MLMIC
MLMIC Insurance Company
a Berkshire Hathaway company

THE SCOPE

DENTAL EDITION

NY

ISSUE 04 | SECOND QUARTER 2021

INSIDE

EXECUTIVE MESSAGE

To Our MLMIC Insurance Company Policyholders:

Spring is in the air, baseball is back, and more and more people are out and about now that mask restrictions have been eased by the federal government. With increased access to the COVID-19 vaccines, New Yorkers have reason to be cautiously optimistic that we will be able to celebrate the 4th of July and enjoy the warm summer months and outdoors, with family and friends.

Imagine waking up to the fact that the dental records for all of your patients are now inaccessible … and being held for ransom! What would you do? Please give FAKS attorney William Hassett's article a careful read and think about the ramifications to your practice if this were to happen. And then consider, am I doing all that I can do to protect both my patients and practice?

On occasion, an individual dentist's rise to prominence warrants recognition in *The Scope*. Dr. Chad Gehani is one such individual: a renowned dental practitioner and leader, distinguished both throughout New York State and nationally, who exemplifies the American success story. His skill, professionalism, and drive led him to the peak of his profession, and it is through this success that he seeks to influence future classes of young dentists. MLMIC is pleased to feature him on these pages.

Should you know of any other such individual who you feel should be recognized by his or her peers for outstanding service or professionalism, or perhaps another distinguishing quality, please do not hesitate to submit his or her name to *The Scope's* Editorial Committee.

Enjoy the warm weather!

John W. Lombardo, MD, FACS
Chief Medical Officer, MLMIC Insurance Company
jlombardo@mlmic.com

Fager Amsler Keller & Schoppmann, LLP

Ransomware: A 21st Century Threat to Dental Practices

Ransomware is the fastest-growing cybercrime in the United States, and attackers are becoming more sophisticated in their methods and diversified in their scope of targets.

The Federal Bureau of Investigation reports that over 4,000 ransomware attacks occur daily, with victims ranging from home users to governmental entities and various sectors of private business.[1]

In recent years, healthcare providers, including dental practices, have become the primary target for ransomware attackers as patient records are a treasure trove of valuable, privileged information. Unlike other business sectors, where such attacks can be a temporary annoyance, dentists and other healthcare providers are uniquely affected by these attacks as they can present an immediate risk to patient safety, cripple day-to-day operations, and severely impact a provider's reputation. Below is an overview of the risks presented by ransomware to dental practices, and recommendations to minimize susceptibility to an attack.

What Is Ransomware and How Is It a Threat to Dental Practices?

Ransomware is a type of malicious software (malware) that is designed to block access to a computer or a network of computers until a sum of money is paid for its release. An attacker will deploy malicious software on devices or computer systems through spam (unsolicited emails), phishing messages (deceptive emails that appear official), and email attachments, or by direct installation, where an attacker has hacked into a system. Once attackers have gained access, they will remove all the data from the system or encrypt the data and demand payment in return for a key to decrypt the information.

There is no guarantee, of course, that the attackers will return the information to the victim after payment is made, or not utilize the mined data for nefarious purposes, even after access has been returned to the victim. The evolution of cryptocurrency like Bitcoin has enabled criminals to fully automate their ransomware attacks, thereby making the attackers highly efficient and very difficult to identify and track after a successful attack.

> **... 30 percent of ransomware attacks were made against businesses employing less than 100 employees.[2]**

The scope of ransomware attacks against healthcare providers can range from the extortion of millions of dollars from large health systems to squeezing several thousand dollars out of a small practice. In fact, studies have shown that 30 percent of ransomware attacks were made against businesses employing less than 100 employees. Attackers focus on smaller businesses as they present weak targets with less sophisticated security and data backup systems. And to avoid having to close down their business for an extended period of time, smaller businesses are also more inclined to pay a ransom to regain access to valuable information such as health records. Many smaller practices also rely heavily on third-party vendors for information technology (IT) services, including data backup and storage. Therefore, an attack on one vendor can simultaneously cripple hundreds, if not thousands, of small practices.

> **... over 400 dental practices nationwide lost access to patient charts, X-rays, and billing information.**

Two attacks that took place in 2019 highlight the vulnerability of dental practices to ransomware and the damage an attack can cause on practice operations. First, an attack against an IT provider, PerCSoft, encrypted the data it maintained in a remote backup service used by dental practices. As a result, over 400 dental practices nationwide lost access to patient charts, X-rays, and billing information. The IT vendor ultimately paid the ransom to obtain decryption from the attacker, but some dental practices were still unable to regain all patient data that was stolen.

Later that year, another IT company, Complete Technology Solutions, suffered a similar attack that impacted roughly 100 dental practices across several Western states. In that instance, the vendor elected not to pay the ransom and focused its resources on

1 "How to Protect Your Networks from Ransomware," https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf

2 "Small and Medium-Sized Practices Under Increased Pressure from Cyberattacks," Alder, Steve, HIPAA Journal, March 5, 2021, https://www.hipaajournal.com/small-and-medium-sized-practices-under-increased-pressure-from-cyberattacks/

decryption efforts, which again resulted in loss of data and extensive disruption to numerous dental practices until the data was recovered.

Ransomware Defense – HIPAA Compliance

The most effective way for a dental practice to safeguard against potential ransomware attacks is compliance with security measures outlined in the Health Insurance Portability and Accountability Act (HIPAA). As defined by HIPAA, covered entities[3] are required to develop and follow procedures that ensure the privacy and security of electronic protected health information (e-PHI) whenever it is transferred, received, or handled.[4]

The Security Rule, as a subpart of the HIPAA regulations, specifies that practices must implement reasonable and appropriate safeguards to ensure the confidentiality and integrity of e-PHI.[5] The Security Rule comprises three categories, called safeguards, that are aimed at protecting and securing e-PHI: administrative, physical, and technical.

> **Dental practices should implement strong password security with multifactor authentication ...**

Administrative safeguards require practices to implement policies and procedures to prevent, detect, contain, and correct security violations.[6] Dental practices should implement strong password security with multifactor authentication on all platforms that have access to patient information, and require that passwords are changed with regularity.

Existing practice security policies pertaining to employees and staff should also be reviewed and updated to ensure there are measures for employee training and education on ransomware, including the identification and reporting of any suspicious emails that could constitute a phishing attack.

Patient e-PHI that becomes encrypted as a result of a ransomware attack is also considered a breach or disclosure by HIPAA regulations. Therefore, any security policy must include the development of an incident response and remediation plan to address breaches, should they occur. The plan should specifically address the manner of notifying the affected patients and potentially the Department of Health and Human Services, as well as law enforcement and even the media, depending upon the nature and size of the breach.[7]

The Security Rule's **physical safeguards** also require practices to implement policies and procedures to limit physical access to its electronic information systems, including desktops, laptops, tablets, and smartphones.[8] Any devices that contain or access e-PHI should be locked with user password access only.

Practices should also consider disabling the USB ports on any devices that access, use, or exchange e-PHI. Ports are a prime source for the introduction of malware via devices such as thumb drives. They allow cyberattackers direct access to implement a ransomware attack.

Lastly, any portable devices with access to e-PHI should be stored after business hours in a locked physical location to prevent theft or unauthorized access.

Finally, the **technical safeguards** of the Security Rule require that practices implement policies and procedures for electronic information systems that allow access to e-PHI only to those persons or software programs that have been granted access.[9]

Practices should also maintain policies that stipulate software updates, including anti-malware applications, are to be regularly performed on office computers, tablets, and smartphones.

Procedures should also be in place for data backup and, when possible, dental practices should maintain multiple backup sets of data.

continued on page 13 ›

3 45 C.F.R. § 160.103 defines a covered entity to include a healthcare provider who transmits any health information in electronic form for billing or insurance purposes.
4 45 C.F.R. § 164.104
5 45 C.F.R. § 164.306
6 45 C.F.R. § 164.306
7 45 C.F.R. § 164.400-414
8 45 C.F.R. § 164.310
9 45 C.F.R. § 164.312

New Electronic Health Information Blocking Requirements

Under the 21st Century Cures Act

The Department of Health and Human Services Office of the National Coordinator of Health Information Technology's (ONC) Final Rule on electronic health record interoperability and electronic health information blocking provisions contained in the 21st Century Cures Act took effect on April 5, 2021.

The Cures Act broadly defines "information blocking" as "a practice that – except as required by law or covered by an exception ... is likely to interfere with access, exchange, or use of electronic health information."

With 95% of hospitals and over 85% of office-based practices using electronic health records, the information-blocking provisions of the Cures Act will have a direct impact on nearly all healthcare providers.

FAKS attorney William P. Hassett has prepared an overview of the information-blocking provisions of the Cures Act that includes how it applies to healthcare providers. Topics addressed include:

- The Access, Exchange, and Use of Electronic Health Information
- Information Blocking
- Exceptions Where Information Blocking Is Permitted
- Enforcement and Penalties
- Considerations for Compliance with the Cures Act Information Blocking Provision

Click here to read the article on this important act's full impact on New York healthcare providers.

FULL CIRCLE WITH

Dr. Chad Gehani: From Mumbai to Queens

From time to time The Scope: Dental Edition *will highlight an outstanding individual in the dental community. The subject of our inaugural piece is none other than Dr. Chad Gehani.*

From humble beginnings in Mumbai, India, to leadership roles at every level of organized dentistry, Dr. Chad Gehani is the epitome of a heartwarming success story and a man with a full personal and professional life.

Serving as president of the ADA through October 2020, Dr. Gehani led the charge to keep dentists apprised of ever-changing information as the COVID-19 pandemic took hold, and provided guidelines and strategies as dental practices began to reopen.

Prior to his tenure at the ADA, Dr. Gehani served as president of the Queens County Dental Society, trustee to the ADA Board of Trustees, delegate to the House of Delegates, and president of the New York State Dental Association. He is the recipient of numerous awards in recognition of service to his profession.

When his tenure as president of the ADA concluded, Dr. Gehani returned to his home base in Queens and to his next role in service of his profession and organized dentistry as the executive director of the Queens County Dental Society.

With such a distinguished career in organized dentistry, we could not help but ask Dr. Gehani to share some of his experiences, as well as his thoughts on why membership is important to both the individual dentist and the profession. MLMIC is pleased to share these with you.

Q: How does it feel to be back in your local society as its executive director?

Dr. Gehani: Home sweet home! I feel great coming back home. I worship work!

I know I can make a difference in organizing, developing leadership, and creating and building new relationships for the Queens County Dental Society.

Being executive director gives me an opportunity to remodel, reenergize, and revitalize the society – and help our dentist friends and welcome new members.

Q: What would you say to a dentist thinking about membership in organized dentistry?

Dr. Gehani: I am a member because we must have unity of our profession. United, we can conquer the world. There are many decisions being made by lawmakers every day that affect our profession, so that strength in numbers becomes critical in having our voices heard.

I tell nonmembers that, while all dentists benefit from the actions of the ADA, as members they can also be part of policymaking and have a voice. The benefits of membership are numerous; however, advocacy on behalf of our patients and our profession is of utmost importance.

Dentists must speak with a united voice if we want to secure our future – not only for us but for the generations to come!

Q: What are some of the challenges facing the profession and organized dentistry today?

Dr. Gehani: One aspect is consumerism. Our patients look upon us as the providers of a service. They look for convenience and cost-effectiveness. The days of hanging out your dentist shingle and patients coming to you by word of mouth are long gone. Web presence, longer hours for patient convenience, and cost-saving services are here to stay.

Organized dentistry must work tirelessly to remain relevant to dentists. We must make certain members and potential members see organized dentistry as the leader for resources, guidance, and support. We must provide members with easily accessible first-rate service utilizing the most up-to-date technology. We must work consistently to anticipate our members' needs. This is what I strive for.

Q: What are some tips for new dentists?

Dr. Gehani: New dentists should not only become members of organized dentistry, they MUST also get involved. Our future depends on it, and so does theirs. They must have a place at the table to have a voice in the future of their profession.

New dentists should consider working with good mentors who can guide them, much as I was guided by my mentor, Dr. Richard Mascola, in the early '80s.

Dentistry is regularly ranked by *U.S. News & World Report* as one of the best career choices.

I am proud to call myself a dentist and a member of the American Dental Association. Dentistry is a trusted profession whose services contribute greatly to our patients' general health and well-being. Above all, we can change a person's life forever by removing pain and giving them a beautiful smile!

Many dentists are also small-business owners. We take pride in serving our communities. And we are often our own boss. In short, dentistry provides many opportunities for professional satisfaction.

Q: What has been one of the greatest accomplishments in your career?

Dr. Gehani: My career has been full of successes. Every day is a blessed day for me. Never a bad day.

As president of the ADA, I was proud to bring my "servant leader" qualities to the role. I certainly did not anticipate becoming known as the pandemic president but was honored to serve the dental community – not only nationally but globally – during this unprecedented crisis. Our doors were open to guide dentists anywhere help was needed.

I was completely consumed with the challenge of managing an extraordinary situation that demanded answers and guidance in virtually unknown terrain. In addition to our 163,000 members, as well as nonmembers, here in the USA, dentists all over the world were looking to the ADA and its leadership to provide science-based facts about COVID-19 in real time under constantly changing circumstances. So, I am proud of what we were able to accomplish during this crisis in bringing necessary information and guidance to dentists and the public, while advocating for dentists as the essential workers we are!

Q: How do you spend your spare time when you are not practicing?

Dr. Gehani: I love my family and love spending time with them. My wife, Rekha, is an orthodontist and the real force of the Gehani family. I have three children – two orthodontists and one ENT surgeon – and six grandchildren. They are the world to me.

Reading religious books and reading about Mahatma Gandhi are great. Bicycling at home keeps me relaxed.

Thank you, Dr. Gehani, for sharing your time and insights with us!

Danielle Zimbardi is Vice President of Dental Underwriting for MLMIC Insurance Company.
dzimbardi@mlmic.com

CASE STUDY:

Poor Patient Relations and Prolonged Treatment Result in Large Settlement

Initial Treatment

A 52-year-old male presented to the MLMIC-insured orthodontist's office requesting treatment to make his teeth perfect. The orthodontist advised the patient that his bite could never be perfect due to a skeletal imbalance in which his upper jaw was narrow and behind the lower jaw. Treatment options of surgery versus orthodontics were discussed, as well as the risks and benefits of these treatments. The patient opted for orthodontics, but a written consent was not obtained.

The orthodontist's treatment plan consisted of the extraction of one tooth to relieve crowding, increasing the upper overjet, using lower 4's as 3's, and expanding the upper arch with wire. She placed upper and lower brackets that day.

> **... the patient frequently failed to keep appointments and often rescheduled.**

The patient was seen at least once a month by the orthodontist, sometimes twice, although the patient frequently failed to keep appointments and often rescheduled. He was also seen for several emergency visits. After four years of treatment, he regularly expressed concerns about the aesthetics of his teeth. The orthodontist attempted to address these concerns and answer all the patient's questions.

First Complaints

Six years into treatment, the patient complained that his voice had changed due to the elastics, and that he had developed a lisp. The orthodontist observed and noted in the record that the patient exhibited a lisp only when he discussed the lisp during office visits. She also documented that the patient seemed to be unstable, nervous, jumpy, and paranoid, and that he continued to refuse to wear the elastics.

At one visit, the orthodontist asked the patient if he wanted to attend a photo shoot for images to be used at a future American Association of Orthodontics event. The patient initially declined, but then agreed to do the orthodontist a favor and asked her to provide him with event details when they became available.

Seven years after the initial treatment, the orthodontist addressed with the patient the skeletal discrepancy that prevented him from having a "perfect bite," unless he opted for surgery. The patient wanted to have his braces removed before an upcoming family wedding, to which the orthodontist was invited but had declined to attend.

Social Media and Final Treatment

When the patient and the orthodontist subsequently became friends on social media, the patient learned that the American Association of Orthodontics event had already taken place. He became very upset that the orthodontist had not informed him about the scheduled date. He sent her an email in the middle of the night expressing his disappointment and demanding that his braces be removed immediately.

> **She concluded by stating that the professional relationship had broken down ...**

The orthodontist replied with an email by addressing the importance of maintaining a professional relationship, and restating the treatment limitations she had discussed with him when he was first seen. She concluded by stating that the professional relationship had broken down; she considered his care to be complete; the patient should return to her office for removal of the braces; and she would recommend another orthodontist if the patient wanted further treatment.

One month later, the patient returned for his final visit. He stated that he had removed the braces himself using a power thread. The orthodontist then removed any remaining cement, and the patient was pleased with the result. The orthodontist documented that she had informed the patient about her findings of root resorption, but the patient did not appear to be listening to what was said. Impressions were taken for retainers.

> ... the patient was obsessed with the minute aesthetic details of his teeth, and he consulted with additional providers.

Six months later, the patient went to a periodontist, who noted that there were blunted roots at #8 - #10 and #23-#27. There was mobility of a total of 10 teeth. The patient presented to another orthodontist, who indicated that no further orthodontic treatment could be provided, and that the patient needed to stabilize his condition. However, the patient was obsessed with the minute aesthetic details of his teeth, and he consulted with additional providers. All agreed that he was not a candidate for further orthodontic treatment.

Lawsuit Filed

The patient filed a lawsuit claiming that the orthodontist's treatment was careless, reckless, and contraindicated. Allegations included failure to perform diagnostic procedures, negligent performance of orthodontic treatment, failure to refer the patient to an oral surgeon, and failure to provide informed consent. The patient sought compensation for pain, mental anguish, TMJ symptoms, malocclusion, periodontal breakdown, loss of bone and root structure, and future loss of teeth.

During the orthodontist's deposition, she conceded that the estimated treatment was 18-24 months, and the average adult orthodontic case lasts two to three years, but that this case went on too long. She also testified that treatment was completed after four years, but she continued to treat the patient to address his concerns.

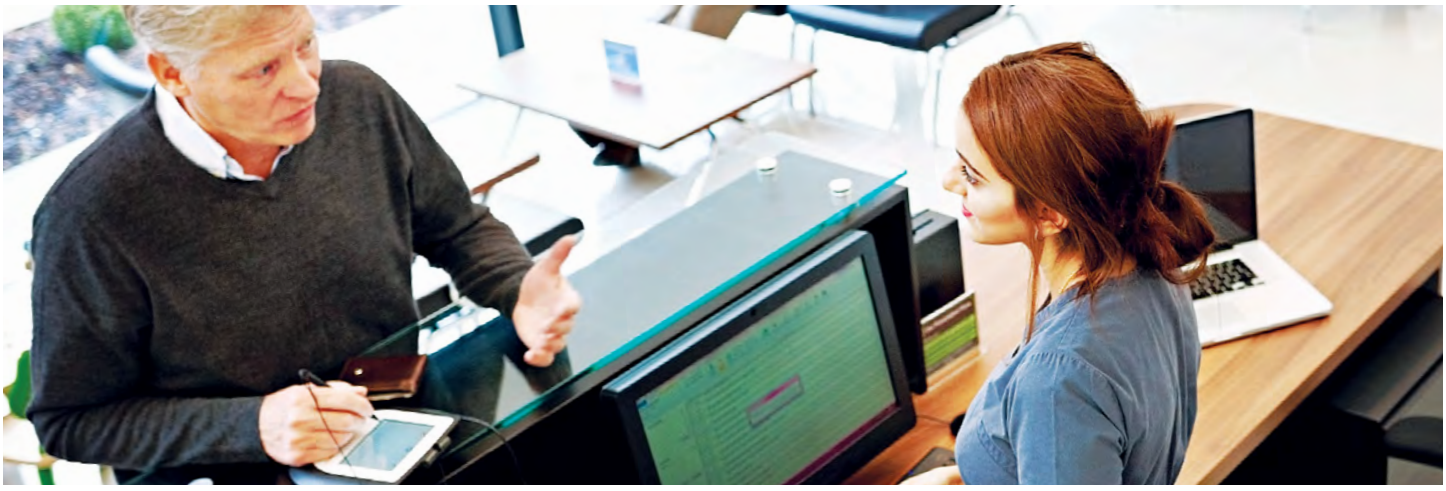
The District Claims Committee that reviewed the case concluded the orthodontist had deviated from accepted standards of care on multiple levels. It was critical of the absence of a signed informed consent form, the failure to obtain films or review those taken by other dental practitioners, the extended length of time the patient wore braces, and the patient's ability to dictate care.

The orthodontist wanted the lawsuit to be settled, but the patient's initial settlement demand was $1 million. Mediation was attempted, and the suit was ultimately settled for $245,000.

> It was critical of the absence of a signed informed consent form ...

A Legal and Risk Management Perspective

This malpractice case illustrates the potential implications of crossing professional boundaries. There were many instances of the orthodontist's conduct throughout the course of protracted treatment that blurred the line between a personal and professional relationship. She fed into the patient's unrealistic expectations by allowing him to dictate the duration of treatment. In addition, she altered the nature of the professional relationship by extending an invitation to an orthodontic event and friending the patient on social media.



She fed into the patient's unrealistic expectations ...

The patient may have misconstrued these overtures, which added insult to injury. He felt further slighted by the orthodontist's failure to follow up with event details, and her refusal to accept a family wedding invitation. All of these disappointments fueled the patient's anger over an unacceptable outcome, causing him to send the orthodontist an admonishing email in the middle of the night. Removing his own braces may have been proof positive of the patient's desperation.

It is important to note that Section 2.G. of the American Dental Association Principles of Ethics and Code of Professional Conduct (ADA Code) states, in pertinent part: "Dentists should avoid interpersonal relationships that could impair their professional judgment or risk the possibility of exploiting the confidence placed in them by a patient." Standards of ethical conduct impose a fiduciary duty on professionals to practice basic principles of dental ethics. Complexities that arise out of dual relationships may adversely impact professional conduct and judgment. Violations could result in compromised trust, dissatisfaction, findings of professional misconduct, probation, practice limitations, and/or licensure suspension or revocation.

Any interference with a therapeutic relationship could lead to serious consequences. Becoming friends with patients on social platforms in settings outside of the office could convey an inappropriate message and cause an erosion of the professional relationship. Socializing with patients, or exchanging invitations or gifts, could also compromise the integrity of a professional relationship. Any conduct that represents a risk or appearance of exploitation or potential harm to a patient must be avoided.

Dental professionals have responsibilities to patients and the dental profession to fulfill expectations of trust in the provision of competent treatment that meets patients' dental needs. Proper treatment protocols should always be adhered to, and documentation should be complete relative to informed consent, review of X-rays, and referrals to specialists. In addition, it is essential that dental providers maintain distinct parameters with patients, act responsibly, and adhere to ethical principles in a professional environment to prevent complaints, misinterpretation, and litigation.

Linda Pajonas is a Claims Specialist with MLMIC Insurance Company.
lpajonas@MLMIC.com

Marilyn Schatz is an attorney with Fager Amsler Keller & Schoppmann, LLC.
mschatz@fakslaw.com

FROM THE BLOG

MLMIC's dental blog provides ongoing and up-to-date news and guidance on important events and announcements that affect the practices of our dentist and oral surgeon policyholders.

APRIL 12, 2021

Study Shows the Mouth Is an Important Site for COVID-19 Infection

The oral cavity is an important site for COVID-19 infection, a recent study in *Nature Medicine* found. The researchers set out to better understand the "involvement of the oral cavity" in COVID-19. What they found has implications for the growing understanding of COVID-19 and the continued global effort to reduce the transmission of the virus. **READ MORE**

APRIL 12, 2021

Tips for New Dentists: How to Thrive on Your First Day in Dental Practice

From making employment decisions to risk management strategies to choosing a professional liability carrier, our "Tips for New Dentists" series has covered important information as you prepare for your first year of practice. Now, we want to focus on that very first day. What can you do to make it as smooth as possible? Here's how to set yourself up for success. **READ MORE**

Risk Management Checklists

MLMIC's series of Risk Management Checklists is designed to assist dentists and their administrators and staff with identifying potential areas of risk in the dental office setting. The strategies presented are drawn from risk management principles as well as our analysis of closed dental professional liability claims that involved office practice issues, improving patient care and satisfaction, helping prevent adverse outcomes, and minimizing professional liability exposure.

To download a complete set of MLMIC's Risk Management Checklists, visit www.mlmic.com/why-mlmic/services-resources/checklists.

COMMUNICATION — CHECKLIST #3

PROMOTING COMMUNICATION BETWEEN REFERRING AND CONSULTING DENTISTS

Lack of communication between dentists may result in poor coordination of care. This may include a delay in diagnosis or treatment, the failure to order diagnostic testing or act upon abnormal test results, or the failure to prescribe appropriate medications. Clearly defining the roles and responsibilities of the referring and consulting dentists will promote safe and effective patient care.

	YES	NO
1. A tracking system is in place to determine if the patient obtained the recommended consultation.	☐	☐
2. There is a process for determining whether a report has been received from the consulting dentist.	☐	☐
3. All consultation reports are reviewed by the referring dentist prior to being placed in the patient's record.	☐	☐
4. If a patient has been noncompliant in obtaining the recommended consultation, follow-up is performed. All attempts to contact the patient and any discussions with the patient, including reinforcement of the necessity and reason for the consultation, are documented.	☐	☐
5. If a report is not received in a timely manner, the consultant is contacted to determine if the patient has been seen and whether a report has been generated.	☐	☐
6. Consultants send reports to referring dentists in a timely manner. These reports should include the: • Findings • Recommendations, including interventions • Delineation of dentist responsibility for treatment and follow-up of test results	☐	☐
7. The consultant contacts the referring dentist when a patient fails to keep an appointment. The record reflects the missed appointment, as well as notification of the referring dentist.	☐	☐
8. All telephone conversations between referring and consulting dentists are documented. Timely communication occurs when an urgent or emergent clinical finding is identified.	☐	☐

MLMIC Risk Management Department (518) 786-2815, RMC@mlmic.com

‹ *Ransomware: A 21st Century Threat to Dental Practices, continued from page 4*

> **… an expansion of a digital footprint is also an expansion of the surface area for a cyberattack …**

Dental practices should also take precautions any time there is a system upgrade or expansion of access to e-PHI. During the COVID-19 pandemic, some dental practices incorporated the use of telehealth platforms to continue patient care without exposure to the coronavirus. Such an expansion of a digital footprint is also an expansion of the surface area for a cyberattack, and dental practices should make sure that no weaknesses are created by digital improvements involving the access, use, and storage of e-PHI.

Ransomware Defense – Vendor Business Associate Agreements and Contracts

As demonstrated by the PerCSoft and Complete Technology Solutions attacks, IT vendors who assist with the maintenance, use, and exchange of e-PHI are primary targets for ransomware, as one successful attack can have a ripple effect on hundreds of dental practices. As a result, it is crucial that dental practices investigate IT vendors and scrutinize all agreements to ensure there are protections in the event of a ransomware attack or breach of e-PHI.

Any time a vendor has access to e-PHI, dental practitioners must require a Business Associate Agreement (BAA) that ensures the vendor will appropriately safeguard any e-PHI that it manages remotely or stores on its software applications. Business associates as defined by HIPAA include subcontractors who create, receive, maintain, or transmit e-PHI on behalf of the covered entity.[10] A business associate can be held directly liable under HIPAA regulations for civil and criminal penalties resulting from the unauthorized use and disclosure of protected health information.

In addition to confirming the vendor's duty to safeguard e-PHI, the BAA should also limit the acceptable uses and disclosures of e-PHI by the vendor. Moreover, it should clarify that at the end of the contractual relationship with the practice, the vendor will return or destroy any e-PHI that it may have in its control. IT vendors will likely already have such BAAs drafted for a dental practice's execution. These agreements should be examined carefully to determine the extent of access and use being given to the vendor of e-PHI.

> **… dental practitioners must require a Business Associate Agreement (BAA) …**

Dental practices should also carefully review existing or new service contracts with IT vendors to determine the extent of protection in the event of a ransomware attack or breach. First and foremost, should a ransomware attack or breach be the result of the vendor's acts or omissions, will there be indemnification for the dental practice's damages, including third-party claims made by patients whose privacy was breached? In many cases, IT vendor agreements will exclude liability for financial costs and lost revenue stemming from a breach. Some agreements may provide for damages, but limit vendor liability to the fees already paid for services, or

10 45 C.F.R. § 160.103

for an amount specified in the agreement that is far below the actual damages likely to be sustained by the dental practice.

Other considerations when reviewing an IT vendor agreement include whether the vendor will assist the practice in the event of a ransomware attack or breach, and whether the vendor is required to maintain cyber-liability insurance with suitable indemnity limits for the associated risks.

> ... IT vendor agreements will exclude liability for financial costs and lost revenue stemming from a breach.

Ransomware Defense — Cyber-Liability Insurance

As the use of digital applications and storage continues to expand, a dental practice should assess its risk to determine whether cyber-liability insurance is necessary to protect against the fallout from a cyberattack or breach of e-PHI. Many claims associated with cyberbreaches are not covered under professional liability insurance policies.

Practice disruption aside, a ransomware attack can be very costly. Besides considering limits of indemnity, a dental practice should review the insuring agreement to determine the coverage for mitigation costs, which can include payment to forensic experts for the recovery of the ransomed data, and/or legal expenses associated with compliance with state and federal notification requirements in the event of an e-PHI breach. Another consideration is whether the insuring agreement provides coverage for regulatory fines and penalties that could result from a breach involving e-PHI.

Ransomware attackers are keenly aware of the valuable privileged information contained in electronic health records, and the devastating effect that even the temporary loss of this data can have on a dental practice. From large health systems to solo practices, the growth and diversification of their attacks is a threat to all healthcare providers and the vendors that provide them with IT services.

By developing or updating HIPAA-compliant safeguards and assessing their risks, dental practices can reduce the potential for a ransomware attack and be well-positioned to minimize damages should such an attack take place.

> ... a ransomware attack can be very costly.

William P. Hassett is a Senior Attorney with Fager, Amsler, Keller & Schoppmann, LLP.

whassett@fakslaw.com

Stay Connected

Get the latest updates and industry news from New York's #1 dental professional liability insurer. No one knows New York better than MLMIC.

LinkedIn

Follow us for important industry updates and risk management resources.

www.linkedin.com/showcase/mlmic-dental

@MLMIC

Get headlines and alerts that impact patient care in New York.

www.twitter.com/MLMIC4Dentists

MLMIC Healthcare Weekly

Stay current with the MLMIC Healthcare Weekly newsletter. Sign up at:

www.mlmic.com/healthcare-weekly

$50 FIRST YEAR COVERAGE FOR NEW GRADS

MLMIC Insurance Company, New York State's leading malpractice carrier, offers new graduates a cost-effective way to obtain dental professional liability insurance.

CALL TODAY

Choose NY's #1 dental liability insurance provider.

MLMIC provides New York dentist from Buffalo to the Bronx with localized risk management guidance, claims protection, and underwriting support. Our policyholders enjoy benefits and expertise not found anywhere else – supported by concierge-level service every step of the way.

For dental professional liability insurance in New York,
nothing compares to MLMIC.

To inquire about coverage with MLMIC,
contact **Luisa Fernandez at (212) 576-9611 or James Simons at (212) 576-9660.**

MLMIC is exclusively endorsed by:

New York State Dental Association

New York City
2 Park Avenue
New York, New York 10016

Latham
8 British American Boulevard
Latham, New York 12110

Long Island
90 Merrick Avenue
East Meadow, New York 11554

Syracuse
2 Clinton Square
Syracuse, New York 13202

Buffalo
300 International Drive
Suite 100
Williamsville, New York 14221

(800) ASK-MLMIC