EXECUTIVE DECISIONS IN
DERMATOLOGY
SEPTEMBER & OCTOBER 2016

HIPAA and Ransomware

Read more on **PAGE 9**

ADAM
Association of Dermatology Administrators & Managers

EXECUTIVE DECISIONS IN
DERMATOLOGY
SEPTEMBER & OCTOBER 2016

inside

Executive Decisions in Dermatology is a bimonthly publication of the **Association of Dermatology Administrators & Managers (ADAM).** ADAM is the only national organization dedicated to dermatology administrative professionals. ADAM offers its members exclusive access to educational opportunities and resources needed to help their practices grow. Our 650 members (and growing daily!) include administrators, practice managers, attorneys, accountants and physicians in private, group and academic practice.

To join ADAM or for more information, please visit our Website at ***ada-m.org****, call* ***866.480.3573****, email* ***ADAMinfo@shcare.net****, fax* ***800.671.3763*** *or write Association of Dermatology Administrators & Managers,* ***1120 G Street, NW, Suite 1000, Washington, DC 20005****.*

ADAM
Association of Dermatology Administrators & Managers

2016
ADAM OFFICERS AND BOARD OF DIRECTORS

Gabi Brockelsby
PRESIDENT
Murfreesboro Dermatology Clinics, PLC, MDC
Murfreesboro, TN

Tony Davis
PRESIDENT ELECT
Dermatology Specialists, P.A.
Edina, MN

Janice Smith
VICE PRESIDENT
Spencer Dermatology Associates, LLC
Crawfordsville, IN

Jill Sheon
SECRETARY/TREASURER
Children's Dermatology Services
Pittsburgh, PA

Elizabeth Edwards
University of Texas
Southwestern Medical Center
Dallas, TX

Bill Kenney
Dermatology Consultants, PA
Saint Paul, MN

Virginia King-Barker
Duke University
Durham, NC

Shannon Page
New England Dermatology & Laser Center
Springfield, MA

Angela Short, MHA, CPCO, CPC-D
Northeast Dermatology Associates
Lawrence, MA

George Smaistrla
Bellaire Dermatology Associates
Ballaire, TX

Jeff Stewart
Mendelson Dermatology
Phoenix, AZ

Wendy Stoehr
Advanced Dermatology and Skin Cancer
Spokane Valley, WA

Diane Turpin, JD
ADAM Headquarters
Washington, DC

Patricia Chan
ADAM Headquarters
Washington, DC

President's *Message*

If we can rely on nothing else about our industry we can rely on change.

Since our last publication, we have seen the proposed 2017 Medicare fee schedule, new requirements for HIPAA training, announcements of HIPAA audits, changes to overtime rules, and much more. The one constant through this is the information ADAM is pleased to provide to the members.

To that end, ADAM is actively updating the Resources and Forms tabs on the website to insure the information available to our members is as up-to-date and relevant as possible. Have you developed a form you think would benefit others? If you send it to ADAM Manager, Patricia Chan at Patricia.Chan@shcare.net, she will upload it to the appropriate tab on the website. Don't be surprised if we periodically ask for your versions of a policy or procedure to add some more depth to the Resources. If you haven't taken a look recently at these sections, available only to Members, take a peek and see what's out there. I expect there will be some major modifications to this area of the website by the end of the year so keep looking!

It is our goal to make ADAM the resource you go to first, whether it is to our newsletter, our website, or our Linked In page. I know it is one of the benefits I value most about ADAM and I hope you do too!

Warmest Regards,

Gabi Brockelsby
ADAM President

WHAT MAKES ADAM A STRONG ORGANIZATION

By **Elizabeth Edwards,** Manager
University of Texas
Southwestern Medical Center

IN OUR WORLD OF EVER TIGHTENING BUDGETS COMBINED WITH NEW REGULATIONS ROLLING OUT OF WASHINGTON EVERY YEAR, IT BECOMES HARDER AND HARDER TO CHOOSE WHICH MEMBERSHIPS TO KEEP AND WHICH ONES TO RELINQUISH. CERTAINLY, ADAM HAS A LOT TO OFFER MEMBERS WHICH ADDS VALUE TO OUR PRACTICES. HERE ARE A FEW OF THE BENEFITS:

- **EDUCATIONAL OPPORTUNITIES**
  Throughout the year, the webinars, View from Capitol Hill, and *Executive Decisions in Dermatology* provide information on practice management, financial reporting, team building, staff engagement, and upcoming legislation. Combined with our Annual Meeting, members have a vast cache of information at their fingertips.
- **NETWORKING**
  LinkedIn, Facebook, and the Annual Meeting offers us a way to connect with each other, make friends, ask questions and get advice.
- **BENCHMARKING**
  This is a new development but very exciting. We now have a tool to help guide us in our practices as we see how we compare to others in Dermatology related to revenues, practice size, staff salaries, etc.

While all of the above are valuable, I don't think they are what make ADAM a strong organization. I think it's our membership. ADAM is made up of large and small practices along with academic medical centers. Together, we encompass all aspects of the specialty to include Medical Dermatology, Mohs Surgery, Cosmetics, Dermatopathology, and Pediatric Dermatology. Beyond that, our membership offers a variety of educational opportunities to residents, fellows, medical students, college students, and PAs within their practices. Our diversity is one of our strengths.

Our wealth of experience is another asset. Our membership encompasses a variety of roles that span a practice. We have Billing Managers, Educational Coordinators, Financial Managers, Attorneys, Practice Managers, Physicians, and Residents, all of which are at different phases of their career in Dermatology – the new and the experienced. Each brings a unique perspective and knowledge base to our organization.

> **THERE IS ALWAYS STRENGTH IN NUMBERS. THE MORE INDIVIDUALS OR ORGANIZATIONS THAT YOU CAN RALLY TO YOUR CAUSE, THE BETTER.**

The noted journalist and author, Mark Shield's wrote, "There is always strength in numbers. The more individuals or organizations that you can rally to your cause, the better." Conversely, building the membership of an organization also strengthens individual members. Growth creates opportunities for expanding existing membership benefits and infuses new creative ideas into an organization which in turn, provides individual members with new, innovative tools/ resources for daily management.

ADAM has helped me grow professionally in so many ways. Here's one example: through the webinars and Annual Meeting, my staff and I have learned a great deal about MACRA and MIPS. Two of the Vice Presidents at my university asked us to share the webinar dates and times with them because we had more information about both then they did. In an academic institution, that's a very rare occurrence. I'm very honored and proud to be part of this group which has mentored, informed, and encouraged me.

With that in mind, I would like to challenge all of us (me included) to reach out to our colleagues within and outside our practice about becoming members of ADAM. **During the month of September, the cost of membership is only $425 and is effective through December 2017.** This is a great savings off the regular price and provides a wonderful opportunity for those just discovering ADAM to try us out. Let's add to our strength by sharing ADAM with others. ■

THE OVERTIME RULES HAVE CHANGED

WHAT IT MEANS TO YOUR PRACTICE

By **Kathy White, FACMPE, PHR**

On May 23, 2016, the Department of Labor's Wage and Hour Division published in the Federal Register the final rule updating the overtime regulations. The new regulations will automatically extend overtime pay protections to over **4 million workers** within the first year of implementation and will no doubt prove to be quite costly to employers. Based on estimates by the DOL, the new regulation will cost private employers $1.8 billion in the first year.

Regardless of the expected impact, most Americans feel that this decision is long overdue. Since 1938, the FLSA–Fair Labor Standards Act- has had seven updates to the salary level requirements for exemption. The decision to increase the salary threshold was based on the DOL's conclusion that the last update in salary level in 2004 was too low. The salary threshold represents one of three tests necessary to support exemption classification for employees:

1. **Salary Basis Test**: the exempt employee must be paid a predetermined and fixed salary that is not subject to reduction based on the quality or quantity of work performed by the employee;
2. **Salary Level Test:** the exempt employee must be paid a set threshold or minimum amount determined by the DOL; and
3. **Duties Test:** the exempt employee's job duties must primarily involve duties related to the classification of executive, administrative, or professional which are defined by the DOL regulations.

With the final ruling effective December 1, 2016, the only changes to the requirements for exemption are related to the "Salary Level Test." It must be noted that any employee considered for exemption will still be required to satisfy the other two unchanged tests related to how they are paid and the required duties based on type of exemption. If an employee's salary threshold does not meet the new requirement he/she will not be classified as exempt and thus will be eligible for overtime pay. The revised regulation (29 C.F.R. 541) changes are as follows:

	SALARY THRESHOLD		OVERTIME ELIGIBILITY	HIGHLY COMPENSATED EXEMPTION
	ANNUAL	WEEKLY		
OLD RULES	**$23,660**	**$455**	**Not Eligible**	**$100,000**
NEW OVERTIME RULES*	**$47,476**	**$913**	**Not Eligible**	**$134,004**

** The DOL changed the regulations to allow nondiscretionary bonuses and incentive payments (including commissions) to satisfy up to 10 percent of the standard salary test requirement. For an employer to be able to credit nondiscretionary bonuses and incentive payments (including commissions) toward a portion of the standard salary level test, those payments must be paid on a quarterly or more frequent basis.*

The DOL has doubled the overtime salary threshold. The impact on small businesses, such as medical practices, will be significant due to the fact that most employees' current salaries may not meet the new requirements. Not only are managers faced with additional staff cost for overtime, they must deal with the obvious morale issues for those who were previously classified as exempt. For many managers this has been an eye opening and stressful issue to address.

Recently, after speaking for a local MGMA Chapter on "Hot Topics in Human Resources," I received a call from a manager who realized that she truly had more to contend with than most who had attended my session. The manager was new to the role of practice manager, having left the hospital setting to manage a small local group.

The topics of the session prompted the manager to look at their payroll and status of each employee. Her findings were that all employees in their organization were in fact paid a salary and none had ever completed timecards. Additionally, none of her employees had a job description.

Many small businesses are faced with the fact that they were not compliant prior to these new changes. This is one of the reasons that we stress the importance of job descriptions

"HER FINDINGS WERE THAT ALL EMPLOYEES IN THEIR ORGANIZATION WERE IN FACT PAID A SALARY AND NONE HAD EVER COMPLETED TIMECARDS. ADDITIONALLY, NONE OF HER EMPLOYEES HAD A JOB DESCRIPTION."

for every employee. This manager had to start from scratch with job descriptions and policies regarding time keeping to ensure compliance with the regulations currently in place before she can even begin to focus on the new overtime rules. One of the concerns voiced by her physicians is the potential for morale issues. Changing an employee's status from salary to hourly may feel like a demotion. Under the new requirements, in this scenario, the manager will be the only administrative employee who meets the test for exemption.

We discussed the importance of effectively communicating the value of all employees, their roles and commitment to their practice. Secondly, it was important to point out that the practice would now be paying time-and-a-half for any time worked over 40 hours in a work week. They further evaluated workload and methods that they could use to control overtime, such as working as a team.

As a result of the recent SVMIC Webinars presented by Scott Hickman, JD with Sherrard, Roe, Voigt & Harbison in Nashville we have received many calls regarding what managers should do to prepare for the imminent changes. Managers should lay the groundwork now by doing the following:

- Ensure that all employees have **up-to-date job descriptions.**
- Identify your current exempt employees whose **annual compensation is less than $47,476** and verify that the duties test is met before proceeding in analysis.
- Determine how much overtime each of these exempt employees routinely work. Then **annualize the annual hours to properly calculate the potential overtime cost for a year.** Compare the outcome to the new annual threshold. Having this information in a report format will assist in the review.
- Evaluate **issues that may impact overtime and require new policies** regarding tracking such as:
  - Working from home – offsite including phone calls, text messages and emails after hours
  - On-call time
  - Commuting between offices
- Meet with management/board to **determine the most cost-effective option** for each affected employee who will now be eligible for overtime pay.

OPTIONS ARE:

- **Increase the employee's salary** to the minimum necessary to remain exempt ($913 per week).
- **Re-classify the employee as non-exempt** and pay overtime for any hours worked over 40 hours in a week. Those employees whose duties meet the requirement for exempt status should be reevaluated annually.
- **Pay overtime above salary.** Employers can continue to pay employees who will now be eligible for overtime (non-exempt) a set weekly salary but must pay overtime for hours worked over 40 hours in a week. This may be an option for employees who have been guaranteed a salary and typically work less than 40 hours except when there are occasional weeks that require overtime.
- **Develop your action plan for communicating the changes** required for each affected employee. It is likely that many of your employees will be looking for answers about how this will impact them.
- **Evaluate options for job sharing** and hiring additional part-time staff to reduce overtime.

As each practice manager prepares for these changes, it is important to also review policies related to meal and rest breaks and to understand both state and federal requirements. Changes may be necessary related to the rotation of lunch breaks and other breaks to ensure staffing is adequate at all times.

One important objective is to train supervisors on the necessary changes in managing staff workflow and monitoring overtime. This will require advance planning for staff scheduling to best meet the workflow of the practice. Lean process analysis may prove to be helpful in reworking responsibilities to meet these challenges. Additionally, training and discussion will be needed related to "off-the-clock" work that may have been done in the past by employees who now may be non-exempt. For many employees, this transition from exempt to hourly will be a difficult transition because they may still think like exempt personnel, potentially resulting in their decision to finish up work from home after hours.

Management must determine the best method to monitor remote access to systems by employees to properly keep up with time worked while outside the practice. This may require creating rules regarding working from home which prohibit access to the network outside of employer's defined hours. Additionally, the practice's IT department may need to implement monitoring software that records all activity on computers on or off the network and alerts Management of access after-hours. With effective technology the practice may choose to alert those logging in that they cannot access their system after hours without supervisor approval. ■

Additional Information:

- For details on the final overtime rule: https:// www.dol.gov/whd/overtime/final2016
- For review of SVMIC Overtime Webinar: https://www.svmic.com/Home/education/webinars/
- When state laws differ from the federal FLSA, an employer must comply with the standard most protective to employees. Links to your state labor department can be found at www.dol.gov/whd/ contacts/state_of.htm
- Or your practice corporate counsel or accountant

HIPAA AND RANSOMWARE

By **Gabi Brockelsby**
Administrator, Murfreesboro Dermatology Clinic

HOSPITALS, PHYSICIAN OFFICES, LARGE AND SMALL BUSINESSES, LAW ENFORCEMENT AGENCIES, AND GOVERNMENTAL AGENCIES HAVE ALL RECENTLY BEEN IMPACTED BY RANSOMWARE. THE DEPARTMENT OF HUMAN SERVICES AND OFFICE OF CIVIL RIGHTS HAVE RECENTLY ISSUED NEW GUIDANCE ON RANSOMWARE AWARENESS, TRAINING, AND PREVENTION.

Ransomware is a malicious software, sometimes referred to as malware, that encrypts, or locks, your data until a ransom is paid. The distinction between malware that may infect your computer with a virus and ransomware is that ransomware denies the user access to their data. Most often this is done using a key known only to the hacker who employed the ransomware. After the data is encrypted, the ransomware instructs the user to pay the ransom using an untraceable form of payment such as Bitcoin in order to receive the decryption key. But there are other, more destructive forms of ransomware as well.

Ransomware has been around for a few years but the frequency of the attacks is dramatically increasing. The concept dates back to the distribution of the "AIDS Trojan Virus" via floppy disk through the postal system back in 1989. The next documented attack was via e-mail in 2005. Since then hackers developing ransomware have evolved to embedding their malware in malicious advertisements, USB drives, macros embedded in documents, archived files, fake websites and more.

HOW PERVASIVE HAVE RANSOMWARE ATTACKS BECOME?

3% of attacked individuals and entities pay the ransom;

Last year about **$20 million** was paid due to ransomware attacks;

So far in 2016 over **$200 million** has been paid;

One government interagency report indicates an average of **4,000** daily ransomware attacks since early 2016

Ransomware attacks have increased by **2000%** (and, yes, that is two THOUSAND) in the last 9 months.

Imagine not being able to access your patients' electronic medical record. Imagine never being able to access the records again. The ramifications could be disastrous financially and from the ability to treat patients. Earlier this year Methodist Hospital in Hendersonville, Kentucky went into an "internal state of emergency" following a ransomware attack. Additionally, we have to consider the implications under both the Privacy and Security Rules of the Health Insurance Portability and Accountability Act or HIPAA.

According to the Department of Health & Human Services (HHS), the presence of ransomware or any other form of malware on a covered entity's computer system is a security incident under the HIPAA Security

> **Employees should not be allowed to plug in their cell phones into a computer because ransomware can spread over cell phones as well.**

Rule. A security incident is defined as "the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." According to 45 C.F.R. 164.308(a)(6), once detected, we must initiate security incident and response and reporting procedures. If you are reading this and you don't know what those are, I encourage you strongly to coordinate with your IT department or vendor to insure your security protocols are in place. HHS has created a Frequently Asked Question (FAQ) entitled Ransomware and HIPAA available at www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf which may also be helpful.

HIPAA requires us to take steps to safeguard our data from ransomware attacks. This includes the development and implementation of reasonable security incident procedures and response & reporting procedures that are reasonable to the individual entity. There is no one-size-fits-all solution and I would encourage you to work closely with your IT firm or department during this process.

INTERNET USAGE POLICY

Review your internet usage policy. If you don't have one create one. This policy should clearly outline internet access rules for your practice as well as other forms of communications such as e-mail, social media, and cell phone usage. Your policy should clearly state employees are only allowed to access the internet to do those things necessary to do their jobs.

Checking personal e-mails is not typically necessary to conduct your job. If you use social media or want to allow your employees to access the internet for non-job-related functions, provide a separate computer that does not connect to your billing or medical record servers in any way. And, yes, this applies to everyone in the office, including the physicians, nurses, and mid-level providers.

Cell phones are prevalent in today's society. Employees should not be allowed to plug in their cell phones into a computer because ransomware can spread over cell phones as well. Nor should users ever be permitted to use personal removable media (thumb drives). This is not

unique to ransomware; HIPAA has frowned on this practice for some time but it is a great time to reinforce your policies on these two issues.

Once you have a solid policy in place, have every employee review the policy and sign to document both their understanding of the policy and their agreement to comply with this policy.

Sample policies may be found on the Forms tab in the Members' section of the ADA-M website.

Also update your HIPAA Security & Privacy procedures and policies to specifically address ransomware prevention and mitigation.

EMPLOYEE TRAINING

Having the best policies in the world is not enough if you don't train your employees.

Conduct a training with your employees specifically addressing ransomware, steps to prevent, and actions to take if attacked. Make sure to retain a copy of the sign-in sheet for the meeting as well as the training materials. Best practice is to have employees take a brief quiz answering questions about the training and retain those as part of your training documentation.

Other points of discussion during this training should include reinforcing the notion that you should only open e-mails you expect and to be suspicious of any unexpected e-mails containing attachments labeled "Invoice," "Resume," "Statement," and other things that appear to be legitimate. Hackers are smart. They have developed icons that lead you to believe they are sending you Word or Excel documents. Another misconception is that you have to be an administrator to be able to spread a virus or open a malicious document.

Provide guidance on what an employee should do if they identify a suspicious e-mail. Should they contact in-house IT or an outside firm? These e-mails are typically quarantined and destroyed by IT. If you have an anti-virus software, you may choose to run it if a potentially malicious e-mail has been identified. If you don't have an anti-virus program it may be a good investment. Also make sure you have adequate spam filtering on your e-mails.

The best advice though is to ask before opening. ▼

DATA SECURITY

Conduct a risk analysis to identify threats and vulnerabilities. If you use an outside source require a written report of findings. Then develop a written plan to mitigate or remediate any identified risks.

Develop a plan to mitigate damage if you are attacked. Who should be called? How do you reach them? (Don't forget to contact the FBI, the law enforcement agency who deals with ransomware attacks.) What is the scope of the incident: what systems, networks or applications are infected? Who initiated the attack? Where were you attacked? When were you attacked? What was done? Is the attack finished or on-going? And how did the attack occur – what tools and methods were used or what vulnerabilities were exploited?

Do multiple back-ups of your data. Most practices now back up to an off-site server farm or the cloud but consider backing up regularly to a removable device. Certain strains of ransomware can encrypt backups so you cannot restore backup files. In either case, be sure you are regularly testing your ability to restore backed up files to your server.

Explore the feasibility of encrypting your data if it is not already encrypted. This can be a costly proposition for some practices and HIPAA only requires practices to do what is reasonable for the size and type of practice. However, encryption can minimize the risk of a breach – whether through a ransomware attack or through theft or loss of equipment such as laptops. At what point do the costs outweigh the benefits?

Monitor your network activity to identify suspicious behavior and to address security problems early. If you employ an IT firm ask, and document, how they are monitoring your network. While this is not mandatory, it is good general business practice. Someone needs to mind the store!

If you are attacked, immediately contact your IT vendor or department and the FBI. As you continue to analyze the depth and breadth of the attack, you will determine whether or not protected health information was accessed. The existence of malware is a HIPAA Security breach by definition. If protected health information was accessed, this may be a violation of the Privacy rule depending on the facts and circumstances of the attack. HHS guidance on breaches and disclosures can be found at 45 C.F.R. 164.402 and 45 C.F.R. 160.103, respectively.

The threat of a ransomware attack is real. While there is no one-stop safeguard to prevent an attack, make sure you have made every reasonable effort to safeguard your network and your patients' protected health information. ■

Sources include: fbi.com, kpmg.com, hhs.gov

DERMATOLOGY IN THE DIGITAL AGE:

PATIENT PERCEPTION AND SATISFACTION

By **Virginia King-Barker**
Senior Administrator
Duke University Medical Center

THE SLR DIGITAL CAMERA IN CLINIC IS BECOMING LESS PREVALENT AS SMARTPHONES AND ELECTRONIC PADS ARE INCORPORATED INTO OUR IMAGE CAPTURE PROCESSES. Whether a private practice with one physician or an academic department with 10+ providers and subspecialties, proactive management and ongoing monitoring of your digital imaging process and image storage is critical to mitigating HIPAA risk. Transparency with your policy and communicating your process with your patients can improve patient satisfaction.

OVER 30% OF DERMATOLOGISTS POLLED IN THE NORTHEAST REPORTED THAT THEY STORED PATIENT IMAGES ON THEIR PERSONAL SMARTPHONES AND 48% OF THAT GROUP HAD UNENCRYPTED STORAGE.

In a recent JAAD article[1] that addressed this topic, over 30% (27 out of 90) of dermatologists polled in the Northeast (Philadelphia and surrounding areas) reported that they stored patient images on their personal smartphones and 48% of that group had unencrypted storage. The respondents were asked about patient consent of image taking and storage, and 76% of dermatologists obtained patient consent, 69% of which were written consent and 31% verbal consent. HIPAA security rules for storage of PHI prohibit this lack of control over access to and storage of the digital images.[2]

In addition to HIPAA Privacy and Security Rule violations, patients are not comfortable with their doctor using their personal smartphone during the encounter.

The shift from "professional" equipment to personal smartphone has also been noted in a 2015 study[3] that 97.7% of patients (n=300) from a cross-sectional survey of adult patients in academic and private practice setting preferred the "hospital" or clinic based equipment to a personal device for taking photographs. The majority of the respondents reported that a smartphone is appropriate as reference tool, but not for image management. In light of the significance of patient reported satisfaction as it relates to value, patient perception is a factor in evaluating your image taking and storage processes in clinic. Patients will consider how professionally we manage their digital images, and perception can be affected by how the process is communicated and then carried out during the visit.

If your practice has not clearly outlined your data management and storage policy, there are steps you can take to protect your practice and your patients.

Using a personal smartphone may be convenient for the physician, but the clinic can implement a process to include providing a device (I-touch, Note tablets, a SLR digital camera) and maintaining or replacing it. Use of personal devices can lead to unexpected breach, i.e. accidental upload to a cloud storage service connected to the phone's service, or loss/theft of the smartphone. The tens to hundreds of thousands of dollars in fines, not to mention undermining patient confidence in your practice's ability to thoughtfully and legally manage the contents of their EMR is a reasonable trade-off for inconvenience. Financial and other legal considerations are also resolved- who owns the device, replaces it and the covers the cost of it, who owns the images. If you have Advanced Practice Providers and/or multi-provider practice, turnover can present challenges if you do not have established protocols in place to control digital images. In addition to providing the device, the clinic can confirm that all images have been transferred and the device has had data deleted. Performing this daily eliminates the potential for PHI breach.

Data devices and storage cards can be encrypted, adding an additional layer of protection to the PHI. The extra layer of security can be added peace of mind for the patient.

The conversation about digital imaging can begin during the intake process and culminate in providing a consent form that addresses the devices that are used, how the images are stored, how long they are stored, who has access to the images, and the purpose for which the images will be used.

"Dr. Jones will be using an I-touch to take photographs of your skin. These photographs will be transferred to our [secure electronic medical record/ secure server] so that we can refer to them during future appointments to determine if any changes have occurred since your last visit. These images are deleted from the device daily and we encrypt our devices to ensure additional security of the images. Dr. Jones and his coverage partner, Dr. Mercury, will have access to these images to use as a diagnostic tool to guide your care. We will maintain these images in your file for (your state/institutional/policy timeframe). Do you have any questions about our digital image procedure and management plan?"

***Academic institutions may use consent forms that allow images to be de-identified and used for clinical research.*

By standardizing the digital imaging policy and the process in your practice, you can successfully address HIPAA Privacy and Security compliance and improve the understanding and comfort level of your patients. Your attention to their concerns can impact their perception of their care, and of the satisfaction they have with your dermatology practice.

SOURCES

[1] Smartphones, photography, and security in dermatology. Anyanwu, Cynthia O. et al. Journal of the American Academy of Dermatology, Volume 72, Issue 1, 193 – 195

[2] HHS HIPAA Security Rule reference - http://www.hhs.gov/hipaa/for-professionals/security/laws- regulations/index.html

[3] Patient perception on the usage of smartphones for medical photography and for reference in dermatology. Hsieh C1, Yun D, Bhatia AC, Hsu JT, Ruiz de Luzuriaga AM. Dermatol Surg. 2015 Jan; 41(1): 149-54.

[3] HHS HIPAA Security Rule reference - http://www.hhs.gov/hipaa/for-professionals/security/laws- regulations/index.html.

A WORD TO THE WISE:

HOW TO USE ONLINE ADVERTISING FOR THE HEALTH CARE INDUSTRY

By **Paula Lynch**,
Google Certified Media Coordinator,
Market Mentors, LLC

FROM SEO TO PPC, DIGITAL MARKETING TERMS CAN LOOK LIKE ALPHABET SOUP TO THE UNTRAINED EYE. HOWEVER, SEARCH ENGINES ARE WHERE PEOPLE TURN FOR INFORMATION IN THIS DIGITAL AGE, INCLUDING WHERE TO GO FOR HEALTH CARE, SO IT IS IMPORTANT TO UNDERSTAND ONLINE ADVERTISING OPTIONS.

In fact, the Pew Research Center reported that 72 percent of internet users say they looked online for health information in the past year (based on the most recent survey). Furthermore, 77 percent of online health seekers say they began with a search engine – such as Google, Bing or Yahoo!. Just 2 percent said they started research at a more general site like Wikipedia – and only 1 percent say they turned to a social network, such as Facebook. That means people are more interested in the results a search engine returns than asking friends on social media, which is why digital advertising should be a part of any health care marketing strategy.

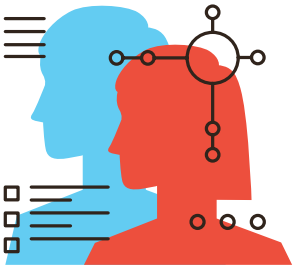
UNDERSTANDING SEARCH RESULTS

When someone enters a query into an online search engine two sets of results appear, advertisements and "organic" search results. The organic results are the list of the most relevant websites based on the search terms used. Ranking higher on that list can be achieved by search engine optimization (SEO). Depending on the search terms – or keywords someone uses to find information – it can be very difficult to propagate in the organic section because there is just so much information online. Furthermore, large health care organizations such as the Centers for Disease Control (CDC) or large governing bodies may be more highly rated by the search engine for relevance, therefore their results would appear before a smaller health care practice. The good news is that digital advertising can help ensure a brand or company appears on that first page of search results – the best real estate online. One of the most effective ways to advertise on search engines is to use pay-per-click (PPC) advertising.

"ONE OF THE MOST EFFECTIVE WAYS TO ADVERTISE ON SEARCH ENGINES IS TO USE PAY-PER-CLICK (PPC) ADVERTISING."

ADWORDS

While it might look like a typo to a non-marketer, AdWords is a branded process of PPC advertising used on Google and Bing (note that other search engines like Yahoo! have PPC platforms as well). Whether practice administrators are looking to attract new website visitors, grow online sales, get the phone ringing or keep customers coming back for more, AdWords is a solution. Using AdWords, a company can strategize when an ad should appear based on the keywords entered into a search. The best part is that this marketing initiative is budget friendly – a business can set a budget for advertising and only pay when people click the ads. **Here are a few best practices for using AdWords:**



THINK LIKE A CUSTOMER WHEN CHOOSING KEYWORDS. Avoid industry jargon that the "average Joe" wouldn't know. While it's probably spot-on for relevance, if the average person doesn't know what it is they won't think to put it in the search box… which means the ad won't show up. Instead, think about what people might search for – and define the list of keywords from that brainstorming process.

KEYWORDS SHOULD MATCH WEBSITE CONTENT. Not only should keywords be those that the average person should know, they should also be featured on the website for the company. If someone finds the content on an ad relevant enough to click on, they will want to see related content on the webpage the ad directed them to view. For the best results, keywords should be chosen from those used to develop website content and identified during the search engine optimization process.

CONSIDER GEO-TARGETING. AdWords helps businesses choose a target audience based on geography. It wouldn't benefit a Los Angeles-based health care provider if a patient in Atlanta clicked on the ad. AdWords make it easier to narrow in on the target audience by providing filters that let a company set a geographic region for a campaign. That means that only those people who are in the region specified will see the ad – or click on it, which is how a company is charged for the advertisement.

BUDGET AND MONITOR TO CHANGE BASED ON WHAT IS AND ISN'T WORKING. AdWord campaigns are budget friendly because a company is only charged when someone clicks on the ad – not when they see it but don't click. When someone sees the ad but doesn't click, it's called an "impression." Google provides data so a company can see if the campaign is generating results – by identifying click-through rates and impressions. If a campaign is working well, there will be a higher click-through rate – the number of people who click on the ad divided by the number of impressions. If a campaign isn't working well, the number of impressions will be high and the number of clicks will be low. At any time, that data can be monitored and changes can be made to the campaign accordingly. A company will never be charged more than what they budgeted – the ad will simply no longer appear as an option for users who enter common search terms if the budget is maxed-out. However… that's a great problem to have! For that instance, a company may want to increase the spend because the ad is generating a lot of interest.

CREATE A CALL TO ACTION. While the data provided by Google is a useful tool that shows how many times people click on an ad, the real value comes when someone books an appointment, buys a product or provides contact information for a company to follow-up. When someone takes action based on an ad, that's called a "conversion." Consider what

ADVERTISING COSTS MONEY, BUT IF DONE EFFECTIVELY IT SHOULD GENERATE MORE THAN IT COSTS.

end result, or conversion, is most desirable and create a call to action on the webpage the ad pushes people to view. From contact forms where people fill out a name, phone number and email address to online scheduling for booking appointments, there are many ways to capitalize on when someone clicks on an ad that will benefit a company's bottom line. After all, advertising costs money, but if done effectively it should generate more than it costs.

"GOOGLE-CERTIFIED PARTNERS HAVE A PROVEN UNDERSTANDING OF THE PLATFORM THAT GOES BEYOND BEST PRACTICES FOR THE BEST RETURN ON INVESTMENT."

EXPERTISE MATTERS

Just like health care credentials such as board-certification, Google has a training process to help generate the best results. Google-certified partners have a proven understanding of the platform that goes beyond best practices for the best return on investment. Not only does a Google preferred partner understand the platform better – but they are likely to drive better results because partners have passed tests administered by Google to assess skill and expertise. Consider challenging someone to earn the Google certification (or work with a partner that has already earned the distinction). ■

INFECTION CONTROL DO'S AND DON'TS

To see if you are compliant with the Do's & Don'ts of Infection Control, review the list below.

FOLLOW PROPER PROCEDURES

If you understand just what might/can happen when your office does not follow proper infection control policies, it will make a huge difference in the functioning of your work place.

REVIEW & UP-DATE

Always review and up-date guidelines and documentation on a day-to-day basis. This will help with the effectiveness and public health recommendations.

STANDARDS OF PRACTICE FOR ALL

All those who work in a medical facility need to be practicing infection control. Doing this means: You are practicing OSHA blood borne pathogen standards

TB & ECP (TUBERCULOSIS & EXPOSURE CONTROL PLAN)

- Use standard precautions for **ALL** patient care
- Strictly maintain environmental infection prevention practices
- Track employee illnesses.

ENVIRONMENTAL PROTECTION

When educating employees on infection control preventive measures, do not overlook: standard precautions, barrier precautions, and transmission and monitoring. Close attention should be paid to all these things.

Observe these practices:

- Hand washing
- Employee health
- Patient infections
- Reasons for standard precautions
- TB & other infectious diseases
- Staff evaluation.

Employees can spread germs to others even if they only have the common cold. This, by itself, is contagious through droplets and contaminated hands. Those who may have cold sores should avoid touching their faces. Not all cold sores are dry lesions, so they need to be kept covered.

Shingles can be transmitted from one to another. If a health care worker has shingles, the risk of transmission will be less if the health care worker covers any lesions.

Taking proper prevention measures in the workplace is a **MUST**. Designate people to be responsible for cleaning and disinfecting the environment and equipment in the facility. This will make a huge impact in the facility's operation. Facilities should use an EPA registered disinfectant, and all products should be reviewed periodically because they can change and it is imperative to know that the products that are being used will kill all bacteria.

Cleaning and disinfecting any patient care areas, after each use, is of extreme importance. Concentrate on the areas that are used, surfaces that are touched (by patients and workers), exam tables, blood pressure cuffs, stethoscopes, chairs, otoscopes, door knobs as well as counters.

One of the best ways to know what a patient might touch is to pretend to be one and then walk through your facility. Once you realize how and where bacteria can/might be, you will have a better understanding of how to keep *"Mr. Nasty"* out of the work place.

IMPORTANT SUGGESTIONS

Always wear PPE (personal protective equipment) when dealing with patients and when cleaning patient areas. The Infection Control Guidelines listed below will help to keep your facility compliant.

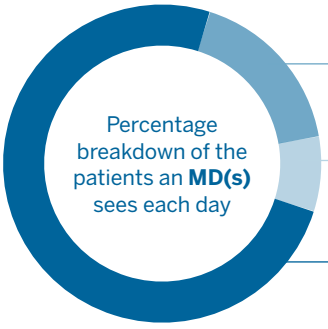
- Infection control risk assessment
- Understand your risk factors
- Geographic location & community population being serviced
- Occupational health related infections
- Environmental/patient equipment
- Areas for hand washing/or alternative forms of same
- Understanding roles & responsibilities

ALWAYS REMEMBER:

Educating the staff on infection control leads to a better understanding of what to do, and it promotes a cleaner facility for all.

By **Mandy E. Martin, RPSGT**
Compliance Consultant
MedSafe: The Total Compliance Solution

PATIENT VOLUME SURVEY RESULTS

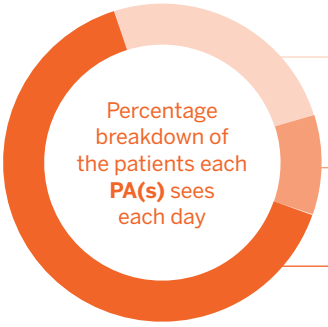


Percentage breakdown of the patients an **MD(s)** sees each day

19% New Patients

11% Surgical Patients

70% Returning Patients

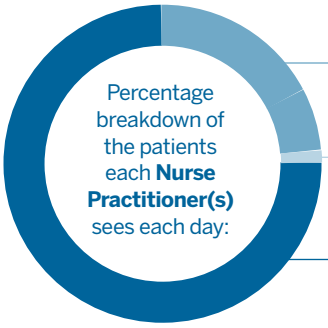


Percentage breakdown of the patients each **PA(s)** sees each day

26% New Patients

11% Surgical Patients

63% Returning Patients

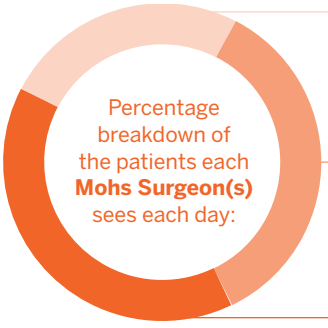


Percentage breakdown of the patients each **Nurse Practitioner(s)** sees each day:

29% New Patients

1% Surgical Patients

70% Returning Patients



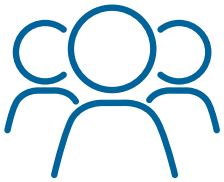
Percentage breakdown of the patients each **Mohs Surgeon(s)** sees each day:

22% New Patients

39% Surgical Patients

39% Returning Patients

Average **number of patients** each of the below see per day



MD 43

PA 27

Nurse Practitioner 14

MOHS Surgeon 8

Average **number of hours** each of the below sees each day

MD | 7.5 hours

PA | 6.5 hours

Nurse Practitioner | 4 hours

Mohs Surgery | 5 hours

Does your practice use **paper** or **electronic** charts?

15% **VS.** **85%**

ASK THE EXPERT Q&A

with Bob McKown, President, XMi Human Resources Solutions

QUESTION: We are a company with less than 50 employees in Indiana. We have an employee who's pregnant and keeps mentioning that she'll be "disabled" when she has her baby. She came to us from a large hospital system, and has been with us for over a year. Because she is a part-time employee (she works about 30-32 hours/week) and does not have any paid time off, how would her claim of disability affect us?

ANSWER: This is a common yet complex situation because there are multiple laws related to leave and disability. The quick response…it is possible that under Americans with Disabilities Act Amendments Act of 2008 (ADDAA) there could be circumstances that would make pregnancy a disability.

The longer answer…Often times, state laws are more generous than federal laws. When evaluating these requests, employers must look at their past practices, but really the best place to start is your employee handbook or other policies regarding leave. If you have policies does this individual fall into any of your existing leave policies? If so, she may be eligible for temporary leave under current policies regardless of part-time status and lack of paid time off.

If you don't have a policy, begin by exploring leave laws on your local and state level. You should always comply with the law that provides the most benefit to the employee. In this particular instance, Indiana does not have any specific laws governing leave for private employers, so a review of federal leave laws will follow. Since you have less than 50 employees you would not be covered by the Family Medical Leave Act of 1993 (FMLA).

As I mentioned above, pregnancy is sometimes considered a disability under the Federal ADAAA, but not always. When an employee requests leave or additional leave for a medical condition or disability, employers must provide reasonable accommodation for the request

Under PDA, an employer may not single out pregnancy-related conditions for special procedures or medical documentation to determine a woman's ability to work, and **employers must also hold a job open for a pregnancy-related absence** the same length of time they would hold a job open for employees on sick or disability leave.

unless doing so would impose an undue hardship on the company. This is the case even when the employer does not offer unpaid leave or disability leave, the employee is not eligible for FMLA or for the employer's leave policy, or any paid leave has already been exhausted. To be protected by ADAAA, an individual must have a qualified disability and be qualified to perform the essential functions of the job, with or without a reasonable accommodation by the employer. Pregnancy alone and temporary disability resulting from a normal childbirth is not considered a qualified disability and is not protected by ADAAA. However, a woman experiencing high-risk pregnancy complications or having additional impairments resulting from pregnancy may be covered.

Absent undue hardship on the employer, you may have to provide ADAAA reasonable accommodations for a disability related to pregnancy, but accommodations are made on a case-by-case basis because the nature and extent of a disability and the requirements of a job will vary from employer to employer and even job to job.

The Federal Pregnancy Discrimination Act of 1978 (PDA) also comes into play here because it covers employers with 15 or more employees. It states that any woman affected by current or past pregnancy, childbirth or related medical conditions shall be treated the same as other employees for all employment-related purposes. Any benefit a company would give to a non-pregnant and disabled employee must also be given to a pregnant one. Under PDA, an employer may not single out pregnancy-related conditions for special procedures or medical documentation to determine a woman's ability to work, and employers must also hold a job open for a pregnancy-related absence the same length of time they would hold a job open for employees on sick or disability leave. In addition, employers may not force a current or previously pregnant employee to take leave; she must be permitted to work as long as she able to perform her job. If an employee has been absent from work as a result of a pregnancy-related condition and then recovers, her employer may not require her to remain on leave until the baby's birth, nor may an employer prohibit an employee from returning to work for a certain length of time after childbirth.

Every situation is different and there are multiple laws and regulations that you must be sure you consider. Please remember, this is answer is not meant to replace legal advice and only highlights concerns from a human resource perspective. ■

ASK THE LAWYER Q&A

with Michael J. Sacopulos, JD,
Medical Risk Institute

THE ENEMY WITHIN

QUESTION: With social media playing a big part of everyone's daily life, we have found a staff member had posted negative comments/posts about the office and referenced her direct supervisor (but never gave names). It is my understanding that the employee can post anything they want and are protected as it is freedom of speech. However, can you legally reprimand them with a counselling or written warning for office negativity or hostility towards the work environment?

ANSWER: Sadly, it is not as difficult to believe that an employee would post negative comments about his or her employer as it used to be. Whether this is a generational habit or general shifting of the workplace cultural, I cannot say. What I can tell you is that the employer has legal rights too. First, let's dispel with the freedom of speech. The 1st Amendment protects an individual from the government interfering with his or her speech. The 1st Amendment does not protect an individual from his or her fellow citizens or employer. The notion that the 1st Amendment will protect a people from the natural consequences of voicing their idiocy is wrong.

In many situations an employer would be within his or her legal rights to immediately terminate an employee for the type of comments and posts you describe in your question. This is the place to start. The general presumption is that you can terminate the employee for negative online comments about supervisors or the practice. From there we begin to look at specific exceptions.

When and where the employee created the negative post makes a difference in some states. Certain states prohibit an employer from disciplining and employee for action done on their own time (so long as those actions are legal). In these states, an employee could not be terminated or disciplined for posting negative comments about his or her employer if the post was written outside of the workday.

The National Labor Relations Act sets forth rules which protect communication between employees about the terms and nature of their employment. So the National Labor Relations Act may be called into question based upon the wording the posts or comments. For example, if a group of employees

post comments criticizing management or general working condition at the practice, this could be found to be protected activity for which the group of employees could not be disciplined or terminated.

A few states protect political speech of employees. In these states, an employee cannot be disciplined or terminated for an expression of his or her political beliefs. If the post said, "Dr. Jones is a complete clown for supporting Frank Smith for School Board. What Boneheads!" the employee could not be disciplined or terminated in these states.

Most negative posts by employee can result in the employee being disciplined or terminated. Any type of comment about of a physician's lack of medical skill or knowledge may result in an immediate termination. For example, if my employee says "I feel sorry for Sacopulos' clients. He does not know the first thing about practicing law. Further, he wears some wicked ugly ties." I could immediate terminate my employee for posting such comments.

If all this makes you a little nervous, it may be worth consulting an employment law attorney. States' employment laws vary and some of Federal law can be confusing when it comes to this topic. You might want to consult an employment law attorney before you show that hostile employee the door. I wish you great success and safety when dealing with your disgruntled employee.

Association of Dermatology
Administrators & Managers

1120 G Street, NW, Suite 1000
Washington, DC 20005

phone: 866.480.3573 | fax: 800.671.3763
adaminfo@shcare.net

ada-m.org

MISSION

Serving the dermatology profession through education, resources and networking opportunities.

VISION

The trusted resource for dermatology practice management.