NEW HOME OF THE
DCMA
Highland Park Office Center
1011 Sunnybrook Rd
Suite 904
Miami, Florida 33136
Save the Date

DADE COUNTY MEDICAL ASSOCIATION

Presidential Installation

June 23, 2018  7:00 p.m.

BARBARA MONTFORD, M.D.

Will Be Installed as the First African-American Female President of the Dade County Medical Association

JW MARRIOTT
1109 Brickell Avenue, Miami, Florida 33131
$250 per person. Formal Invitation to follow.

DaDe Coundy Medical Association

political action comittee

Yes, I want to make a difference in Tallahassee.

Name:_____________________________________
Address:___________________________________
Phone:_____________________________________
Fax:_______________________________________
Email:_____________________________________

DCMA/PAC can do without your time, but not without your money!

☐ Physician $100
☐ Spouses $100
☐ Resident/Medical Students $5.00

Please make your check payable and mail to:
DCMA Political Action Committee
Highland Park Office Center
1011 Sunnybrook Road, Suite 904
Miami, Florida 33136

NOT YET A MEMBER OF THE DADE COUNTY MEDICAL ASSOCIATION?

Go to the DCMA website
www.miamimed.com
Click on – Join the DCMA on-line – and follow the instructions.

ALREADY A MEMBER OF THE DADE COUNTY MEDICAL ASSOCIATION?

Have you paid your 2018 dues?

Go to the DCMA website
www.miamimed.com
Click on – Renew your membership dues online – and follow the instructions.
Or call the DCMA at 305 324-8717.
Addressing a Curriculum Gap in Medical School: Professional Development, Personal Financial Literacy, and Compliance

Raul Ravelo, MD
President, Dade County Medical Association

This year marks my thirty-eighth year in practice after graduating from medical school. In those years, I have not only witnessed the scientific advancements and medical breakthroughs that have revolutionized the delivery of healthcare in our country, but I have also learned how to constantly develop my own skills and expertise so that I can provide excellent care to my patients. In fact, the medical profession is built on the adrenaline-pulsing foundation of constant innovation. It is truly an exciting and fulfilling career for any young mind to aspire towards.

Thus, with changes to the medical profession, comes changes to the structure and curriculum of medical schools. For example, the Association of American Medical Colleges recently conducted a study of the curriculum changes occurring from 2016 to 2017 at medical schools across the country. Of the 118 medical schools that responded to the survey, 98 stated that they are providing “enhanced integration of basic science content (such as an organ-system/case-based curriculum),” 95 stated that they are providing “enhanced clinical correlations in the preclinical years,” 40 stated that they are providing “enhanced coordination/ integration of clerkships (such as a longitudinal clinical clerkship),” 78 stated that they are providing “enhanced use of simulation,” and 94 stated that they are providing “enhanced interpersonal education.”

Moreover, top medical schools are overhauling their curricula to adequately prepare future doctors for practice. In 2015, Harvard Medical School revamped its curriculum so that the classes are more interactive, interdisciplinary, and application-focused. Further, our healthcare system moves toward a reimbursement model based on value-based care, the American Medical Association (“AMA”) has also suggested the introduction of classes on payment models. In furtherance of the AMA’s goal, it has given $11 million in grants for 32 schools to foster innovative projects that have the potential to transform the medical school education system, including a grant to our very own Florida International University Herbert Wertheim College of Medicine as it developed the Green Family Foundation Neighborhood Health Education and Learning Program. To state that medical school today is very different from when I went to medical school would be a grave understatement.

Yet, there are still some items I wish I learned in medical school, and they are yet to be addressed in most curriculums around the country. After medical school, for example, I had instances where I asked myself the following questions: How do I prepare for a job interview? When they give me an employment agreement, how do I know if it is a “good” or “fair” contract? How do I get out of debt, and how long will it take? This action makes good business sense but is it legal? What if my supervisor asks me to do something that feels wrong?

As the medical school curriculum continues to transform and restructure towards more practice-oriented classes and interdisciplinary courses, as noted above, so that medical students can best serve their patients, it is also important to focus on the wellbeing—both personal and professional—of the students themselves so that they can be better prepared for their careers. Notably, there are three areas that I think should be addressed.

First, there needs to be a greater emphasis on career planning at medical schools. There should be an increase in support for students as they put together their job application packets, weigh options for jobs post-residency (e.g., employment agreements), and prepare for job interviews. Most importantly, I believe, is to help students understand how to weigh the different options when they receive a job after residency and for students to fundamentally understand how to read an employment agreement. The medical field is one of the few employment sectors that not only requires a written agreement, but also one that includes regulatory components within those agreements. Thus, it is important for a future doctor to understand how to read an agreement and how to measure one agreement against another.

Second, medical students should be educated on their financial future. While residency timelines and locations can vary a medical student’s average salary, there is a pretty reliable financial outlook for a medical student and an average level of debt, $119,000 to $150,000. Therefore, medical schools would be able to teach, at the very least, some foundational financial skills to all students that include an overview of the expected loan repayment timelines and programs, debt consolidation strategies, and financial strategies for the students’ medical school, residency, and post-residency years. If students learn how to manage their debt, then their financial worries and lifestyles will not seriously detract from their professional obligations or put their finances at risk through bankruptcy or diminished credit scores.

Lastly, medical schools should teach a more thorough legal course about the medical profession. So much of our days are spent addressing life-changing and life-threatening issues. Indeed, making those decisions is hard enough without worrying about the legal ramifications of our actions or inactions. Seemingly innocuous actions can have legal and regulatory impacts, especially under the Anti-Kickback Statute, Stark Law, and the False Claims Act. These future doctors may enter into the grey areas of these laws themselves, but it is also likely that they may be asked to do something that will violate those laws. To prevent those issues from occurring, they should learn early in their practice how to act ethically and legally under these legal frameworks. In fact, it should be quite simple given that the Office of Inspector General for the U.S. Department of Health & Human Services has developed materials geared towards new physicians.

If medical schools were to adopt more in-depth courses dedicated towards the future professional and personal wellbeing of medical students, then the overall wellness of doctors will ultimately improve. With these tools, I feel that more doctors will report increased satisfaction in their life because they will remain at ease during what are often very stressful times and situations.

Raul Ravelo, MD
President, DCMA 2017-2018

References
MIAMI-DADE
MATERNAL MENTAL HEALTH SYMPOSIUM

Thursday, May 3, 2018

Jackson Memorial Hospital
Diagnostic Treatment Center (DTC)
Room 259

Approximately 35,000 women in Florida experience depression or anxiety around pregnancy each year. Up to 75% of these women are not screened or treated.

Join us for a discussion of maternal mental health issues and the ways in which healthcare professionals can assist women and families struggling with this burden.

For question & additional information, please email HSCMDTraining@hscmd.org
EHRs Can Advance Good Medicine – If Doctors Are Aware of the Risks

By David B. Troxel, MD, Medical Director, The Doctors Company

Historically, the doctor-patient relationship has been at the heart of medical practice, with administrative tasks and record-keeping at the border.

Today, that critical balance is at risk. Nearly all hospitals and 80 percent of medical practices use electronic health records (EHRs), presumably to help improve access to health information and increase productivity. The problem is that none of these digital tools were designed specifically to advance the practice of good medicine.

Consider these stark statistics: Every hour doctors spend with patients, they dedicate nearly two more hours to maintaining EHRs and clerical work. Yet even when physicians are with patients, they’re spending approximately 37 percent of their time interacting with EHRs or other desk work.

We are now witnessing the highest levels of physician burnout on record. Indeed, the rise of documentation demands and decrease of meaningful patient interactions has led to major physician frustrations—while making it harder for physicians to deliver quality care.

For these reasons and more, the EHR has introduced patient safety risks and unanticipated medical liability risks. According to a new study from The Doctors Company, the nation’s largest physician-owned medical malpractice insurer, the number of EHR-related medical malpractice claims has risen over the past 10 years.

Factors Behind EHR Errors

For the most part, the EHR is a contributing factor in an EHR-related claim and not the primary cause. This and their low frequency (0.9 percent of all claims) suggest that EHRs infrequently result in adverse events of sufficient severity to develop into a malpractice claim.

When EHRs are a factor in a claim, the study showed that user factors (such as data entry errors, copy-and-paste issues, alert fatigue, and EHR conversion issues) contributed to nearly 60 percent of claims. As computer users, we all copy and paste. Therefore, it’s no surprise that time-pressured physicians embrace the same habits when using EHRs. In fact, the University of California San Francisco Medical Center—today considered a top five medical center in the United States—reviewed more than 23,000 of their own progress notes over an eight-month period and found that, on average, clinicians manually entered just 18 percent of the text in each note, while 46 percent was copied and 36 percent was imported.

System factors (such as data routing problems, EHR fragmentation, and inappropriate drop-down menu responses) contributed to 50 percent of claims. EHR fragmentation was among the most prominent system factors, contributing to 12 percent of errors. This factor means that different components of a single patient encounter might not be located together in the EHR. Consequently, doctors must check in different places to find laboratory and x-ray results, histories and physicals, etc.—resulting in important information being overlooked or unidentified.

Re-Claiming the Doctor-Patient Relationship

One overwhelming response to adjust to burdens introduced by EHRs has been the rapid growth of medical scribes. Nearly 20 percent of medical practices are using scribes to help untether physicians from the EHR, with many doctors citing improved efficiency and satisfaction. Yet while scribes can offer great advantages, they can be a double-edged sword. According to a survey of hundreds of physicians from The Doctors Company, the lack of standardized training and variability in experience among scribes poses risks to data accuracy and delivery of care—which could increase liability for the patient and physician alike.

With or without scribes, lowering risk begins with each patient visit. At the beginning of each new session, doctors should inform patients of the purpose of the EHR and emphasize they are listening closely even though they might be typing during the appointment. Practices can set up treatment rooms so the patient can watch the screen and see what is being typed. It is also helpful to summarize or read the note to the patient to demonstrate that you have listened, and ask, “Do I have it right?” If the doctor is using a medical scribe to untether them from their EHR, the same principle applies.

Patients must also become their own advocates. They can ask their doctor to read back the EHR notes or review what has been written. Patients can interact with their health record online through patient portals and review their medical record as well as disease-specific educational materials and drug safety information. It is important that they communicate any errors they find as well as personal information updates to the physician.

What the Future Holds

As with any challenge of major proportions, progress will take time. But I’m optimistic that the EHR will evolve over the next 5 to 10 years and improve both the quality of medical care and patient safety.

Optimizing the EHR will involve:

• Redesigning EHR workflows to reflect clinical practice workflows in hospital, clinic, and office environments. It is essential that physicians and other healthcare providers be involved in this endeavor.
• Developing standardized diagnostic and treatment protocols.
• Researching medical artificial intelligence (AI). This is underway and will doubtless play a significant role in future medical practice.
• Making EHR interoperability a high priority.
• Applying “big data” techniques to healthcare. This is underway and, like AI, will lead to new knowledge insights that will change the practice of medicine.

Today, what I hear from The Doctors Company’s 80,000 member physicians is encouraging. Doctors are eager to “reclaim” their profession and refocus patient relationships amidst the new demands of today’s digital age. Into the future, new protocols, policies, and training programs must take these small successes to a large scale.

The guidelines suggested here are not rules, do not constitute legal advice, and do not ensure a successful outcome. The ultimate decision regarding the appropriateness of any treatment must be made by each healthcare provider in light of all circumstances prevailing in the individual situation and in accordance with the laws of the jurisdiction in which the care is rendered.
Peace of Mind.
Women Physician Event
On March 8, 2018, the Dade County Medical Association and New York Life Insurance presented

Critical Moves Under The New Tax Laws
On Thursday, March 8, 2018, the DCMA and Vickie Frazier-Williams with New York Life presented a program geared to women physicians on how the new tax laws will impact their practice and financial future. The conversation was led by Gerri Lazarre, CPA. The event was held at Caffe Abbracci in Coral Gables.
Many physician practices and healthcare organizations not affiliated with hospital systems remain confused concerning the difference between a corporate compliance plan and a HIPAA compliance plan. These organizations point to a notebook on a shelf in the administrator's office that sets out policies and procedures for staff in avoiding and reporting violations of the federal and Florida illegal remuneration/kickback prohibitions and the physician self-referral restrictions included in the so-called Stark Law and the Florida Physician Self-Referral Act; i.e., a corporate compliance plan. Unfortunately, that plan is unlikely to address the issues raised by HIPAA.

Corporate Compliance Plan vs. HIPAA Compliance Plan

Most healthcare organizations are familiar with corporate compliance plans, which are intended to minimize the likelihood of an organization violating either the federal or Florida illegal remuneration/kickback prohibitions or these jurisdictions' physician self-referral restrictions (the so-called “Stark Law” and the Florida Physician Self-Referral Act). In contrast, a HIPAA compliance plan (“HIPAA Plan”) is designed to enable a healthcare provider to comply with the requirements imposed by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”), and their implementing regulations (collectively referred to herein as “HIPAA”). A HIPAA Plan addresses risks and vulnerabilities posed by the creation, maintenance, storage, and transmission of medical records – both paper and electronic.

While the Federal Sentencing Guidelines provide a frame for developing a corporate compliance plan, the parameters of a HIPAA Plan may not appear to be clearly delineated. Perhaps this is a consequence of HIPAA’s focus on the collection, storage, and transmission of patients’ personal health information (“PHI”), which causes many healthcare practitioners (and their legal counsel) to throw up their hands. Perhaps it is because the HHS-Office of Civil Rights (“OCR”), has left it up to each affected party (that is, each “Covered Entity” and “Business Associate”) to develop a HIPAA Plan that best fits its unique challenges. Perhaps it is because HIPAA is comprised of three separate and distinct sets of obligations; the Security Standards for the Protection of Electronic Protected Health Information (the “Security Rule”), Notification in the Case of Breach of Unsecured Protected Health Information (the “Breach Notification Rule”), and Privacy of Individually Identifiable Health Information (the “Privacy Rule”). In any case, every Covered Entity and Business Associate is expected to develop, implement, maintain, and (over time) revise its HIPAA Plan.

HIPAA Plan – Steps To Develop

STEP 1: COMMITMENT

Like a corporate compliance plan, the initial steps in the HIPAA Plan process are to have the organization’s governing body and senior management (i) clearly commit to this initiative, and (ii) provide sufficient resources (ex. money and manpower) for the organization to develop and implement a HIPAA Plan. Without a clear commitment from the governing body and senior management, the organization’s employees and independent contractors are unlikely to support the effort to develop, implement, and maintain an effective HIPAA Plan. A commitment to provide the needed resources to this initiative tangibly demonstrates the seriousness with which the organization’s governing body and senior management view this effort. It also sets the stage for developing a HIPAA Plan that addresses that organization’s obligation to protect the privacy and security of patients’ protected health information.

STEP 2: SCALABILITY

In developing the Privacy, Security, and Breach Notification Rules, OCR recognized that Covered Entities and their Business Associates vary widely in size, resources, and vulnerabilities. This agency has made clear that it expects each organization to commit resources to its HIPAA Plan that reflect that organization’s size and resources. Thus, for example, OCR expects the resources a multihospital healthcare system commits to its HIPAA Plan are going to be significantly greater than the resources a solo physician can devote to this effort.

STEP 3: BREAKING PLAN DEVELOPMENT INTO SMALLER COMPONENTS

Developing a HIPAA Plan can be divided into three (3) segments: the Privacy Rule, the Security Rule, and the Breach Notification Rule. Although these Rules focus on different issues, they are interrelated. Consequently, it is likely that some or all of the organization’s staff assigned to developing its HIPAA Plan will focus on more than one Rule.

a. Privacy Rule

HIPAA’s Privacy Rule, generally speaking, focuses on measures designed to protect the confidentiality and integrity of personal health information stored and transmitted in both a physical medium (ex. paper medical records) and electronically. These measures are divided into three (3) categories: Physical Safeguards, Technical Safeguards, and Administrative Safeguards.

Physical Safeguards involve those physical measures, policies, and procedures a Covered Entity or Business Associate is expected to adopt in order to protect the privacy of the personal health information in its possession. Examples of these safeguards include storing paper records in cabinets that are locked when not in use, and positioning computer screens so they are not visible to the public.

Technical Safeguards are the technology, and policies and procedures used to protect electronic personal health information and control access to it. These safeguards include requiring that each member of the workforce have access to only those elements of patients’ electronic personal health information (“ePHI”) necessary for performing their duties. For example, a laboratory technician has no reason to access a patient’s radiology findings. Other examples of Technical Safeguards include ensuring that all software updates are timely installed and using current anti-virus software.

Administrative Safeguards focus on the organization’s internal policies, procedures, and maintenance of security measures to protect both PHI and ePHI. Establishing and maintaining a Business Associate Agreement that reflects the then-current expectations for Business Associates is one type of Administrative Safeguard. Another example of an Administrative Safeguard is the organization’s ability to readily
terminate an individual's access to both physical and electronic personal health records (PHI and ePHI) immediately upon termination of his/her employment or contractor relationship with the organization.

b. Security Rule
The Security Rule addresses protecting ePHI in particular. Specifically, the Security Rule applies to Covered Entities and their Business Associates who transmit ePHI. Although an organization of any size or sophistication probably can develop policies and procedures that address the Privacy Rule without the assistance of outside expertise, the Security Rule raise a number of issues for which smaller organizations are likely to need outside expertise.

The Security Rule obligates Covered Entities and Business Associates to maintain reasonable and appropriate administrative, technical, and physician safeguards (see, Privacy Rule discussion, above) for the purposes of:

- Ensuring the confidentiality, integrity, and availability of ePHI;
- Identifying and protecting ePHI in its possession from reasonably anticipated threats to its integrity or security;
- Protecting ePHI from unauthorized uses or disclosures; and
- Ensuring that the organization's workforce complies with these safeguards.

The first step in satisfying the Security Rule is for the organization to conduct a “Risk Analysis”. The purposes of this analysis are to:

(i) identify and evaluate the likelihood and impact of potential risks to ePHI;
(ii) initiate the implementation of appropriate security measures in light of that evaluation;
(iii) document the security measures chosen and the rationale for doing so; and
(iv) maintain ongoing, reasonable and appropriate security protections.

OIG has made clear that the Risk Analysis process should be on-going. Thus, organizations that cannot justify the expense of in-house IT personnel to perform this function will need to seek the assistance of an outside contractor with the relevant expertise on an on-going basis.

The Security Rule also divides its standards into three categories—administrative, physical, and technical. While some of these standards are “required”, others are “addressable”. An organization cannot ignore an “addressable” standard. However, the organization has the ability to determine whether that standard is reasonable and appropriate for it to implement. If the organization determines not to implement an “addressable” Standard (for example, it is cost prohibitive to do so), it is expected to document the basis for that decision. Thus, the Security Rule is one area in which the concept of scalability (discussed above) is particularly relevant.

A question that permeates the Privacy and Security Rules is what are a Covered Entity’s or Business Associate’s obligations in the event PHI or ePHI is improperly disclosed, whether innocently or as the result of malice within or outside of the organization? Generally, the Breach Notification Rule requires the Covered Entity to notify a patient that their PHI or ePHI has been disclosed without authorization within sixty (60) days after it is discovered. Depending upon the number of patient records involved in a breach, the Covered Entity also must notify OCR within that same time frame.

If an unauthorized disclosure of PHI or ePHI (a “breach”) occurs with respect to information in the possession of a Business Associate, the 60-day clock runs from the date that entity discovers the breach. Thus, while not expressly included in the Breach Notification Rule, the Business Associate Agreement between a Covered Entity and its Business Associates should require these contractors to report any breach of the Covered Entity’s PHI or ePHI in a shorter period of time.

Covers Entities and their Business Associates also must be aware of any relevant state breach notification requirements. For example, under the Florida Information Protection Act an individual must be notified of a breach within thirty (30) days and, depending on the number of individuals whose information is improperly disclosed, the national credit reporting agencies also must be notified.

STEP 4: PUTTING THE HIPAA PLAN TOGETHER
It may not be possible, or practical, for an organization to implement its complete HIPAA Plan at one time. An organization may decide to do so in stages. If that is the case, there are a couple of considerations to keep in mind. First, a committee should review all of the policies and procedures in order to both ensure that the Plan is cohesive and does not inadvertently overlook a known risk or obligation. Second, that same committee should be responsible for reviewing the Plan, whatever its stage of development, to ensure that there have been no changes in law, circumstances or the organization’s experience that require the modification of any portion already adopted. Third, as with the corporate compliance plan, reviewing and updating a HIPAA Plan should become a regular and scheduled activity of every organization that adopts one.

Finally, an effective HIPAA Plan depends on the organization’s commitment to satisfying all of the Rules’ standards to the best of its ability. Adopting, implementing, maintaining and regularly reviewing policies, procedures, and practices intended to minimize the likelihood of an unauthorized breach of patients’ PHI or ePHI has become a “standard business practice” in the health care industry and for those vendors with which its members do business. Neither the public nor OIG will dismiss a data breach as not important or “the cost of doing business” any longer, regardless of the size or sophistication of the organization. If your organization has not done so already, the prudent course is for it to reach out to those who work in this area and begin the process of developing a HIPAA Plan ASAP.

About the Author: Stephen H. Siegel, Esq.
Mr. Siegel’s assists physicians, other healthcare providers, and vendors maximize their businesses while minimizing their legal and business risks. A member of Broad and Cassel’s Health Law and White Collar Defense and Compliance Practice Groups, Mr. Siegel is Board Certified in Health Law by the Florida Bar and Certified in both Healthcare Compliance and Healthcare Privacy Compliance by the Health Care Compliance Association. He received his Juris Doctor from the Georgetown University Law Center.

1 That is, every health plan, health care clearinghouse and health care provider that stores or transmits electronic health information. 45 C.F.R. §160.103-Definitions.
Attention

The Board of Directors has voted to amend certain sections in the DCMA Bylaws. Please go to the DCMA website – www.miamimed.com to review. Comments should be sent to phandler@miamimed.com no later than May 1, 2018.

Miami Medicine is the official publication of the Dade County Medical Association (DCMA).

Advertising in Miami Medicine does not imply approval or endorsement by the DCMA. Any ads stated approval by the DCMA have been declared by the DCMA as worthy of consideration by its members; however, the DCMA shall have no liability in the event the user is dissatisfied. The DCMA maintains a sponsorship program which endorses select vendors and organizations whose products and services may be beneficial to the membership and/or from which the DCMA may receive financial support.

Miami Medicine assumes no responsibility for statements made by its contributors. Opinions expressed by authors are their own, and not necessarily those of Miami Medicine or the DCMA. Miami Medicine reserves the right to edit all contributions for clarity and length, as well as to reject any material submitted.

Subscription: $53.50 annually; single issue $5.35
Regions’ Doctor Mortgage Program

Whether you are a seasoned physician or just beginning residency, our Doctor Mortgage program was designed specifically with you in mind. Simply put, this top-class loan program meets the unique demands of physicians seeking home financing.

Here are the program’s features:

- Open to medical physicians, including residents, fellows, doctors of dental medicine (DMD/DDS), or doctors of osteopathy (DO).
- Proof of valid employment agreement or minimum three years self-employed.
- Fixed rate and adjustable rate available.
- Private mortgage insurance not required.
- Loan to Value (LTV) up to 100% in stable markets.
- Only available for primary residences, single-family residences, and townhomes.
- Loan amounts up to $1,000,000.
- No limitation to years in practice.

Contact me to learn more about Regions’ Doctor Mortgage Program. I look forward to working with you.

Frank Silva
NMLS# 546580
Mortgage Loan Originator
305-774-5217 (o)
305-333-5723 (c)
frank.silva@regions.com

What’s Your Next Move?

Buying that cyber policy you keep putting off just might be one of the best decisions you will ever make.

Rather than paying the ransom and having to deal with all of the headaches, problems and HIPAA violations triggered by the attack, a solid cyber insurance policy will give you much more than just peace of mind. One call can get a team of experts at your defense, covering expenses and taking your practice back!

If you have a standard cyber policy, you are most probably alarmingly underinsured. Put the experts at your defense in this ever-changing cyber environment. Call Danna-Gracey at 800.966.2120 for a no-obligation assessment of your current cyber policy. Your practice is worth it.

800.966.2120 • tom@dannagracey.com • www.dannagracey.com
Tirelessly defending the practice of **GOOD MEDICINE**.

*We’re taking the mal out of malpractice insurance.*

By constantly looking ahead, we help our members anticipate issues before they can become problems. And should frivolous claims ever threaten their good name, we fight to win—both in and out of the courtroom. It’s a strategy made for your success that delivers malpractice insurance without the mal. See how at [thedoctors.com](http://thedoctors.com)