderator during the meeting.

Due to our being compliant with social distancing, we are postponing our spring Outreach Meetings. We hope to reschedule those for June. We are still anticipating holding our Summer Conference in Biloxi on August 23-25, 2020 at the Beau Rivage. We are excited once again to share this conference with MGMA LA. This continues to be an amazing networking opportunity for our members. An educational and informative agenda is being confirmed and will be shared with you soon. Please "Save the Date".

I saw the following quote the other day on Instagram that I felt was appropriate for these days…

"Challenges are gifts that force us to search for a new center of gravity. Don't fight them. Just find a new way to stand." - Oprah

Let's keeping standing strong together MGMA MS!

SAVE THE DATE

Momentum 2020

The Beau Rivage
Biloxi
August 23-25, 2020

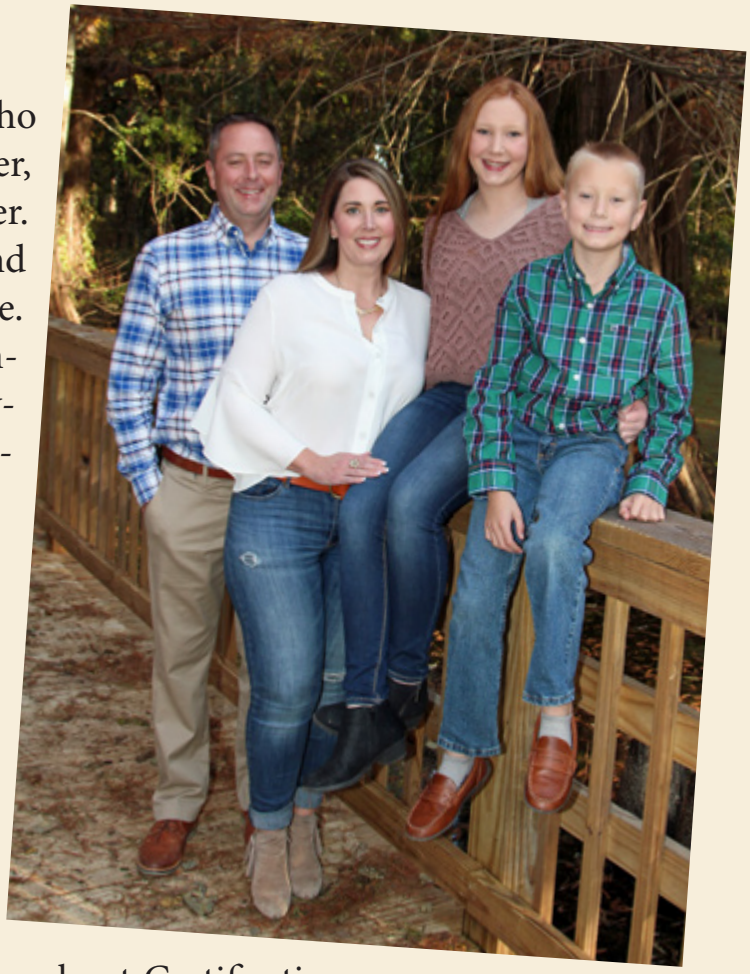
Board Member Spotlight

Janet Benzing

Executive Director of Ancillary Services, Delta Regional Medical Center

Job Responsibilities

Currently have oversight of 9 specialty clinics and 4 primary care clinics



Personal Info / Hobbies

My husband and I have two wonderful children who keep us moving! We love spending time together, especially during the recent "safe at home" order. We've completed more home projects, baked, and taken more walks and bike rides during this time. My other hobbies include traveling, reading, enjoying the outdoors, listening to music and playing the piano when no one's watching TV or playing Xbox.

Why MGMA MS?

I've been a member of National MGMA since 2007. I joined at the encouragement of a mentor and it's been one of the best investments in my professional growth. In 2013, my family and I moved to Mississippi and I quickly got involved with the Mississippi Chapter of MGMA. The first person I remember meeting was Joy Yates. She had led a session at one of our state meetings about Certification through the American College of Medical Practice Executives (ACMPE). Certification had been a goal of mine for several years but I had this fear of not passing the exam. Joy led me to resources available through MGMA to help me prepare as well as hosted a practice session. All of that really gave me the push I needed and in 2015 I passed the CMPE exams. Following in 2019, I achieved Fellow status with ACMPE. Long story short, I wouldn't be where I am today without MGMA MS. The networking, resources and education are unmatched in the world of practice management. We are fortunate to have such a strong State Chapter here in Mississippi and I'm proud to be a part.

Did you know that MGMA MS membership includes all of the following?

- Free monthly webinars for members
- Opportunity to upgrade skills, knowledge, connections
- Educational conferences, programs
- Resources on practice management issues
- Legislative advocacy
- Electronic News Digests and Alerts
- Research data
- Career enhancement
- Information exchange
- Problem-solving
- Networking
- Job Postings free of charge

Be sure to take full advantage of your membership today! Visit our website to check out our webinar library and career center. www.mgmams.com

Not a member of MGMA MS yet? Join us today!

Contact our office with any questions: info@mgmams.com

UPCOMING WEBINAR

Register today at www.mgmams.com

CARES Act Provider Relief Fund: Important Information on Payments, Reporting and More

Tuesday, June 9th from 12:00pm-1:00pm

ABOUT THE WEBINAR:

The CARES Act's $100 billion provider relief fund has certainly helped those on the front lines of COVID-19. Yet it also raises questions about how the money can be used, which expenses qualify, reporting requirements, and whether funds should be returned if they're not needed.

Jay Hutto, CPA and partner at James Moore & Company, will address these concerns and more in this presentation. He'll discuss the HHS restrictions, what we know and don't know regarding reporting requirements on provider relief, as well as the importance of having detailed supporting information available for a possible audit.

Areas to be covered include:

- How payment amounts are determined, approved or rejected
- The terms and conditions of the payment
- What we know and don't know regarding reporting requirements for payments, lost revenue and expenses
- Tax implications
- Revenue recognition for payments
- … and more!

ABOUT OUR SPEAKER:

Jay Hutto, CPA – Partner, James Moore & Co.

Jay has over 25 years of experience providing a wide range of accounting services. The leader of the firm's Healthcare Services Team, his work includes tax services, revenue cycle enhancement, business valuations, auditing and assurance, and more.

Webinars are FREE for MGMAMS members!

Click here to register today!

MOMENTUM 2020

Building Better. Together.

at The Beau Rivage, Biloxi from August 23-25, 2020

Interested in getting more involved with MGMA MS?

We are always looking for an extra hand to help make this association thrive.

Please contact Kristina at kristina@m3solutionsllc.com to see how you can help!

Intruder Alert! Protecting Against Insider Vulnerabilities in Healthcare Organizations

Healthcare industries have several threats to consider that are happening from both inside and outside of their organizations. We often hear from several organizations about concerns about how they can prevent an external attack against their organization from happening. External threats, such as cybersecurity attacks, are important for organizations to be concerned with, however, there seems to be less concern over internal threats. Perhaps, it is because the types of external threats to healthcare typically make the evening news with data breaches that are wide-ranging in whom they affect.

External threats, like cyberattacks against organizations, generally look for vulnerabilities to exploit or for other ways into the network of an organization. Insider threats can be more challenging to recognize than external ones. This is why last year the, Office of Civil Rights (OCR) *Summer 2019 OCR Cyber Security Newsletter: Managing Malicious Insider Threats*, OCR referenced the 2019 Verizon Data Breach Investigation Report. The report states that trusted insiders were responsible for 59% of all security incidents and breaches - both malicious and inadvertent. The report also indicated that the primary motivation for incidents and breaches perpetrated by insiders was financial gain.

Malicious Insider Threats

Malicious insiders are generally successful with their objectives, exposing their organization to a wide range of security threats simply because they are considered trustworthy or have access to sensitive data like health information. Common malicious insider threats could include the following:

- Accessing the medical records of celebrities for financial gain and using patient information to commit fraud and identify theft.
- The exfiltration of sensitive information stored within an organization's IT systems can be accomplished in several ways, such as transmitting information in encrypted messages, copying information to a mobile or storage device (e.g., cell phone, USB drive), or unauthorized physical removal or theft of equipment.
- Transmitted or copied data could be further hidden using subtle means such as by embedding data within other data to hide it.

Vulnerabilities Can Come in Many Forms

OCR reminds us that forms of harm, including loss of data, damage to the organization's reputation, civil liability exposure, and potential federal and state regulatory enforcement actions, are all possible due to malicious insider attacks. Individuals who are affected by a data breach could be at risk for identify theft, fraud, or blackmail. Keep an eye out for these types of

employees:

- **The desperate employee** – Employees that may be desperate to steal or sell information for financial gain. The employee could be desperate for the extra cash for numerous reasons or could just desire to increase their financial situation illegally.
- **The disgruntled employee** – Unhappy employees that have the motive to steal or leak information intentionally. The employee can use their knowledge of the organization to exploit vulnerabilities or access information.
- **The distracted employee** - These employees may be distracted by personal responsibilities or are simply overloaded in their job responsibilities. This situation is creating opportunities to make accidents, such as errors in sending emails, oversharing of patient information, misusing social media, or losing a USB drive.

Guidance and Recommendations

OCR knows that detecting and preventing data leaks by authorized insiders is a challenge for all organizations. Early detection of malicious activity – whether from an insider or outsider threat – helps to prevent or mitigate the impact. Below is a summary of the guidance OCR has provided along with recommendations for healthcare organizations to detect and prevent malicious insiders.

1. The where, what, and how of safeguarding critical data.

It's crucial to understand where data is located, the format used, and how the data flows throughout the organization. This is an essential part of performing an accurate and thorough assessment of the risks to the confidentiality, integrity, and availability of an organization's critical data. From there, once risks are understood, policies and procedures can be developed or updated, and security measures implemented

Continued on page 7

to reduce identified risks to a reasonable and appropriate level.

In other words, healthcare organizations must identify risks and threats to their sensitive data and electronic protected health information (ePHI). Performing assessments such as a HIPAA Threat Matrix, HIPAA Virtual Walkthrough, and most importantly – a Security Risk Analysis (SRA) are instrumental in understanding the where, who, what, and how your critical data is safeguarded.

Who is permitted to interact with ePHI and other sensitive data?

An organization should establish who is permitted to interact with its data and what data those users are permitted to access in determining appropriate access controls. Access controls can take many forms, for example, physical access controls, network access controls, and role-based access controls.

A good time is to consider what access controls are appropriate is while performing or reviewing your SRA. In doing so, it comes down to need to know or need to access: what areas in the facility does an employee really need access to? What network(s) should an employee access?

Is their role-based access appropriate for their job duties? These are all questions that should be considered. From there, policies and procedures should be implemented to ensure access controls are communicated to all employees and enforced.

3. For what purpose are users interacting with data?

Another important consideration is how an organization's users will interact with data. Do the duties of the user's job require the capability to write, download or modify data, or is read-only access sufficient? Do users need to access data from laptops, smartphones, or mobile storage devices (such as thumb drives)?

If you allow employees to use their personal devices, a Bring Your Own Device (BYOD) policy should be implemented. Due to how many individuals have personal devices in a healthcare organization, whether you allow personal devices to be used or not, a BYOD or similar policy should be in place that addressed mobile devices should be in place. Additionally, any devices that can access, create, store, or modify ePHI – such as a laptop or smartphone – should be encrypted and have access controls (e.g., unique user ID and strong password requirements, dual-factor authentication) in place. It is also recommended to maintain an up-to-date inventory of these devices.

4. Real-time visibility and situational awareness.

The migration to cloud computing, the increase use of mobile devices, and the adoption of Internet of Things (IoT) technology can greatly reduce an organization's ability to detect anomalous user behavior or indicators of misuse by either a trusted employee or third-party vendor who has access to critical systems and data.

Healthcare organizations must have safeguards in place that detect suspicious user activities such as traffic to an unauthorized website or downloading data to an external device (e.g., thumb drive). Audit controls such as system event logs, application audit logs, and user access and changelogs in the EMR, should be reviewed. These types of security measures are a HIPAA Security Rule requirement that can assist in detecting and identifying suspicious activity or unusual patterns of data access.

5. Security is a Dynamic Process.

Good security practices entail continuous awareness, assessment, and action in the face of changing circumstances. The information users can and should be allowed to access may change over time; organizations should recognize this in their policies and procedures and in their implementation of those policies and procedures.

Healthcare Compliance Pros agrees – over time, a user›s need to access may change. If it does, role-based access should be re-evaluated and, if needed, modified. Policies and procedures must be in place to terminate physical and electronic access to data before any user leaves the organization. Including the disabling of all the user›s computer and application accounts, changing or disabling facility access codes known to the user, and retrieving organization property, including keys, mobile devices, electronic media, and other records, etc.

Have Additional Questions?

Healthcare organizations can limit their vulnerabilities from external attacks by having policies and technological measures in place that can allow more focus on internal risks. Having training and monitoring implemented from within the organization can help with minimizing these internal threats. However, these internal threats will never be entirely preventable. For further information on how to safeguard your organization from either internal or external threats, please contact Healthcare Compliance Pros by email: support@hcp.md or phone: 855-427-0427.

12 Social Media Procedures to Ensure HIPAA Compliance

Ever purchased a misleadingly easy to put together piece of boxed furniture and decided in arrogance to build it without looking at the instructions? Setting the instruction booklet aside, to be used, only if needed. The finished product sometimes turns out ok, perhaps with a few extra screws, and other times it turned into a disaster! Instructions are important and provide key steps to accomplish a wide-ranging variety of tasks. Yet, in a busy world, many would instead attempt to get things done quickly, their own way than to take the time to follow a step, by step process. The top reasons consumers report not taking the time to read the instructions is because they are poorly written, or they are hard to understand.

Instructions in the world of healthcare compliance consist of policies and procedures. When it comes to Social Media and ensuring HIPAA Compliance, it is not only important for the policy to be read; it is critical for the procedures (which are really the instructions and key steps) to be read and followed. When procedures are poorly written or hard to understand, it could lead to a violation of the HIPAA Privacy and HIPAA Security Rules or compromise your organization's commitment to confidentiality and respect. To help your organization comply with HIPAA requirements, we recommend the following 12 procedures:

Compliance with standards of patient privacy and confidentiality.
In the healthcare industry, patient privacy and confidentiality is vital. The importance of patient privacy and confidentiality extends beyond the walls of the practice, including the internet and social media platforms. Healthcare organizations and their employees must not post any identifiable patient information online without patient authorization unless posting in a patient portal. Patient identifiers (including photographs of patients) such as name, date of birth, diagnosis, etc. should be careful not to be disclosed. Anytime you see anything that looks like it may be a privacy breach, immediately report it to your Compliance Officer.

Maintain separate personal and organization social media content.
It's extremely common to see the blending of business and personal activities. Doing so does come with risks, especially when blending social media activities. Employees should not connect with patients or the patients' families on their personal social media websites. Instead, if an invitation is received to connect with patients or patients' families, ask them to connect with the organization's social media website.

Observe ethical boundaries.
Observe all ethical boundaries and guidelines while connecting with patients. It's essential to consider the patient's perspective of who they believe they are connecting with and their intentions in doing so. Is the interaction in hopes of obtaining advice or to simply be "friends" with the healthcare professional? It is very easy for these boundaries to be blurred when it comes to social media activities between patients and healthcare professionals.

Use privacy settings.
Use privacy settings for both your personal and professional social networking websites. By managing your privacy setting, it is possible to be able to control who sees your information, who can contact you, post on your website, etc. Additionally, it is advisable to examine which third-party applications have access

Continued on page 9

to your profile. Make sure only trusted and verified applications are allowed on your social media websites.

Do not respond to negative comments (unless it is your job to do so).
Never post in response to unfavorable comments on health care rating websites. It is also important to refrain from posting anonymous comments supporting your organization in response to patient grievances. If a negative comment or complaint is posted, bring the matter to the attention of your Compliance Officer or whoever is assigned to respond to and manage social media content. Your organization should carefully decide on the response or action, if any, including whether contacting the host site and asking them to remove the comment is appropriate.

Report inappropriate behavior.
Inform the Compliance Officer or whoever manages social media for your organization of any social media behavior that is inappropriate or if you observe any suspicious activity.

Use disclaimers.
Because you work in the healthcare industry, what you post could be interpreted as medical advice. Therefore, when posting about healthcare topics on personal and professional social media websites, it is important to use disclaimers or statements such as “in our/my opinion” or “according to the (insert name of source).”

Individual behavior is a reflection on the organization.
Recognize that behavior on social media websites is a reflection on you, your co-workers, your organization, and the healthcare industry. The reputation of an organization could be either bolstered or ruined with an individual’s social media behavior.

Never provide medical advice on Social Media.
Avoid discussing patients anonymously and be sure to never provide medical advice or comment on medical issues through social media websites. Doing so could be construed as practicing medicine (with or without a license) and forming a doctor/patient relationship. It is also could be a HIPAA breach, depending on what is implied or disclosed.

What you post online is subject to discovery.
Recognize that anything said or otherwise posted on social media websites is in the public domain and potentially subject to discovery. Regardless of if the post was made through a private social media account or a professional account on social media. If you wouldn’t say it in openly in public places such as a coffee shop or an elevator, do not post it on social media.

Be cautious with what you post and how you post it.
Don’t post anything that could be considered defamatory, profane, libelous, threatening, harassing, abusive, obscene, knowingly false, or otherwise inappropriate. Do be mindful of any content you share, as sharing too much information could compromise your identity, patient information, or sensitive organization data. In the healthcare industry, the fewer details you share online, the safer your information will be.

Never comment on legal issues involving your organization.
While we all have the best of intentions for the organizations we work for, commenting on legal issues, your organization may be involved in on social media sites is a no-no.

While this list is not all-inclusive, by following these 12 procedures, you are on your way to safely using social media while ensuring HIPAA compliance when doing so.

Preparing for healthcare's "new normal" — Managing and leading through and after the COVID-19 crisis

By Owen Dahl FACHE, CHBC, LSSMBB
Independently Contracted Consultant MGMA Consulting

It is important to have a perspective of your role in your organization: Are you managing, leading or both? In a crisis, the tendency is to manage — to get through the issue or the day. This has been essential at least in the initial phase of the COVID-19 pandemic. You have had to address patients, employees, suppliers, payers and so much more.

Do you find yourself staying in this crisis mentality due to issues that constantly arise? Do you have time to stop and think about the future? Can you do both or do you delegate and free up time to do what you do best and/or what your organization needs?

A manager works with and through resources to accomplish a desired result. You may manage resources [e.g., personal protective equipment (PPE)] to an optimal level by distributing and sharing based on the biggest need. But that's only part of the equation. A bigger and equally important (if not paramount) concern is how you manage the team. During this crisis it is essential to maintain high-quality staff, reduce their level of anxiety and prepare them for the future.

In times of crisis, managers should keep these key ideas in mind:

- Don't always react; act as necessary. How effective are you when you react to a situation as opposed to being prepared to address it through thought and awareness? There are on-the-spot decisions that have to be made, but if you reflect on most of your decisions, thoughtful processing leads to better outcomes.
- Delegate. According to former U.S. Sen. Byron Dorgan, "You can delegate authority but not responsibility." This speaks volumes about how you approach a situation that would benefit from others' help or may require others to act. We must delegate authority and responsibility to those who need it at the appropriate time.
- Be flexible. There may be similarity in 80% of situations and the opportunity to build based on past experiences. The other 20% require new actions based upon new circumstances. It is important to recognize these situations and to adapt your approach to managing them or an individual.
- Listen. We often talk about communication and sharing information about the practice with staff. This is essential. But it is equally important to listen to staff and their situation. Listening is a skill we often don't practice because we're too busy. Employees have concerns about their family and the future; they need an outlet to meet their needs.
- Include yourself in the narrative. Don't be afraid to share your concerns and situation with the staff. After all, you are human.
- Trust yourself and others to make it through.
- Look ahead. Think about today, tomorrow and next year when you are dealing with each issue.

Leadership is somewhat different. Leaders offer direction as well as many of the points noted above. As Warren Bennis put it in Learning to Lead: A Workbook on Becoming a Leader. "Managers do things right while leaders do the right thing." This suggests that planning for the future is an essential part of being a leader. That means being optimistic and realistic at the same time.

The three-phase plan presented by federal officials for reopening the country outlines potential changes for businesses, schools and other organizations coming in a matter of weeks or months. What happens during that time and after is anyone's guess, but now is the time for practices to develop a full-scale plan for recovery.

Identify and accept that there are barriers to the future, which include "the way we've always done it" (TW2ADI). The independent nature of each physician breeds the belief that their way is always the best way.

Still, most practices will need to review key processes, such as patient access concerns.

- If your practice is currently only handling telehealth visits, this could be a time to consider changes to your front office and waiting area to optimize that space when patients return.
- With a new mix of virtual visits, your practice likely will need to revisit scheduling and wait times.
- If you rapidly adopted telehealth technology, it's time to start thinking about long-term needs and reimbursement, to optimize further use and development.

This list could be huge, and leaders should identify and prioritize the practice's future needs now before the surge in deferred care comes later this year.

In assessing the response to COVID-19, it is also important for a leader to accept that there have been failures. This is not to dwell on negative outcomes, but rather to use them as learning opportunities. Focus on what can be done to improve and lead your practice into the future.

The leader and the manager aren't necessarily different people; they are different roles that one individual can play, and individual strengths will vary. One is not better than the other, and both roles are necessary to transition your practice to the new normal.