## Cyber Security for Dental Practices... continued from page 1

The Health Insurance Portability and Accountability Act requires healthcare providers to maintain the privacy of patient health information and to take security measures to protect this information from abuse by staff members, hackers and thieves. The penalties imposed upon health care providers for HIPAA violations are great. The monetary penalties can range from a fine of $100 to a fine of $50,000 per violation, with a $1,500,000 maximum annual penalty. In addition to the federal penalties, dentists may face penalties imposed at the state level as well as lawsuits filed by disgruntled patients whose health information has been compromised.

It is crucial for dentists to take steps to ensure that their practice is in compliance with HIPAA provisions regarding computer security. Because the majority of data security breaches occur when staff members fail to follow office procedures or exercise poor judgment, the location of computers in the dental office is key. All computers should be placed in areas where the computer screens are not visible to patients and visitors, and encrypted passwords should protect access to each computer. Passwords should contain mixed case letters and include numbers or symbols and should be changed regularly. In addition, passwords should not be written down under keyboards or kept on desks or surfaces where the public may be able to access them. Dentists should ensure that all staff members understand the importance of maintaining the privacy of patient health information.

Every dental practice should have a policy that includes steps for safeguarding patient information and educate staff members as to how to comply with the office policy. A strict Internet and computer use policy should be enforced that prohibits staff members from checking personal e-mail accounts or visiting Internet sites that aren't work-related. It is also important that dentists ensure that all firewalls, operating systems, hardware and software devices are up to date, strong and secure and that wireless networks are shielded from public view. Antivirus software should be installed on every computer, kept updated, and checked regularly.

When accessing office data remotely, dentists should use only trusted Wi-Fi hot spots and never use shared computers. Smartphones and tablets should be password protected to prevent easy access to patient information in case the device is lost or stolen. In addition, all hard copies of documents with patient information should be shredded. Finally, to ensure that your dental practice is HIPAA compliant, data transmitted to payers, health plans, labs and other healthcare providers may need to be encrypted to ensure that a hacker will not have access to this data.

Because dental practices are subject to heightened government enforcement and the scope of fines and penalties for data breaches have increased, many dental practices have relied on cyber insurance for protection in the event of a breach of cyber security. These insurance policies cover the cost of investigating a theft, compensate the insured for all state and federal fines and penalties imposed, and fund all related lawsuits and legal fees, thus relieving dentists of the financial and time burdens imposed as a result of the breach in security.

It would be prudent for all dentists to invest in data security and in the proper training of staff members as to acceptable use of office computers. If plans and policies are put in place proactively and steps are followed to ensure HIPAA security compliance, a dental practice should be able to prevent the significant cost and headache involved in responding to a cyber-breach.

If a security breach in a dental office does occur, it is imperative that appropriate action is taken immediately, which includes determining how the breach occurred, and the extent of the security breach. In addition, if a security breach does occur, the owner of a dental practice must be very careful whom they initially contact and provide information to. Any improper or accidental disclosure to a third-party other than legal counsel for the dental practice owner may be subject to the rules of discovery if litigation occurs, which could increase the liability exposure of the practice owner.

---

*Stuart J. Oberman, Esq. handles a wide range of legal issues for the dental profession including cyber security breaches, employment law, practice sales, OSHA, HIPAA compliance, real estate transactions, lease agreements, noncompete agreements, dental board complaints, and professional corporations.*

*For questions or comments regarding this article, please call (770) 554-1400 or visit www.obermanlaw.com.*

---

[1][2][3][4]*Articles reprinted with permission from Excellence In Dentistry, LLC (1-800-337-8467), publisher of The Profitable Dentist® Newsletter (www.theprofitabledentist.com).*



## Secrets to Coach Your Team to be Telephone Winners!

*by Chris Mullins[2]*

1. Teach your team how to focus on one call at time. Visualizing is a great tool for staying focused on the next call. Think about "Mary," the next prospect in line to call. What does she look like; how can you be of service to Mary?
2. Create a voice message script. Create an outline for the messages your team members will leave. Again, hold them accountable for using the script.
3. Provide headsets that work for your team members. It's faster and easier for them to navigate, and it cuts down on fatigue
4. Observe your team members as they make and take calls. Listen carefully to the tone of voice. How are they doing, really? Watch their body language. Should they be in this position? Do they need a break? Do they need water?
5. Teach your team to use good listening techniques by paying attention to the tone, the voice and the breathing of the patients, as well as the background noise.
6. Teach your team to keep detailed notes on each call, especially documenting the exact language and vocabulary of your prospects. Remember that without the telephone, you're out of business. Pay close attention to how your phone (leads you paid for) is being answered and monitor those calls to be sure you're capturing all sales opportunities. Give your team all the important ongoing coaching, training and information they need to be successful. Set them up to win, not fail.
7. Decide that the First Impressions Director (front desk, reception position), is critically important to your business. Rollout the red carpet! Stop dealing with turnover. Sell with integrity.
8. Monitor all team members that use the phone, chat, text, email, fax, etc. You must Inspect What You Expect™. However, you must go at this from a positive point of view. Share with your team that the purpose of monitoring calls is to identify all the great things they do so you can repeat them and all the areas that need to be tweaked fast. This technique is the quickest way you can grow your business.
9. Teach self-critiquing. Your team members should know how to critique their own calls and then provide you with feedback.
10. Implement a bonus plan (commission works best) that promotes more business for your practice, which will make even more money for your team members.
11. Have fun! Don't give up! You can do this!

---

*Chris Mullins (aka The REAL Phone Sales Doctor) is president and founder of Mullins Media Group TM, a communications and consulting firm for dental practices.*

## MARKET YOUR PRACTICE FROM THE INSIDE–*OUT*

*by Mary Fisher-Day[3]*

**Marketing from the inside-out is the most effective and inexpensive way to get new patients. Patient referrals are key. The key to keeping the patients you have and have them refer their friends, family and coworkers is letting them know you appreciate them. Below is a list of the 12 things you can do TODAY to market your practice at little or no expense.**

- Thank your patients for coming in and tell them it was good to see them. This is will go very far when a patient is trying to decide between you and another dentist.
- *Your patient waiting area should be inviting and peaceful.*
- Make every effort to see your patients at their appointed time. If they have to wait, they will be agitated by the time you see them. If you must make them wait, apologize.
- *Look patients eye to eye when speaking. This will create a bond and build trust.*
- Never make a patient feel stupid for asking questions. Make sure your team follows this rule as well.
- *When having a casual discussion with a team member in the presence of a patient, always include the patient in your conversation.*
- Your patients' time is important too. If you can save them a trip by doing one extra procedure, do it... it's more cost effective for everyone involved.
- *Treat every patient the way you want to be treated. When you're with them, give them your undivided attention. They should feel like the most important person in your office.*
- Ask your team to abstain from wearing perfume. Many people are allergic and they won't say anything about it... they just won't come back.
- *Patients should see that your team respects you and their co-workers. If they see tension of any kind, they may not come back and certainly won't refer friends and family to you.*
- Having nicely framed posters in treatment rooms is an inexpensive way to promote your services. Display posters of services available in your practice. i.e.: Invisalign™, 6 Month Smiles, implants and implant restoration, whitening services, specific cosmetic procedures and materials, same day crowns, oral cancer screening, etc.
- *My favorite and number one tip for inexpensive and yet, very effective, marketing is: Make your own post op phone calls and give your patients the unexpected. This will go further than you can imagine and will tell everyone they know about you.*

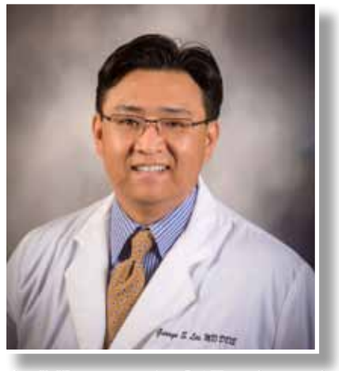
---

*Mary graduated with honors from Florence-Darlington College and continued her education by studying Business Management at Limestone College. In 2002, she started The Dental Business and continued her work as a practice management consultant and coach guiding her clients to quick results. Mary can be reached at mary@thedentalbusiness.com*

ISSUE 26
OCTOBER / NOVEMBER 2017

2285 RUDOLPHTOWN RD, SUITE 200 • CLARKSVILLE, TN 37043
P: 931-552-3292 • F: 931-552-3243
WWW.CUMBERLANDSURGICALARTS.COM

# CUMBERLAND
SURGICAL ARTS, PLLC
GEORGE S LEE, MD, DDS
MATTHEW A DEFELICE, DDS



## FROM THE DESK OF GEORGE S. LEE, MD, DDS:

### BLEEDING RATE DURING ORAL SURGERY OF ORAL ANTICOAGULANT THERAPY PATIENTS WITH ASSOCIATED SYSTEMIC PATHOLOGIC ENTITIES*

Oral anticoagulant therapy (OAT) patients have international normalized ratio (INR) safety windows for oral surgery, the lower limit of which is determined by the thromboembolic risk, with the upper limit typically 3.0. The authors sought to assess whether these limits will also be true with comorbidities that favor bleeding, such as diabetes, liver disease, and chronic renal failure. The study was designed for 500 consecutive extractions. Patients with an INR greater than 3.0 were switched to heparin and used as controls. The primary outcome was the incidence of bleeding with the need for reoperation, in connection with 3 principal predictors: the INR, reasons for OAT, and comorbidity type. Continuous variables were analyzed using appropriate statistical analysis. The reliability of the INR as a bleeding predictor was assessed using receiver operating characteristic (ROC) curves.

Extractions in patients receiving OAT without comorbidities had a success rate of 99.7% against severe bleeding. Despite equivalent INR values, patients with comorbidities had a significantly lower rate (81.3%). For these patients, the ROC curve procedure indicated lower INR upper limits, 2.8 for mechanical heart prosthesis subjects and 2.3 for all others. Among the comorbidities, diabetes was associated with the greatest frequency of bleeding (31%) compared with liver disease (15%) and kidney failure (11%). Patients with comorbidities should be advised to bring their INR within narrower safety windows (upper limit of 2.5 to 2.8 for mechanical prosthesis and 2.0 to 2.3 otherwise) or be switched to heparin. Alternatively, the authors proposed applying to the socket, a platelet-rich growth factor preparation to foster hemostasis.

### 5 OR 5 CAMPAIGN

This year we would like to invite your office to participate in our 5 or 5 Giving Back Campaign. We are collecting shelf stable food, personal items, and monetary donations for Urban Ministries. Donations are key to the success of this ministry and I hope your office will join us in this effort. We are challenging each office to collect at least $5 or 5 food/personal items from each team member.

The challenge will start on Monday, October 21st, and run through Monday, November 20th. We will pick up all items on the week of November 20th to deliver to Urban Ministries. Acceptable items include shelf-stable foods, such as canned goods and boxed foods, personal hygiene items, and baby supplies such as diapers and wipes. If your office is limited on space, we would be more than happy to pick up items as your box fills up.

**The office with the most points per team member receives a catered lunch on us!**

- Each dollar will be 1 point.
- Each food/personal supply item will be 1 point.

We want to make this challenge fair for offices of all sizes. The winner will be based on an average that accounts for the number of team members. We will average the points per person in the office. For example, an office of 4 employees turns in 15 items and $5 = 20 points all together. Then an office with 10 employees turns in 20 items and $10 = 30 points all together. By averaging the offices, the office with 4 employees would win because they averaged 5 items per person (20/4), where as the office of 10 employee's averaged 3 items per person (30/10). To register your office, call Christy at 931-552-3292 or email at cdenote@cumberlandsurgicalarts.com.

** Cocero N, Mozzati M, et al. J Oral Maxillofac Surg. 2014 May;72(5):858-67*

## Cyber Security for Dental Practices

*by Stuart J. Oberman, Esq.*[1]

The provision of health care is changing at a rapid pace as healthcare providers endeavor to maintain maximum efficiency while navigating the technology rich climate. As a result of the reliance on electronic data, dental offices have become vulnerable to cyber security threats. The growing volume and sophistication of cyber-attacks suggest that dental practices will have to grow increasingly vigilant to ward off these threats. A breach of cyber security will inevitably lead to significant expenses, both financial and reputational, which can wreak havoc on a dental practice.

Many dentists believe that cyber criminals are not a threat to their small dental offices. However, when choosing between a large corporation or bank with security teams and firewalls preventing access to databases and a dental office with no firewall or security team, the dental practice will be the chosen target. In fact, many hackers specifically target small dental offices because they believe that small businesses may not have the resources for sophisticated security devices and do not enforce employee security policies.

Dental practices are an increasing target for cyber criminals. These offices hold a vast amount of data, including names, health history, addresses, birth dates, social security numbers, and even banking information of hundreds, if not thousands, of patients. The threat of this information being stolen by a staff member or a cyber-criminal is great, and dental practice owners must address this concern before a theft creates a legal nightmare for the dental practice.

Healthcare organizations make up roughly 33% of all data security breaches across all industries and the healthcare industry is the most breached industry in the United States. According to the US Department of Health and Human Services, almost 21,000,000 health records have been compromised since September 2009. It has been shown that human error causes the majority of personal health information data breaches and that actions of health care employees cause 3 times as many breaches as external attacks.

The most common causes of data breaches in health care organizations are theft, hacking, unauthorized access or disclosure, lost records and devices and improper disposal of records. A significant proportion of healthcare breaches are a result of lost or stolen mobile devices, tablets and laptops. In addition, security breaches are not solely inflicted upon the large HMOs, as more than half of all organizations that suffer from security breaches have fewer than 1,000 employees.

**Continued on page 2**