MLMIC
MLMIC Insurance Company
a Berkshire Hathaway company

THE SCOPE

MEDICAL EDITION

ISSUE 02 | THIRD QUARTER 2020

INSIDE

"[My defense attorney] was extremely professional and very encouraging... She is excellent!"

MLMIC-Insured Anesthesiologist
Westchester County, New York

EXECUTIVE MESSAGE

To Our MLMIC Insurance Company Policyholders:

Over the course of the three months since our inaugural issue of *The Scope* was released, it has been encouraging to see the COVID-19 situation in New York improve. Hospitalizations and cases are down significantly from their peak in April and May, and most practices are now operating in this "new normal" of increased vigilance in which we find ourselves.

Throughout it all, the staff of MLMIC realizes that it is you, the physicians, dentists, and advanced practice providers out there in the field, who are working the hardest to pull the people of New York back from the edge of this dire situation. Not the politicians. Not the pundits. Not the armchair quarterbacks.

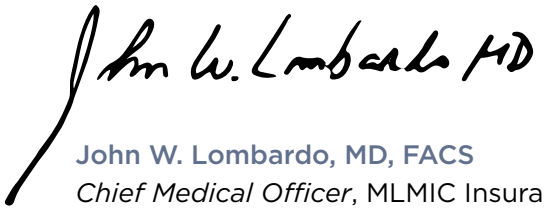
We also realize that your professional focus is on your patients, your practice, and your coworkers. Not your medical professional liability insurance. As such, it has been MLMIC's aim to unobtrusively support you by offering guidance and resources when appropriate.

Issue #2 of *The Scope* hits the hot-button topic of telehealth from the perspective of medical professional liability, MLMIC's expertise.

So how are we doing? Are you hearing from us too much or not enough? Are you finding the guidance and support provided to be of value? What topics would you like addressed in a future issue of *The Scope*?

As a physician not long removed from active practice, I want to hear from you. Please do not hesitate to **contact me** at any time to share your thoughts, experiences, and suggestions … or perhaps just to swap "war stories."

Please stay safe and, to inject a little levity from a classic film, **"Go do that Voodoo that you do so well!"**



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

Telehealth & Cybersecurity Considerations

The COVID-19 pandemic catapulted telehealth to the forefront of healthcare as an effective means for physicians to continue to provide care without exposing themselves or their patients to the highly contagious coronavirus. Through waivers of state and federal regulations, the use of this technology quickly accelerated, with many providers using common platforms such as Skype or FaceTime to communicate with their patients.[1] As New York state slowly emerges from this health crisis, the use of virtual treatment through telehealth continues to expand as both practitioners and patients have realized its benefits.

However, the rapid expansion in the use of this technology has increased the risk of privacy breaches as well as cyberattacks. Health records present a treasure trove of valuable information for cybercriminals, and telehealth provides yet another avenue to gain access and exploit these materials for nefarious purposes. This article will provide an overview of applicable Health Insurance Portability and Accountability Act (HIPAA) standards related to cybersecurity, with a focus on practices that can help reduce the risk of privacy breaches or cyberattacks related to the use of telehealth.

Telehealth and the HIPAA Security Rule

HIPAA requires covered entities[2] to develop and follow procedures that ensure the privacy and security of protected health information (PHI) whenever it is transferred, received, or handled.[3] These requirements apply to all forms of PHI, including information obtained or transmitted via telehealth or teleconferencing.

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 electronic PHI.[4] Although the Security Rule provides basic standards, it allows for flexibility of approach and permits practices to evaluate their own needs and use any security measures that allow compliance with the standards. In deciding what security measures to incorporate, the HIPAA regulations provide that a practice must consider its size, complexity, and capabilities, as well as its technical hardware, its software infrastructure, and the costs associated with security measures. The Security Rule is composed of three categories, called safeguards, that are aimed at protecting and securing PHI: administrative, physical, and technical.

The Security Rule is composed of three categories, called safeguards, that are aimed at protecting and securing PHI: administrative, physical, and technical.

ADMINISTRATIVE SAFEGUARDS

Administrative safeguards require practices to implement policies and procedures to prevent, detect, contain, and correct security violations.[5] Similar to any other device or software containing PHI, practices should implement strong password security on any telehealth platforms used to communicate with patients. Practices should also ensure that its practitioners using telehealth maintain individual passwords on these platforms and require that the passwords are changed with regularity.

Existing practice security policies pertaining to employees and staff should also be reviewed and updated to accommodate additional risks presented by

telehealth. This should include the development of an incident response and remediation plan to address breaches should they occur. This plan should specifically address the manner of notifying the affected patients and potentially the Department of Health and Human Services or law enforcement, depending upon the nature and size of the breach.

Finally, practitioners must require that their telehealth platform vendor enter a Business Associate Agreement (BAA) that ensures the vendor will appropriately safeguard PHI that is stored or transmitted via its platform. Business associates are defined by HIPAA to include subcontractors who create, receive, maintain, or transmit PHI on behalf of the covered entity.[6]

A business associate can be held directly liable under HIPAA regulations for civil and criminal penalties for the unauthorized use and disclosure of PHI. In addition to confirming the vendor's duty to safeguard PHI, the BAA should also limit the acceptable uses and disclosures of PHI by the vendor. Moreover, it should clarify that at the end of the contractual relationship, the vendor will return or destroy any PHI of the practice that it may have in its control.

Telehealth platform vendors will likely already have BAAs drafted for a practice's execution. These agreements should be examined carefully to determine the extent of access and use of PHI being given to the vendor.

PHYSICAL SAFEGUARDS

The Security Rule also requires practices to implement policies and procedures to limit physical access to their electronic information systems, including desktops, laptops, tablets, and smartphones.[7]

Any devices that contain PHI or are used for telehealth should be locked with user password access.

Any devices that contain PHI or are used for telehealth should be locked with user password access. Practices should also consider disabling USB ports on any devices that are used for telehealth transmissions. Ports are a prime source for the introduction of malware via thumb drives and other devices.

The facility where the telehealth devices are housed should be physically locked to prevent inappropriate access or theft.

Most importantly, when a provider is interacting with a patient via telehealth, it should be done in a secure location that would not allow audio or visual access to unauthorized third parties. Always be cognizant of conducting the telehealth patient encounter in the same manner as a face-to-face encounter in an examination room.

TECHNICAL SAFEGUARDS

The technical safeguards of the Security Rule require that practices implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access.[8]

First and foremost, the practice should confirm that its telehealth platform vendor is HIPAA compliant. The practice should also maintain a policy that software updates, including anti-malware applications, are regularly performed on office computers, tablets, and smartphones.

Telehealth communications should be conducted over a virtual private network (VPN). This connection method will provide end-to-end encryption of data between the practice's private network and the patient's device.

Finally, the practice should consider if the telehealth platform is electronic health record (EHR) agnostic and whether its integration with an existing EHR system could cause security weaknesses that could expose additional PHI.

Other Important Considerations

Despite due diligence and developing best practices, privacy breaches or cyberattacks may still occur. In addition to developing or upgrading policy safeguards, there are many other components of risk prevention that a practice should consider relative to telehealth security.

PATIENT RISKS

Unlike practices, patients are not subject to the HIPAA Security Rule and may be their own worst enemies when it comes to a privacy breach stemming from telehealth. Practices should inform patients that the unauthorized use of their smartphones, tablets, and laptops can result in a privacy breach or cyber threat. Patients

should also be informed that the use of electronic devices accessible by others, such as workstations, should not be used for telehealth.

The patient's obligations should also be discussed when obtaining his or her consent to telehealth. When a written patient consent for telehealth is used, a practice should consider incorporating language in the document that acknowledges that the patient was advised and understands the practice has no responsibility for privacy breaches stemming from the patient's own failure to take preventive measures.

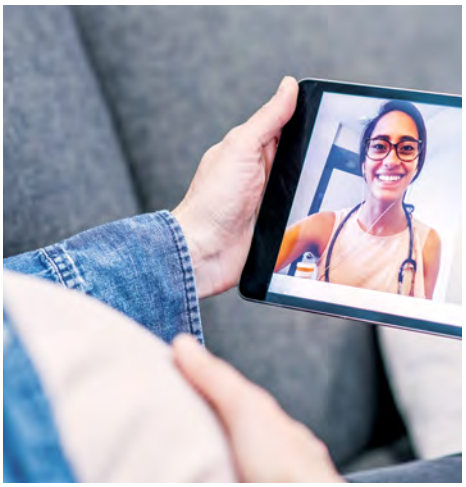
Practices should inform patients that the unauthorized use of their smartphones, tablets, and laptops can result in a privacy breach or cyber threat.

Finally, before commencing a telehealth videoconference, a practitioner should also confirm that the patient is in a confidential location where PHI cannot be overheard by a third party.

TELEHEALTH PLATFORM VENDOR AGREEMENTS

Not all telehealth platforms are created equal. Practices should research telehealth platform vendors and scrutinize contracts and service agreements.

Some of the things to look for in a vendor agreement include whether the vendor will provide assistance in the event of a privacy breach or cyberattack; whether the vendor provides



indemnification for the practice relative to damages stemming from a privacy breach caused by its services; and whether there are limits placed on the vendor's liability, such as an amount specified in the agreement or the fees already paid for service. Finally, the practice should confirm that the platform vendor maintains cyber-liability insurance, including the policy limits, to cover privacy breaches that may be caused by the vendor's negligence.

CYBER-LIABILITY INSURANCE

Finally, a practice should assess its telehealth footprint and risks to determine whether it should maintain cyber-liability insurance to protect against a potential breach or cyberattack.

Many claims associated with cyberbreaches are not covered under a professional liability insurance policy. Without adequate coverage, this can prove costly for a practice.

Besides considering a policy's limits of indemnity, a practice should investigate if the policy provides coverage for regulatory fines relative to HIPAA violations. Also, in the event of a breach or attack, does the policy provide coverage for post-event mitigation costs, including information technology contractors and legal counsel?

Conclusion

The rapid expansion of telehealth has provided many benefits to both practitioners and their patients. As the use of this technology continues to grow, practices must be aware of the risks presented by potential privacy breaches and cyberattacks. By developing HIPAA-compliant safeguards and assessing its own risks, practices can minimize these potential exposures and associated damages.

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

whassett@fakslaw.com

[1] See, Department of Health & Human Services – Office for Civil Rights, Notification, 3/17/20, https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html. See also, Executive Order, Gov. Cuomo No., 202, https://www.governor.ny.gov/news/no-202-declaring-disaster-emergency-state-new-york.

[2] 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.

[3] 45 C.F.R. § 164.104

[4] 45 C.F.R. § 164.306

[5] 42 C.F.R. § 164.306

[6] 42 C.F.R. § 160.103

[7] 42 C.F.R. § 164.310

[8] 42 C.F.R. § 164.312

Checklist to Mitigate Risk with Telehealth

During the COVID-19 pandemic, telehealth encounters have been essential to providing care. While telehealth services may be necessary, there is always a concern that using this technology may lead to liability exposure.

The following is a checklist of factors to consider when using telehealth for the treatment of patients:

- **Is this an appropriate patient for a telehealth encounter?**
  - If not, recommend a traditional office visit.
- **Was consent obtained for the telehealth encounter?**
  - It must be documented in the chart and/or obtained with a signed form, if possible.
- **Where is the patient located?**
  - As telehealth services are delivered where the patient is located, licensing issues may exist for care being provided to a patient located in a state where the practitioner is not licensed.
- **How is the video/audio quality?**
  - Poor audio quality can result in a lack of communication and misunderstandings.
  - Poor video quality can result in potential misdiagnosis.
- **Is the encounter properly documented in the patient chart?**
  - Create, maintain, and update medical records as you would an in-office visit.
- **Is HIPAA-compliant technology being used?**
  - Enter into an appropriate Business Associate Agreement.
  - Use a platform/network that encrypts data for end-to-end protection during the telehealth transmission.
- **Does the telehealth encounter mirror an encounter in the examination room?**
  - Ensure the patient is in a secure location where exchanges are not audible to others.
  - No one should be present at the practitioner's location that should not be privy to the encounter.
  - Consider the presence of a chaperone for encounters of a sensitive nature.
- **Is there a proper plan in place for recommendations and follow-up?**
  - Adhere to the same follow-up requirements as in-office visits.

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

dfogel@fakslaw.com

MLMIC's Preferred Savings Programs

Save between **5%** and **15%** on qualifying programs.

MLMIC has partnered with groups and organizations across the state to help you receive New York's #1 medical professional liability insurance at an even lower cost:

CAIPAcare

Northwell Health*

CHS Physician Partners
Catholic Health Services
At the heart of health

Corinthian Medical IPA

doctor.com

ECAP

Excellus Credentialed Physician Insurance Program

HudsonDoctors

MAGNACARE℠

NYNM NewYork NetworkIPA

Voluntary Attending Physicians

Additional discount opportunities.

Physicians who meet certain requirements can take advantage of valuable reductions on their premiums (potentially in combination with the Preferred Savings Program).

UP TO 50% SAVINGS
for new doctors

UP TO 50% SAVINGS
for part-time doctors

UP TO 12% SAVINGS
for qualified physicians and surgeons with no open or closed claims

5% SAVINGS
when you complete a New York state-approved risk management program

5% SAVINGS
for individual physician policyholders who waive consent to settle a claim

2% PREMIUM CREDIT
for prompt payment of the full annual premium within 30 days of receipt of the invoice

1.4% REDUCTION
of the indemnity deductible

See how much you can save.

Request a quote at **MLMIC.com/psp**, or contact your broker today.

For Risk Purchasing Groups (RPG) programs, membership required. Subject to application and approval. Check our website for the latest information and newest savings opportunities.

Not all discounts are combinable. Risk Purchasing Groups (RPG) are subject to annual review and upward or downward adjustment (including removal altogether), pending approval by the New York State Department of Financial Services, and is based on the overall loss experience of the RPG's members.

*Northwell Health is not affiliated with MLMIC Insurance Company, a Berkshire Hathaway Company. Northwell Health is not engaged in, nor responsible for, the provision of professional liability insurance, related services, and/or products. Any and all policies of insurance, services, and/or products shall be provided by MLMIC Insurance Company. Northwell Health shall not be liable for any claims and/or damages that may arise from the provision of policies of insurance, services, and/or products.

CASE STUDY:

Late Discovery of a Patient's Family History Leads to Delayed Treatment

While MLMIC continuously addresses the need for complete and accurate documentation of patient care as a significant factor in avoiding litigation, the fact remains that poor documentation continues to be a contributing element in many medical professional liability suits. The following case study examines this issue from the perspective of a defense verdict, found in favor of the MLMIC-insured physician, that could very easily have been won by the plaintiff.

The patient in this case was a 42-year-old woman with two young children who worked as a cardiac sonographer earning approximately $90,000 per year. She had been treated by practitioners at a large medical group since 2007.

At the patient's first visit with the MLMIC-insured ob-gyn in February 2011, she had no specific complaints, but did offer a history of heavy monthly menstrual bleeding. She had already undergone two dilation and curettage procedures, the last being in 2009. The patient reported no family history of breast, uterine, cervical, ovarian, or colon cancer. Measures to address the bleeding were discussed, including a NovaSure ablation procedure, but she advised the ob-gyn she did not want an ablation.

The following month, the patient underwent a guided core biopsy of the left breast after mammography and ultrasound noted a suspicious mass. Pathology indicated a benign fibroadenoma, and a six-month follow-up was recommended.

Pathology indicated a benign fibroadenoma, and a six-month follow-up was recommended.

In June 2011, she was seen by her PMD for complaints of decreased energy and feeling tired. Iron supplements were recommended.

In December 2011, the patient underwent a bilateral breast ultrasound. She again reported no family history of breast or ovarian cancer.

The patient returned to our ob-gyn in February 2012, with complaints of significant menorrhagia with her cycles. NovaSure ablation was again discussed, and she consented to the procedure. In preparation, the ob-gyn performed a transvaginal ultrasound for the sole purpose of obtaining measurements of the uterus. He also performed an endometrial biopsy, which was reported as benign. The ob-gyn did not visualize the ovaries.

The following month, the patient underwent a bilateral mammography and breast ultrasound at another facility. Her patient questionnaire again reflected no family history of breast cancer in a parent, sister, daughter, grandmother, or aunt.

Two months later, the ob-gyn performed the NovaSure ablation. At that time, there were no palpable adnexal masses, and no complications from the procedure were noted. Pathology later revealed a benign asynchronous endometrium. A follow-up exam was noted to be negative for pelvic masses.

At that time, there were no palpable adnexal masses, and no complications from the procedure were noted.

In December 2012, however, the patient called her PMD with complaints of bloating and crampy pain. She told this doctor that she had performed an ultrasound scan on herself and believed she had a 4 cm lesion on her right ovary. The patient was advised to contact her

ob-gyn, but he was not available. She then contacted an ob-gyn at another practice and was seen that day. The patient gave that physician a family history of two cousins with breast and ovarian cancer.

Ultrasound revealed a 3.2 cm complex right ovarian cyst. A CT scan was ordered, and the report read, "The right ovary is nodular in contour suspicious for a mass measuring 5x5.2 cm. A 2.4 cm cyst is seen in the right ovary. Nodularity is also seen in the left ovary. This is not enlarged but also must be regarded as suspicious."

The patient was referred for additional testing at Yale-New Haven Hospital and, subsequently, Memorial Sloan Kettering, where she gave a history of a paternal cousin having breast and ovarian cancer.

Test results were reported as stage IIIC ovarian cancer.

She also reported that she was of Ashkenazi Jewish descent, another risk factor. Test results were reported as stage IIIC ovarian cancer. The patient underwent a total abdominal hysterectomy and debulking procedure, and a final pathology report revealed high-grade serous carcinoma in the right and left pelvic peritoneum, paracervical soft tissue, uterine serosa, right and left fallopian tubes, and both ovaries.

Although the patient took part in several clinical trials, her disease became widespread. Additional surgeries were not performed, and she no longer was a candidate for clinical trials.

A lawsuit was filed against the MLMIC-insured ob-gyn and the medical group, which was insured by a different carrier. A joint defense between both parties was discussed and agreed upon since the allegations against the group were vicarious in nature. Allegations against the ob-gyn included a 10- to 12-month delay in the diagnosis of ovarian cancer; the failure to appreciate a significant family medical history involving a first cousin with early onset ovarian and breast cancer; the failure to refer the patient for genetic counseling, which would have resulted in testing for the BRCA mutation; and the failure to visualize her ovaries when performing the transvaginal ultrasound in preparation for the NovaSure ablation.

Damages included the progression of ovarian cancer to stage IV; reduced life expectancy; loss of a chance for a cure; extensive hospitalizations; chemotherapy and radiation; fatigue; pain and suffering; and fear of impending death. A demand of $4.3 million was made.

Expert opinions in ob-gyn, oncology, radiology, pathology, and GYN/ONC were secured as discovery progressed. Based on these opinions, as well as deposition testimony, the matter was deemed defensible on behalf of the MLMIC-insured ob-gyn. Since no offers toward settlement were going to be made by the defense, the plaintiff's attorney asked for an immediate trial date due to his client's rapidly deteriorating health.

Testimony began in early March 2017. The case was tried over a six-day period and became a battle of experts. In the end, however, the jury felt MLMIC's ob-gyn policyholder did not deviate from the standards of care in his treatment of the plaintiff. This was highlighted by the fact that the jury took less than 30 minutes to return a unanimous defense verdict.

A Legal & Risk Management Analysis

This is a case that could have resulted in a million-dollar verdict, but, instead, the defense was successful for both the MLMIC-insured ob-gyn and his medical group. This victory can clearly be attributed to the proper intake and documentation of the plaintiff's family health history during her continued care.

Obtaining an accurate family health history from a patient is an effective tool for physicians and other healthcare practitioners, as it provides for a more comprehensive approach to the overall care and treatment of the patient. In this case, it was the plaintiff's failure to provide an accurate family health history that caused a direct delay in her treatment and timely diagnosis. Specifically, this failure prevented the practitioners from identifying that the patient was at

a higher risk for disease, and as a result, the ob-gyn had no reason to visualize her ovaries during the transvaginal ultrasound. This omission resulted in the ob-gyn not recommending treatments, genetic testing, or any other options that could have reduced the risk of the disease; not recognizing the early warning signs of the disease; and also not developing a plan for any appropriate lifestyle changes.

This victory can clearly be attributed to the proper intake and documentation of the plaintiff's family health history during her continued care.

A common tool used in obtaining a patient's medical history is a family history questionnaire or checklist. This approach allows the patient to complete the questionnaire at his or her own pace, allowing for extra time to communicate with family members, and ultimately provides for more accurate intake of information, which, in turn, can be followed up on by the healthcare provider. Another recommended approach is questioning the patient directly. Not only does this encourage communication, it also allows for the clarification of anything that may be unclear to the patient.

In the case at hand, both these approaches were used and effectively established that the patient denied any relevant family history. This denial went on for approximately 14 months and involved three different providers. It was not until after there was a significant finding at Memorial Sloan Kettering that the plaintiff reported an extremely relevant medical family history.

If even one of the providers had failed to document the plaintiff's family medical history, there would have been a significantly greater chance of her attorney successfully arguing that the plaintiff had never been questioned or, possibly, that the plaintiff had actually reported a positive past medical history to the provider with missing documentation. This would have given counsel a greater chance in proving some of the allegations of this case in front of a jury.

Helen Granich is a Regional Claims Manager for MLMIC Insurance Company

hgranich@mlmic.com

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

mmarkovic@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.

linkedin.com/company/mlmic

@MLMIC

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

twitter.com/mlmic

MLMIC Healthcare Weekly

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

MLMIC.com/healthcare-weekly

Underwriting Update

REMINDER: Adjusting Policy Coverage from Prior COVID-19-Related Accommodations

MLMIC Insurance Company wishes to remind its policyholders of the importance of ensuring that their professional liability coverage properly reflects their current practice status.

MLMIC immediately recognized the impending changes to the practice environment that resulted in reduced office hours and/or the cessation of elective surgical procedures.

In response to the COVID-19 crisis, MLMIC immediately recognized the impending changes to the practice environment that resulted in reduced office hours and/or the cessation of elective surgical procedures. Consequently, premium relief options were developed and offered to policyholders. These options included the suspension of practice, the reduction of coverage from a full-time to a part-time basis, and the reduction in surgical specialty class to a nonsurgical class.

As stay-at-home restrictions have been relaxed and hospitals and surgical centers are allowing for the return of elective surgical procedures, it is essential that policyholders review their coverage and contact MLMIC in writing should any adjustments be required.

The following instructions are provided to assist MLMIC policyholders who adjusted their coverage in response to COVID-19 with reverting their policies to their pre-COVID-19 status.

It is essential that policyholders review their coverage and contact MLMIC in writing should any adjustments be required.

Returning to Full-Time Practice

Prior to returning to full-time practice, policyholders who had their policies endorsed to part-time practice (20 or less hours per week) are required to notify MLMIC in writing (**click here** and select the Policy Inquiry dropdown item) with their request to have their policies endorsed back to full-time coverage. The desired, prospective effective date of this policy change must be specified.

A policyholder's neglect to notify MLMIC in writing of his or her return to full-time practice may

result in coverage issues for the time frame in question.

Returning from a "Suspension of Practice"

For those policyholders who had requested and received a "suspension of practice" endorsement *(Temporary Leave of Absence Endorsement)* to their policies due to the temporary discontinuance of providing professional services, it is important to be aware that MLMIC was obligated to notify policyholders' certificate of insurance (COI) holders of this suspension. **This notice would have clearly stated that no coverage is afforded for Professional Services rendered during the suspension period.**

It is imperative that these policyholders **notify MLMIC in writing prior to their return to practice** (**click here** and select the Policy Inquiry dropdown item) with a request to have a *Temporary Leave of Absence Reinstatement Endorsement* issued to their policies. The request must specify the desired effective date for this change. Reinstatement notices will be sent to all active COI holders commensurate with the issuance of the *Reinstatement Endorsement*.

UNDERWRITING SUPPORT

For questions regarding returning from a "suspension of practice," returning coverage to full time, or any other policy-related matters, MLMIC Underwriting staff is available to assist. Please call us at **(800) 275-6564**, or **click here** to contact MLMIC electronically.

Online Premium Payment Options

MLMIC Insurance Company is pleased to announce the availability of Simple Pay, a new option at **MLMIC.com** that allows premium payments to be made without logging in to a policyholder's portal.

Additional payment options that are available by accessing a policyholder's account via his or her **MLMIC.com** portal include Automated Clearing House (known as "ACH") capability, which allows for paperless payments made directly from a bank account, and the ability to make premium payments with a credit card.* ACH payments process more quickly than traditional payments and are more secure.

We encourage our policyholders and their administrators to take advantage of these expeditious payment options when the policyholder's next premium installment is due.

Credit card payments incur a 3% surcharge fee. ACH payments are available with no added fee. Additional payment options are available **here.*

COVID-19: The Necessity and Benefits of Updating Your Consent Forms

Reopening your practice during the COVID-19 pandemic requires a great deal of planning and consideration to ensure the safety of your patients and staff, as well as to protect yourself from legal liability. One important way to do so during this unprecedented time is to review and update your consent forms to ensure that you cover topics related to COVID-19.

There are two fundamental reasons to review and update your consent forms at this time: the risk of COVID-19 exposure and the expanded use of telehealth to deliver healthcare.

One important way to do so during this unprecedented time is to review and update your consent forms to ensure that you cover topics related to COVID-19.

It is important to first consider that "consent" actually refers to the communication between the appropriate healthcare provider and the patient, and the "consent form" fulfills the legal requirement of documenting it. This being so, it is essential that the consent discussion take place between the appropriate parties (normally a physician and patient) and the discussion cover the key points on the consent form.

FAKS attorneys can assist in providing additional useful information and work with you to tailor consent forms for your practice.

In general, a thorough consent form is preferable, as a consent form that shifts the burden to the healthcare provider can be problematic. FAKS attorneys can assist in providing additional useful information and work with you to tailor consent forms for your practice.

Exposure to COVID-19

As your practice reopens, you should be aware of the possible risk of exposing patients and staff to COVID-19. As part of your reopening strategy (for guidance on reopening strategies, see **MLMIC/MedPro Checklist**), the risk of exposure to COVID-19 should be communicated with patients verbally and documented on a consent form as well as in the patient record. A consent form that informs a patient of the risk of exposure to COVID-19

just by coming in for a visit can (along with following CDC and DOH guidelines and the standard of care) help minimize legal liability exposure for both the patient and potentially third parties.

Sample consent forms for documenting the risk of COVID-19 exposure are available to MLMIC policyholders at no cost by **contacting** Fager Amsler Keller & Schoppmann, LLP (FAKS). FAKS attorneys can also assist you with other questions related to consent issues.

Expansion of Telehealth

The COVID-19 crisis has resulted in the expanded delivery of healthcare using telehealth, which uses technology that limits the delivery of healthcare and also poses possible performance issues, including audio/video quality, platform privacy, and diagnostic limitations.

While a consent for telehealth is not currently required by law, it is important that these limitations and possible technological issues be communicated to the patient before the telehealth encounter, verbally, by documentation in the patient record, and, if possible, on a consent form (conditions permitting).

The COVID-19 crisis has resulted in the expanded delivery of healthcare using telehealth.

A consent form that advises the patient about the possible limitations of telehealth, combined with proper documentation and following the standard of care, can help minimize legal liability.

As a value-added service for its policyholders, MLMIC has partnered with the law firm of Fager Amsler Keller & Schoppmann, LLP (FAKS), to follow legal issues related to COVID-19 and advise MLMIC policyholders on these legal issues both during and after the crisis. MLMIC policyholders may **consult with** FAKS attorneys on these, and other healthcare issues, at no additional cost.

Check out our blog at MLMIC.com

Read about important developments in professional medical and dental liability, get risk management tips, and sign up for MLMIC Healthcare Weekly.

New York City
2 Park Avenue
New York, New York 10016
(212) 576-9800
(800) 275-6564

Latham
8 British American Boulevard
Latham, New York 12110
(518) 786-2700
(800) 635-0666

Long Island
90 Merrick Avenue
East Meadow, New York 11554
(516) 794-7200
(877) 777-3560

Syracuse
2 Clinton Square
Syracuse, New York 13202
(315) 428-1188
(800) 356-4056

Buffalo
300 International Drive
Suite 100
Williamsville, New York 14221