MLMIC
MLMIC Insurance Company
a Berkshire Hathaway company

THE SCOPE

MEDICAL EDITION

NY

ISSUE 06 | THIRD QUARTER 2021

Ransomware:
A 21st Century Threat
to Healthcare Practices
and Facilities

CASE STUDY:
Failure to Repeat Testing
and Obtain Consultation
Resulting in CVA and Death

A Q&A Session with MLMIC
Insurance Company's
Chief Actuary

INSIDE

EXECUTIVE MESSAGE

To Our MLMIC Insurance Company Policyholders:

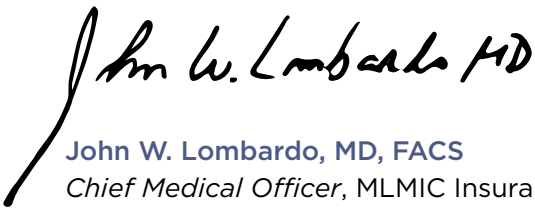
Have you been sued by a patient for malpractice? Approximately 50% of MLMIC Insurance Company's physician policyholders have. Before I became Chief Medical Officer, back when I was another MLMIC insured, I became one of those 50%.

Most practitioners who have been sued for malpractice do not want to talk about it, and that is understandable. In my experience, it is a mostly negative, unpleasant series of events.

I would encourage you to visit YouTube to view the first episode of **MLMIC's Talk Studio:** a presentation on my experiences in which I describe how it feels to be sued. By bringing this process "out of the shadows," I hope to both help prepare other practitioners for what to expect when sued and also commiserate with my peers who have gone through this ordeal. For them, knowing that their experience was not unique may provide some level of comfort.

Future episodes of MLMIC's Talk Studio will offer other presentations of interest to MLMIC's policyholders, as well as to their administrators. Most recently, two attorneys from Fager Amsler Keller & Schoppmann, LLP, counsel to MLMIC Insurance Company, **discussed the 2021 NYS Legislative Session** and its ramifications to healthcare as documented in the most recent issue of **The Albany Report.**

As always, I welcome any comments, questions, and suggestions you may have.



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 Healthcare Practices and Facilities

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 have become the primary target for ransomware attackers as patient records are a treasure trove of valuable, privileged information. In fact, the Federal Bureau of Investigation recently issued a flash warning about Hive Ransomware after it was linked to an attack on a health system in August of 2021.[2] As a result of the Hive attack, Memorial Health System in Ohio had to temporarily suspend its use of IT applications and cancel urgent surgeries as well as radiological examinations. Moreover, staff at the system's three hospitals had to resort to paper charting until its electronic-based platforms could be safely restored. Unlike other business sectors, where such attacks can be a temporary annoyance, Hive demonstrates how 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 and recommendations to minimize susceptibility to an attack.

What Is Ransomware and How Is It a Threat?

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.

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

2 "Indicators of Compromise Associated with Hive Ransomware," Federal Bureau of Investigation, Cyber Division, August 25, 2021. See also, "FBI Warns of Hive Ransomware After Memorial Health Attack in Ohio," Mitchell, Hannah, Becker's Hospital Review, September 1, 2021.

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 fewer than 100 employees.[3]**

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 fewer than 100 employees.[3] 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 practices nationwide lost access to patient charts, X-rays, and billing information.**

Two attacks that took place in 2019 highlight the vulnerability of practices to ransomware and the damage an attack can cause on practice operations. First, an attack against an IT provider, PerCSoft, encrypted the patient data it maintained in a remote backup service. As a result, over 400 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 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 practices across several Western states. In that instance, the vendor elected not to pay the ransom and focused its resources on decryption efforts, which again resulted in loss of data and extensive disruption to numerous practices until the data was recovered.

Ransomware Defense – HIPAA Compliance

The most effective way 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[4] 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.[5]

> **The Security Rule comprises three categories ... administrative, physical, and technical.**

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.[6] The Security Rule comprises three categories, called safeguards, that are aimed at protecting and securing e-PHI: administrative, physical, and technical.

Administrative safeguards require practices to implement policies and procedures to prevent, detect, contain, and correct security violations.[7] 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.

3 "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/

4 45 C.F.R. § 160.103 defines a covered entity to include a healthcare provider that transmits any health information in electronic form for billing or insurance purposes.

5 45 C.F.R. § 164.104

6 45 C.F.R. § 164.306a

7 45 C.F.R. § 164.306

continued on page 14 ›

CASE STUDY:

Failure to Repeat Testing and Obtain Consultation Resulting in CVA and Death

Initial Treatment

A 70-year-old, married, retired male had been sporadically following up with his primary care physician with complaints of diffuse abdominal pain. The patient was seen on May 30, 1996, at which time his blood pressure was 154/82 and his EKG was normal with occasional ventricular contractions. The primary care physician believed the patient had gastroenteritis, but he was also diagnosed with diabetes mellitus, for which the patient took no medications. Blood work revealed an elevated glucose of 220. In addition, the patient had mild abdominal distention. The primary physician prescribed a BRAT (bananas, rice, apples, toast) diet and repeat labs were to be done the next day. The patient didn't return until ten years later.

On May 5, 2006, the patient complained of voiding only small amounts of urine. The primary care physician believed the patient had a urinary tract infection, and the bladder was noted as elevated almost to the level of the umbilicus. Glucose was noted to be at 303 and the prostate was felt rectally to be 2+. Flomax and Cipro were given, and blood tests revealed a PSA of 26.17. The patient was given a prescription for metformin, but he refused to take it. Further bloodwork revealed the patient's glucose level had increased to 304.

Patient Hospitalized

On May 11, the patient presented to the MLMIC-insured hospital's ED with complaints of weakness, unsteady gait, and incontinence. The ED noted that the patient's bladder was extremely distended due to urinary retention. A Foley catheter was placed, obtaining 1200 cc of urine. The then 79-year-old male was admitted for uncontrolled diabetes mellitus and acute and chronic renal failure.

It was noted that the patient had not seen a doctor in the ten years prior to this date. The MLMIC-insured family practitioner affiliated with the hospital, who had never seen the patient before, was placed in charge of the patient's care. He examined the patient and noted that the patient was on no medications and, when given metformin by his PCP, had refused to take it. Lab work was ordered and revealed a fasting blood sugar of 492 and a WBC of 14.5. The patient's troponin was noted to be 0.470 with a potassium of 4.1. BUN and creatinine were elevated to 55 and 2.3, respectively. An electrocardiogram was performed that showed a great deal of body tremor, but no clear-cut evidence of any myocardial damage. An endocrinology consultation was called in by the family practitioner, and it was opined that the patient had uncontrolled diabetes mellitus, type 2, that required insulin therapy due to nephropathy and peripheral neuropathy.

> **He examined the patient and noted that the patient was on no medications and, when given metformin by his PCP, had refused to take it.**

Treatment began with 10 units of regular insulin intravenously and 12 units subcutaneously. The plan was to teach the patient and his family insulin monitoring and intravenous administration. Glucose monitoring by finger stick four times a day before meals and at bed was ordered. Lantus insulin of 50 units at the patient's hour of sleep was ordered to start on May 12.

> **The plan was to teach the patient and his family insulin monitoring and intravenous administration.**

By May 12, the patient was noted to be alert and oriented and was ambulating. The patient's breathing was not labored, and his lungs and chest were clear. The patient's cardiovascular system was noted to be stable, but no repeat troponin levels were taken. The patient's renal function was improving, and the plan was to continue the current therapy. The next day, blood work noted a WBC of 12.6, hemoglobin of 13.5, hematocrit of 40.0, and a fasting blood sugar of 240.

On May 14, it was noted that neither the family nor the patient were catching on with the diabetic teachings regarding insulin dosages. The family and patient at this point wanted oral medication to control the diabetes. The endocrinologist was trying to impress upon the patient that he required insulin therapy due to his advanced diabetes.

> **The family and patient at this point wanted oral medication to control the diabetes.**

By May 15, our insured was planning to discharge the patient within 48 hours due to the improved lab numbers. Insulin administration teachings were ongoing, however, with the family wanting oral medication for the patient. An echocardiogram revealed a normal ejection fraction of 60–65%, with some indication of mitral and tricuspid regurgitation. The family practitioner did not seek further studies, nor did he consult with cardiology.

On May 16, the patient's wife confronted the family practitioner and told him that they spoke with her husband's primary care physician, who stated he did not believe the patient required insulin treatment and that oral medication would be acceptable. The Foley catheter was removed that day, and the family stated they wanted further urology consultation. With the removal of the catheter, the patient again developed a lack of significant urinary excretion. The Foley was replaced and 500 cc of urine was obtained. Urology stated that a further workup would be obtained on an outpatient basis, once the patient improved medically. It was also on this day that the patient and his family advised the family practitioner that he would be discharged as the patient's physician.

> **Urology stated that a further workup would be obtained on an outpatient basis, once the patient improved medically.**

On May 17, the patient was placed on metformin 500mg stat PO and Glucotrol XL 5mg by the endocrinologist. The patient's blood glucose was 112–145 the prior day, most likely due to the previous intravenous Lantus. Without receiving the intravenous insulin, by May 18, the patient's fasting blood sugar was 181 in the morning and 285 prior to lunch. In the interim, the patient had become nauseous and developed anorexia with repeated vomiting the previous day due to the oral metformin. Attempts at convincing the patient and his family to embrace the

insulin monitoring and intravenous administration were again made. The endocrinologist discontinued the oral medications and returned to the insulin therapy; however, it was too late.

> **In the interim, the patient had become nauseous and developed anorexia with repeated vomiting the previous day due to the oral metformin.**

On May 18, at 9:25 PM, the patient sustained a cardiopulmonary arrest and was found in asystole. The patient underwent CPR as per ACLS protocol. The patient was intubated with no aspirate in the ET tube to suggest that the patient had aspirated any vomitus. A nasogastric tube was also placed that revealed three liters of dark material that had been suctioned several times during the code. Resuscitative efforts ceased after 33 minutes. The family was notified, and no autopsy was performed.

Lawsuit Filed

A lawsuit was filed by the patient's family against the family practitioner alleging a failure to order further metabolic testing, obtain a cardiac consultation, and address urinary incontinence and abdominal distension resulted in the wrongful death of the patient.

The case was reviewed by various MLMIC consultants who found problems with the care provided by our insured family practitioner. They opined that he failed to adequately treat the diabetes and ignored a slightly elevated (at 0.47) troponin and an EKG that MLMIC's in-house cardiac consultant did not feel was "normal." In addition, they believed that the troponin levels as well as EKG testing required repetition, especially in a diabetic. The patient had presented with significant metabolic disturbances, and the experts felt it would be routine to continue testing those values. They added that a cardiac consultation should have been ordered, a flat plate of the abdomen should have been done, and, as the patient's abdomen was distended, a nasogastric tube should have been placed to rule out an abdominal obstruction. Finally, the experts believed that the excessive vomiting led to an electrolyte imbalance that was never addressed by the family practitioner. As a result of multiple reviews in numerous disciplines, settlement of the case was recommended.

> **The patient had presented with significant metabolic disturbances, and the experts felt it would be routine to continue testing those values.**

The defense counsel provided a case evaluation that included pain and suffering worth $150,000 to $250,000, and wrongful death with a value of $150,000 to $250,000, with a total value of $300,000 to $500,000. They estimated the case's settlement and jury value to be equivalent. Our insured initially refused to settle this matter, but later agreed.

The plaintiff's counsel made a demand of $400,000. By invoking the culpable conduct of the patient and his family in refusing to proceed with the recommended treatment and acting against medical advice, the MLMIC Claims Specialist eventually settled the matter for $200,000 on behalf of the family practitioner.

A Legal and Risk Management Analysis

Medical professionals often encounter the difficult or noncompliant patient. This patient makes it difficult to provide adequate or proper care. In fact, a patient's failure to follow up or follow medical advice can have negative impacts on their health and overall outcome. In this instance, this 70-year-old patient was sporadically treated by his primary care physician and had a diagnosis of diabetes. He failed to return for ten years, never followed up for his repeat labs, and refused to take a recommended medication. During this time, the patient's condition deteriorated.

> **In fact, a patient's failure to follow up or follow medical advice can have negative impacts on their health and overall outcome.**

It is essential for physicians and providers to have protocols in place to remind patients about their appointments and/or their need for additional care. Also, there needs to be effective communication between doctors and their patients. This will both help the physician discover the cause of the behavior for the noncompliance and assess the patient's comprehension of the treatment plan. Having meaningful exchanges of information with patients is also vital so that they understand and comply with a recommended plan. Better compliance will ultimately lead to better outcomes. All communication with a patient must be documented. Office practices should keep clear, consistent records of missed

A Legal and Risk Management Analysis *(continued)*

appointments and follow-ups as well as their attempts at contacting the patient, what was communicated to the patient, and the patient's response. A well-documented record will show the patient's responses and the provider's attempt(s) to develop a plan of care. Of course, continued noncompliant behavior will disrupt the physician-patient relationship and may require dismissing the patient from the provider's practice.

> **All communication with a patient must be documented.**

This patient's hospital course was complicated by a disruptive family and its dynamics. In this case, the family played a large role in the medical decision making. While families are important to patient care, they should not dictate care unless they are authorized to do so. A demanding family does not remove medical decision making from competent patients. This patient showed no evidence of lack of capacity, so he could make his own healthcare decisions, and there was no requirement for the provider to be so deferential to the family.

> **While families are important to patient care, they should not dictate care unless they are authorized to do so.**

While the family did not want the patient to use insulin, it was the endocrinologist's opinion that insulin was the best treatment option for the patient given his advanced diabetes, a point he tried to make with both the patient and the family. It is important to remember that family members often begin to seem demanding because they are afraid and feel powerless in helping their loved one. Even if a family is being difficult, it is important to effectively communicate and collaborate with them since they can offer important information about the patient. Also, providing information in terms that family members can understand can result in improved patient outcomes. Again, it is important to document what was discussed and counseled to the family and any disagreements with the plan.

The most significant issue during the patient's hospital course involved the family practitioner's failure to obtain further studies and his failure to refer the patient for a cardiology consult due to the patient's uncontrolled diabetes and elevated troponin and EKG results. The patient also needed further studies to rule out an abdominal obstruction.

Physicians have an obligation to bring in a specialist(s) whose background, training, and experience can assist with a complete and thorough workup. Further, the physician's failure in ordering and evaluating further studies can cause health conditions to go undiagnosed or misdiagnosed. The family practitioner's failure to investigate additional sources of these findings ultimately led to the death of the patient.

> **The family practitioner's failure to investigate additional sources of these findings ultimately led to the death of the patient.**

Finally, the primary care physician who was initially discharged by the family and the patient as his physician could also have been named as a defendant in this case as, a day after he was

discharged, the patient developed excessive vomiting. Despite the discharge, the physician may still have been found to be responsible for the care and treatment of the patient until the care was taken over by another physician.

The Education Law indicates the following is professional misconduct: "[a]bandoning or neglecting a patient under and in need of immediate professional care, without making reasonable arrangements for the continuation of such care" (N.Y. Educ. Law § 6530(3)). Despite being discharged, the internist needed to explain to the patient and family that he was obligated to treat and could not neglect any patient in immediate need unless reasonable arrangements have been made for his care.

Robert Graf is a Claims Supervisor with MLMIC Insurance Company

rgraf@mlmic.com

Mirsade Markovic is an attorney with Fager Amsler Keller and Schoppmann, LLP.

mmarkovic@fakslaw.com

Danielle Mikalajunas Fogel is an attorney with Fager Amsler Keller and Schoppmann, LLP.

dfogel@fakslaw.com

Stay Connected

Get the latest updates and industry news from New York's #1 medical 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/company/mlmic

@MLMIC

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

www.twitter.com/mlmic

MLMIC Healthcare Weekly

Stay current with MLMIC Healthcare Weekly's monthly newsletter. Sign up at:

www.mlmic.com/healthcare-weekly

Challenging Times Ahead for the Medical Professional Liability Sector:

A Q&A Session with MLMIC Insurance Company's Chief Actuary

The financial rating agency AM Best issued a report last spring ("Continued Uncertainty Clouds the Horizon for MPL Insurers") indicating that, due to a myriad of factors, 2020 marked the sixth consecutive year of underwriting losses for medical professional liability (MPL) insurers.

Citing the continued pressures of depressed demand, concern over rate adequacy, rising claim cost trends due to social inflation (i.e., changing societal attitudes), and diminishing reserve redundancies, along with the potential for an increase in claims frequency owing to the pandemic, the report stated that it maintains a negative market segment outlook on the MPL insurance market sector.

To help our readers gain an understanding as to what this means for not only MPL insurers such as MLMIC, but for purchasers of MPL coverage as well, we have posed relevant questions to Thomas Ryan, MLMIC's Chief Actuary.

Q: Given the concerns stated in the AM Best report, in your opinion, what impact do you feel these factors will have on the New York MPL marketplace in the short and long term as well as for MLMIC and its Insureds?

A: The MPL insurance marketplace is very diverse and varies widely between states based on legislation, regulation, and market competition. In New York, protection for healthcare providers can be provided by commercial insurance entities including admitted insurers (those regulated by the New York Department of Financial Services, or DFS) like MLMIC, and nonadmitted insurers such as risk retention groups, which are not regulated by the New York DFS. Coverage for MPL claims can also be provided through self-insurance, which is usually employed by large physician groups or hospital systems. In their role as a financial rating agency, AM Best's report focuses on the commercial insurance market. But many of the concerns raised, such as rising claim costs and the potential increase in claims frequency, could impact self-insurers as well.

Despite these concerns and the overall negative outlook for the MPL sector, New York should have a competitive MPL insurance marketplace for the foreseeable future. While New York's numerous competitors in the market will ensure there is insurance availability to healthcare providers, these providers will likely pay more for this protection due to greater claim frequency and rising costs.

Insurance rates for healthcare providers are based on analyses of both the number of claims made against providers and the cost to defend and settle these claims. The number of MPL claims reported in New York has been relatively flat in recent years, but higher than expected settlement amounts have resulted in many insurers raising the rates they charge. For admitted carriers such as MLMIC, physician rates are set by the DFS based on its view of the loss experience for the marketplace and individual insurers. Nonadmitted insurers are not subject to regulation by the DFS and can readily implement large rate increases for providers when faced with new claims or large settlement amounts on existing claims.

Q: Do you think the COVID-19 pandemic will have a dramatic effect in either direction on the future costs and availability of insurance in the overall MPL marketplace?

A: Due to the recency of the pandemic and the long delay in reporting and settling most MPL claims, there is still a great amount of uncertainty as to the impact of the pandemic on insurer loss experience and the resulting insurance rates and availability. While there were reduced volumes of care and limited immunity provisions in place during the peak of the pandemic, which would tend to lower future claims, there are also concerns over more severe MPL claims resulting from delayed treatments and diagnoses. Additional uncertainty results from court closures and delays due to the pandemic, which have limited opportunities to resolve reported claims.

In the long term, the insurance marketplace will be impacted by the pandemic more from changes to the practice and business of medicine rather than by any resulting claims. As noted by AM Best, the decrease in the volume of care resulting from the pandemic resulted in the acceleration of several trends such as the retirements of older physicians and the consolidation of individual practitioners and smaller groups into larger entities, which will result in depressed demand that may never be replaced. Also, telehealth, with its own unique risks, played a large role during the pandemic and will likely continue, resulting in insurers addressing any possible telehealth coverage concerns from insureds.

Q: Are MLMIC's finances sufficient to withstand the anticipated challenges that lie ahead for MPL insurers?

A: MLMIC is the largest writer of MPL insurance in New York and has maintained this market leadership position for over 45 years. Recognizing its quality and stability, MLMIC was acquired by Warren Buffett's Berkshire Hathaway in 2018. As part of Berkshire Hathaway, MLMIC has enhanced financial strength and recently received an A+ rating (Superior) from AM Best. MLMIC is ready to meet any challenges – anticipated or unanticipated – that lie ahead in the marketplace.

Q: What actions can healthcare providers take to help temper claims in order to keep rates more stable?

A: Perhaps the most valuable tool that healthcare practitioners can avail themselves of in this regard is the completion of effective risk management courses such as those offered by MLMIC. These ongoing courses offer useful insights on identifying current liability issues and claim trends, while also providing risk management strategies to help prevent suits and claims. Beyond this, MLMIC's Claim Data Analytics program identifies loss drivers pertinent to a given organization, specialty, or region. Healthcare providers can work with MLMIC Risk Management Consultants to mitigate identified risks and improve quality of care and patient outcome, thereby reducing liability exposure.

Q: The AM Best report cited that "given the liability uncertainties of today, innovation is becoming more important for MPL insurers." What has MLMIC done to adhere to this observation?

A: MLMIC has always been sensitive to the challenges faced by our customer base. The Company has developed several exciting new programs aimed at identifying and addressing the needs of our policyholders during this time of change and uncertainty. From our existing, well-respected risk management programs to the implementation of our **Preferred Savings Programs** and our latest SILO insurance program, which was designed to provide comprehensive protection for employed physicians, MLMIC continues to monitor and quickly react to changes in the industry.

SILO offers solutions to these challenges through flexible coverage options, direct risk mitigation reviews, detailed claims data analytics, and a team of dedicated professionals with unparalleled experience to guide any health system through the many managerial and financial uncertainties that exist in today's practice environment. The SILO solution is built upon a foundation of strong collaboration and the desire to jointly achieve early resolution of incidents, claims, and lawsuits. For more information on this program, **please click here.**

Robert Pedrazzi is an Assistant Vice President of Underwriting with MLMIC Insurance Company.
rpedrazzi@mlmic.com

Thomas Ryan is a Senior Vice President of Analytics and Chief Actuary with MLMIC Insurance Company.
tryan@mlmic.com

FROM THE MLMIC INSIDER

The MLMIC Insider provides ongoing and up-to-date news and guidance on important events and announcements that affect the practices of our insured physicians and other healthcare providers.

If you are interested in receiving informational posts such as the following, please be sure to sign up to receive MLMIC's *Healthcare Weekly* – the latest MLMIC Insurance Company news and links to relevant and valuable industry articles.

AUG 24, 2021

"Hybrid Future" for Telehealth and In-Person Care Requires Thoughtful Integration of Technology

As the nature of healthcare delivery moves toward a hybrid blend of telehealth and in-person care, thoughtful policies and protocols must be created to preserve the physician-patient relationship. **READ MORE**

AUG 18, 2021

Long-term Impact of COVID-19 on Healthcare Industry, Including Vaccine Misinformation

We remain cognizant of the impact that COVID-19 has had on our insureds, their staff, and their loved ones. We recognize the rising Delta variant and its impact on communities with a high unvaccinated population and continue to battle vaccine hesitancy and misinformation. **READ MORE**

‹ *Ransomware: A 21st Century Threat to Healthcare Practices and Facilities, continued from page 3*

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.[8]

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.[9] 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.

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.[10]

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, multiple backup sets of data should be maintained.

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

Healthcare practices and facilities should also take precautions any time there is a system upgrade or expansion of access to e-PHI. During the COVID-19 pandemic, some practitioners 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 such 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 practices. As a result, it is crucial that IT vendors are investigated and all agreements scrutinized 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, 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.[11] 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.

8 45 C.F.R. § 164.400–414
9 45 C.F.R. § 164.310
10 45 C.F.R. § 164.312
11 45 C.F.R. § 160.103

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. These agreements should be examined carefully to determine the extent of access and use being given to the vendor of e-PHI.

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

Healthcare practices and facilities 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 any 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 for an amount specified in the agreement that is far below the actual damages likely to be sustained by the practice or facility.

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.

> **In many cases, 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 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, insuring agreements should be reviewed 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. 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, healthcare practices and facilities can reduce the potential for a ransomware attack and be well-positioned to minimize damages should such an attack take place.

William P. Hassett is a senior attorney with Fager, Amsler, Keller & Schoppmann, LLP.

whassett@fakslaw.com

The MLMIC Insider

Timely Information and Insights for Policyholders

Since its founding in the mid-1970s, MLMIC Insurance Company has curated a vast library of information and educational resources relating to medical professional liability insurance coverage, malpractice litigation, legislative matters, risk management tips and insights, broader industry news, and so much more.

To make that wealth of content more easily accessible, MLMIC has launched the **MLMIC Insider**, which can be found on our website and at **https://www.mlmic.com/mlmic-insider**.

With the **MLMIC Insider** and its robust search capabilities, the company will endeavor to keep its policyholders up to date on an array of important matters and continue to serve as a leading resource for risk management education and other topics of interest to medical professionals.

Specifically, the **MLMIC Insider** contains:

MLMIC Talk Studio

A video series also available on MLMIC's YouTube channel covering important and trending issues in professional liability, healthcare law, and risk management.

The Scope: Medical Edition

Published quarterly, this newsletter offers the latest healthcare, legal, risk management, and insurance information.

The Albany Report

The latest edition focuses policyholder attention on proposed legislation that would expand liability in MPL cases.

Risk Management Checklists

A series designed to enhance and inform the risk management practices and processes of medical offices, practices, and facilities.

Medical Malpractice FAQs

Answers to the questions most asked by MLMIC Insurance Company policyholders.

MLMIC Blog

An insightful series of over 600 posts covering a wide range of topics relative to healthcare.

Event News

Details on upcoming industry events, educational webinars, CME offerings, and other important reminders relating to policy matters, industry activities, and more.

We encourage you to bookmark the MLMIC Insider homepage and visit regularly!

You can also subscribe to **MLMIC's Talk Studio YouTube channel** so you can be notified as soon as new episodes become available.

If there are any topics you would like to see more of, please let MLMIC know!

New York City Healthcare Heroes Parade

MLMIC Insurance Company is proud to have participated in the New York City Healthcare Heroes Parade on July 7 in lower Manhattan. With hospitalizations and cases down earlier in the summer, it was a breath of fresh air to celebrate our healthcare providers and all they have done for their patients in the State of New York.

As the COVID-19 pandemic persists, and our medical communities and frontline healthcare workers continue to face unimaginable adversity, MLMIC would like to remind New York's healthcare providers that we stand with and support you. We sincerely thank you for all you do.

Have you seen Talk Studio yet?

Check out MLMIC's new video series on important and trending issues in professional liability, healthcare law, and risk management.

Recent episodes of Talk Studio include:

- Malpractice Lawsuits From a Defendant's Perspective
- 2021 Legislative Impacts on New York Physicians and Hospitals

Watch now at MLMIC.com/talkstudio.

P.O. Box 1287
Latham, New York 12110

New York City | Long Island | Colonie | Syracuse | Buffalo

(800) ASK-MLMIC