MLMIC

Dateline

VOLUME 14

NUMBER 1

spring 15

A NEWSLETTER FOR MLMIC-INSURED PHYSICIANS & FACILITIES

MLMIC.com

Dateline **is published under the auspices of MLMIC's Patient Safety & Education Committee, Donald J. Pinals, MD, Chairperson.**

Editorial Staff

John Scott, Editor
Frances Ciardullo, Esq.
Kathleen L. Harth
Matthew Lamb, Esq.
Robert Pedrazzi
Donnaline Richman, Esq.
Daniela Stallone
Linda J. Trentini, CIC
Michael Zeffiro, Esq.

Breach Notification Under HIPAA—When Health Information is Compromised

Laurel E. Baum, Esq.
Hancock Estabrook, LLP

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual." So stated Chief Justice Earl Warren in 1963, well before the Health Insurance Portability and Accountability Act of 1996 (fondly, HIPAA) became a household word.[1] Despite Justice Warren's forewarning, it is doubtful that even he could have imagined the extent to which our personal information, including our health information, now resides and moves in an electronic environment.

Certain provisions of HIPAA were fashioned to promote the electronic interchange of health information with the goal of increasing healthcare, payment efficiencies, and, ultimately, it is hoped, patient well-being. The sheer proliferation of electronic health information, however, requires additional protections. Obligations to safeguard Protected Health Information (PHI) arose because of concerns that electronic access and transmission of information increased the susceptibility of PHI to unauthorized use and disclosure. Thus, to help protect PHI in an electronic environment, HIPAA established a floor of privacy and security protections which cover PHI in any media, from ePHI to handwritten notes.

Background

By now, it is well understood that protecting the privacy and security of patient information is a responsibility of every "covered

1. Lopez v. United States 373 U.S. 427 (1963).

continued on page 8

Reflections on Being a Defendant in a Medical Malpractice Case

The following article was submitted by a MLMIC policyholder who wished to remain anonymous.

At a county medical society meeting in September of 2012, I heard a MLMIC representative say, "It's lonely to be a defendant in a medical malpractice case." Truer words were never spoken.

From the beginning of my recent experience as a defendant in a malpractice case, I decided I would use this as a learning tool, for me and for others. I made the conscious decision not to shout my being sued from the rooftops, but not to make any attempt to hide

continued on page 16

Physician Office Practice Surveys: Findings and Recommendations—Part II

Bonnie Paskewich, RN
Director, Long Term Care Facilities
MLMIC Risk Management

Mark Ambrose, RN
Risk Management Consultant
MLMIC Risk Management

Introduction

As part of the ongoing Risk Management activities performed by Medical Liability Mutual Insurance Company (MLMIC), 43 medical office practice surveys were conducted over the past two years. These surveys were conducted at the request of both individual insured physicians and various MLMIC committees. The offices surveyed included numerous primary care, surgical, and specialty practices. The surveys focused on several areas, including: general office appearance; personnel; office protocols; billing/collection practices; medication control; appointment scheduling; dismissal of patients from care; medical records; telephone coverage; and office equipment. The first five areas of concern were addressed in the Fall 2014 issue of *Dateline.* Here we will focus on, and offer solutions to, the subsequent five areas of concern.

1. Safety

There were a total of 40 recommendations made with respect to overall safety. An essential part of minimizing liability risk is keeping patients, visitors, and staff free from harm. Patient identification errors occur at all stages of treatment. A written policy and procedure for the use of a "two patient identifier" system will decrease the possibility of these types of events.

An effective biomedical program should be in place for the proper maintenance of all medical equipment. A written policy and procedure should indicate which equipment is subject to safety and performance testing. A signed contract should be on file when using outside biomedical engineers. New equipment should be inspected prior to being placed in service. All medical equipment should be inspected and calibrated by a biomedical engineer on an annual basis, or more often if recommended by the manufacturer. All equipment should have a visible sticker indicating the date it was last inspected, the initials of the inspector, and the date when the next inspection is due. A log of these service checks should be maintained. All staff utilizing any equipment need to be properly trained on its use and documentation of their training should be kept in their employment files.

A policy and procedure must address any clinical equipment involved in an actual or potential adverse patient outcome. The involved equipment should immediately be sequestered to prohibit reuse or tampering. MLMIC should be notified of any serious events and before any sequestered equipment is sent for inspection. Any clinical equipment that malfunctions and is not involved in a serious event should be immediately removed from service, tagged "not for use," and inspected or repaired by a biomedical engineer who is able to replicate the malfunction before repairing it.

Offices with Automated External Defibrillators (AED) need to perform and document monthly inspections, including verification that the pads have not expired and are ready for use.

If autoclaves are used, they must be maintained per manufacturer recommendations. Spore testing also needs to be performed and documented when autoclaving. When gas cylinders, including oxygen tanks, are used, they should be secured to a wall or stored in an approved storage rack, stand, or cart at all times. They should also be checked periodically to insure that they are adequately filled.

Good hygiene practices decrease the spread of infections. Infection control policies should address procedures to reduce cross contamination. All surface areas must be cleaned with an approved disinfectant after each patient encounter. Clean and dirty items must be stored in separate areas and not stored under sinks. All infectious waste should be stored in a covered container and be appropriately labeled as "infectious/biohazard" waste. Sharps containers should be tamper proof, locked, and mounted out of the reach of children, but easily accessible to staff. Safe needle devices that cannot be tampered with or removed should be utilized. We do not recommend accepting used sharps from patients for disposal. For further suggestions on infection control and safe sharp handling, go to www.oneandonlycampaign.org.

Slips, trips, and falls are risks for patients, visitors, and staff. Sidewalks need to be maintained and floors should be dry. Caution signs should be used when they are wet. Rugs should be secure, smooth, and flat to the floor, with no frayed edges. If electrical cords are on the floor, they should be properly secured. The hallway should be kept clear and any equipment must be stored to one side of the hall.

The waiting room must be visible to staff at all times. For patients of size, there needs to be seating and equipment inconspicuously coded with weight limits throughout the office, as well as a system in place to identify patients of size.

2. Medications

There were 39 recommendations made related to this topic. Medications have been found to be responsible for a significant number of adverse events. To prevent such errors, practices should focus on medications used in the office setting, medication reconciliation, sample medications, and the storage of prescription pads. Prescription pads are the responsibility of the prescriber and must be locked in a secure area.

A written policy and procedure should be developed to address monthly inspections for expiration dates of office medications and other outdated supplies such as syringes and alcohol prep pads. All medications need to be stored in a securely locked area.

Refrigerators for medication storage are to be kept separate from food, specimens, and laboratory supplies. A daily log should be maintained indicating the refrigerator temperature. If there is no generator backup, there should be an alert system in place to ensure that all medications have remained within an acceptable temperature range in the event of a power outage. A written policy and procedure should detail this practice.

The use of single dose vials is encouraged. Any multi-dose vials or bottles should be properly labeled and checked for expiration dates. No prefilled syringes should be used unless packaged and labeled by the manufacturer in unit dose measures.

There should be a written policy and procedure outlining the medication reconciliation process, which is the responsibility of a licensed professional (registered nurse, mid-level practitioner, or physician). A licensed practical nurse may list the patient's medications in the medical record. However, the physician or mid-level practitioner must verify the medication list with the patient. Medical assistants cannot perform this function. A medication list should be maintained separate from the encounter notes and should be updated at each visit. The list should contain all prescription medications, OTC medications, and herbal supplements. The name of the medication, dose, frequency, prescriber, date prescribed, and the date the medication was discontinued should also be documented. A separate list of immunizations should also be maintained and reviewed at regular intervals.

Sample medications should be dispensed only by providers. Medications must be labeled according to the prescriber's order, with the same labeling requirements as a pharmacy, in accordance with NY State Education Law § 6807(1)(b). There must be a visible patient name, date, route, frequency, and total number or volume noted on the label. Alerts such as "may cause drowsiness" should also be noted on the package. The same information that is on the label must be noted in the medical record as well as in the patient education information that was provided to the patient.

All sample medications should be stored in a securely locked area. There should be a formal, written process for the inventory and maintenance of all sample medications, including the name, lot number, number of samples, and their expiration dates. Expiration dates should be checked and documented on a monthly basis. Expired drugs should be disposed of in accordance with regulations or returned to the manufacturer. A log should be kept when medication samples are dispensed or disposed of and when any medications are delivered to the office by the pharmaceutical representatives, who should not be allowed in the sample medication area without direct supervision.

3. HIV

There were 33 recommendations made regarding the request for medical records containing HIV information. A written policy and procedure should be developed to guide staff on how to respond to these requests. The policy should include the requirement of specific patient consent for the release of HIV-related information and the prohibition against

continued on page 4

re-disclosure of such. If you receive a subpoena for medical records containing HIV-related information, you should contact the attorneys at Fager Amsler & Keller, LLP for advice on how to address the release of this information. All records containing HIV-related information should contain confidential coding to alert staff that this information should not be released without specific patient consent or an appropriate court order. A notice of prohibition against redisclosure must accompany the release of all HIV information.

4. Confidentiality

There were 29 recommendations addressing confidentiality issues. Each record should contain a signed Notice of Privacy. The Notice of Privacy practices should include permission to leave a message on the patient's answering machine or voicemail. A signed privacy consent should be present in the chart for the use of emails and the use of post cards that contain the patients' and providers' names. Patients should be asked to identify the names of any family members or friends with whom health information can be shared. Fax cover sheets also need to include a confidentiality statement.

All records should be kept in a secure area. Computer systems must be password protected. Passwords should be changed on a routine basis, and the passwords of former employees should be deleted immediately. Computer work station screens should not be visible to patients and/or visitors. Computers that are logged in should not be left unattended.

Always remember that noise can travel. It is recommended that staff speak at a low volume to maintain confidentiality.

A written policy and procedure should be developed to address the handling of legal paperwork received, such as a subpoena or a summons and complaint. The procedure must include immediate notification to the involved provider. Designate the appropriate person (CEO, administrator, medical director, office manager) responsible to receive legal paperwork. When a record is released, there must be a log (electronic or written) maintained of when and to whom it was released. Always obtain the written consent of minor patients before releasing medical records containing information about their reproductive issues, including STDs.

Patient education, opportunities to ask questions, and the consent must take place prior to the administration of any medication that could impact judgment.

5. Informed Consent

Twenty-one recommendations were made in this category. The duty to provide informed consent rests with the provider and is a non-delegable duty. Therefore, the treating provider must obtain the actual informed consent, but office staff can witness the patient's signature on the form. A policy should be developed that outlines your consent process. Fager Amsler & Keller, LLP offers consent forms that can be used for many procedures. A separate consent for anesthesia must be signed by the patient in the presence of the provider. Patient education, opportunities to ask questions, and the consent must take place prior to the administration of any medication that could impact judgment. The discussion about the risk, benefits, and alternatives to the proposed treatment, including the option of no treatment and the risks of the alternatives, should be documented in the record.

Conclusion

There are many risk management strategies that providers and practices can implement to decrease the potential risk of liability and improve patient safety in the office practice setting. The office surveys conducted by MLMIC found that the highest number of recommendations were made in two areas.

The first was the need to develop a practice specific policy and procedure manual. The manual needs to remain up-to-date and reflect current standards of care. Staff should be continually educated about these guidelines. Consistently following these policies and procedures will reduce the risk of professional liability for providers and practices.

The second is the need to establish and maintain personnel files to support the verification of an employee's credentials. Human Resource files should contain background and reference checks, license verification, signed confidentiality agreements, up-to-date job descriptions and training, and performance appraisals. This demonstrates that you have confirmed the quality and competence of both newly hired and long-tenured employees.

Adoption of these recommendations will assist in the development of a well-rounded risk management program that can reduce the risk of patient injury. In the event of litigation, they will also contribute to a strong defense.

Our medical office practice surveys can help improve patient care and reduce the risk of claims that may arise in the physician office setting. An on-site review and evaluation of individual office practices and procedures may be conducted by our Risk Management Consultants, with recommendations to improve the practice provided upon completion of the survey. Requests for this service can be made either through our website, MLMIC.com, or by calling the Risk Management Department at the MLMIC office closest to your location. These services are provided at no cost to MLMIC policyholders. ❖

Case Study

Poor Patient Selection for Abdominoplasty

William F. Fellner
Assistant Vice President, Claims
Medical Liability Mutual Insurance Company

The 69-year-old obese female plaintiff had a history of abdominal liposuction, chin liposuction, and bariatric (gastric sleeve) surgery, all without any complications.

Two years after the gastric sleeve procedure, the plaintiff consulted with the defendant plastic surgeon about undergoing breast reduction surgery. At the initial consultation, the defendant allegedly advised her that a more pressing issue was her excessive abdominal skin due to her weight loss after the gastric sleeve surgery. At this initial visit, the plaintiff was 5' 1" tall and weighed 161 pounds. During a physical examination of the plaintiff's abdomen, the defendant discovered what was believed to be a hernia and referred her to the co-defendant, a general surgeon. He advised the plaintiff that if she had a hernia, it could be repaired during the abdominoplasty procedure. The defendant had a close working relationship with the co-defendant. There was no further discussion between the plaintiff and defendant about her undergoing breast reduction. The defendant plastic surgeon documented the examination on forms belonging to other physicians who shared the defendant's office but were not part of his practice. The defendant additionally met with the plaintiff at his home to discuss this surgery.

The patient saw the recommended co-defendant general surgeon, who was not insured by MLMIC. Although he did not observe a clear defect, he did identify a weakness at the midline of the plaintiff's abdomen, along the sides of the rectus sheath. The co-defendant advised the plaintiff that she might benefit from the placement of mesh over her abdominal musculature, to reinforce the area following the abdominoplasty. He said he would work closely with the plastic surgeon. He discussed with her the risks, benefits, and alternatives to this procedure and documented that he had done so. He also advised the plaintiff that she needed to obtain medical clearance prior to undergoing this procedure.

The plaintiff obtained all required medical clearances and underwent the surgery in a hospital. An incision was made by the defendant plastic surgeon around and below the umbilicus. Lateral and superior dissection created extensive flaps for the abdominoplasty. The defendant then corrected the *diastasis recti* and tightened the abdominal wall by placing interrupted horizontal sutures. Following the defendant's repair of the *diastasis*, the co-defendant general surgeon examined the abdominal fascia and placed mesh without difficulty. Once the mesh was in place, the plastic surgeon completed the procedure by excising the excess skin and fat from the abdominal flap and approximating the wound edges. The defendant then proceeded to perform liposuction to the plaintiff's thighs, removing approximately 450 milliliters of adipose tissue from each thigh without difficulty. At the conclusion of the procedure, the plaintiff appeared to be in stable condition. She was extubated and taken to the recovery room.

The operative report of the co-defendant, which was generated on the day of surgery, indicated that both procedures were completed without difficulty. However, the defendant did not dictate an operative report immediately after the surgery. He waited until 6 weeks after the procedure was performed to dictate his report.

The plaintiff's first post-operative day was relatively uneventful. However, during the early morning hours of the second post-operative day, the plaintiff's oxygen saturation levels began to decrease. She was given six liters of oxygen via nasal cannula to maintain a 90% oxygen saturation level. By mid-morning, however, the nasal cannula had to be replaced by a face mask. Shortly thereafter, the plaintiff was noted to be tachypneic, with an oxygen saturation level of 89%. A chest x-ray revealed atelectatic changes at the base of both lungs and mild central pulmonary vascular congestion. There was no evidence of pneumonia or congestive heart failure, but a pulmonary embolus had not been ruled out. The plaintiff's laboratory test results revealed a significantly elevated creatinine level of 2.6. The defendant wanted to intubate the plaintiff to "relax" her for several days, believing that the plaintiff's oxygen saturation and creatinine levels would both improve. However, the co-defendant recognized the seriousness of the plaintiff's condition. He recommended that she be promptly transferred to a facility with more appropriate intensive care capabilities.

By late afternoon, the plaintiff had been transferred to the ICU of another hospital. Upon her arrival, she was intubated and her oxygen saturation and kidney function levels remained stable. A sonogram ruled out the presence of a

continued on page 6

Case Study

continued from page 5

deep venous thrombosis. Bladder pressures were in the low 20's. Abdominal compartment syndrome was the suspected cause of these complications. For the next two days, although plaintiff's oxygen levels and kidney function did not decrease, they did not show significant improvement. Therefore, the co-defendant emergently returned the plaintiff to the operating room, but without the assistance of a plastic surgeon. When the co-defendant opened the plaintiff's abdomen, her oxygen saturation levels and bladder pressures rapidly improved. She remained hospitalized for the next 10 days, during which time she was followed solely by the co-defendant. She was visited only on one occasion by the defendant plastic surgeon.

The plaintiff commenced litigation against both the defendant plastic surgeon and the co-defendant general surgeon. She alleged that the plastic surgeon did not adequately and properly examine her prior to performing the abdominoplasty. She further alleged the defendant failed to give due consideration to her history of prior liposuction, gastric sleeve surgery, weight problems, and underlying medical conditions, prior to determining whether she was an appropriate candidate for abdominoplasty. She also complained that an abdominoplasty was not why she originally came to see the defendant. The plaintiff alleged that the defendant had placed the abdominal sutures too tightly, resulting in severe oxygen deprivation which necessitated emergency surgery. The plaintiff further alleged that both defendants provided inadequate and inappropriate postoperative care, including: failing to address her pain and breathing difficulties in a timely manner; failing to consider the cosmetic consequences in their postoperative treatment decisions; and, most critically, failing to diagnose abdominal compartment syndrome in a timely manner. The damages claimed by the plaintiff included: deformity and disfigurement of the abdominal area; severe diastasis recti; ventral and umbilical hernias; dental trauma; vision loss; cognitive impairment due to oxygen deprivation; vestibular trauma; and aggravation of her underlying medical conditions.

Multiple experts reviewed this case for MLMIC on behalf of the insured defendant. The MLMIC plastic surgery expert expressed serious reservations regarding the defensibility of the matter. He opined quite strongly that abdominoplasty is not the procedure of choice for an obese patient. The plaintiff was not an appropriate patient for this procedure, which is typically performed on thinner patients with excess abdominal skin, rather than patients who have a significant amount of abdominal adipose tissue. Because the plaintiff was obese, she should have undergone additional weight loss before being accepted for such a procedure. This expert expressed serious concern as well about the significant and obvious antagonism between the two defendants, which would certainly be revealed at trial. Finger-pointing between defendants clearly makes defense of a lawsuit more difficult.

The internal medicine expert who reviewed this case had specific expertise in cardiology. He opined that the plaintiff's difficulty in breathing post-operatively was directly related to the fact that the abdominoplasty sutures were too tight. He stated that the plaintiff's anesthesia record fully supported this conclusion. During the first portion of the surgery, the plaintiff's systolic blood pressure was in the 120's. However, at the mid-point of the procedure, the systolic blood pressure consistently began to decrease, until it stabilized in the 90's. The decrease in the plaintiff's systolic blood pressure directly coincided with the tightening of the abdominal sutures. He stated that tightening the sutures would decrease the venous return to the upper half of the plaintiff's body and thus decrease her blood pressure. Finally, the operative report from the second surgery confirmed that, once the sutures were removed, the plaintiff's oxygen saturation rapidly improved. These two factors, in conjunction with the changes in her bladder pressures, provided clear evidence that the plaintiff had abdominal compartment syndrome. Finally, this expert was very concerned that the defendant's resistance in transferring the plaintiff to a hospital where she could receive proper intensive care caused the defendant to appear either unable to recognize the seriousness of the plaintiff's quickly deteriorating condition or strangely out of touch with the plaintiff's acute medical needs.

Because of these many serious deficits in the defendant's care, as well as poor communication, settlement discussions were undertaken. The plaintiff initially demanded $12 million dollars to resolve the suit. Due to this excessive demand, and MLMIC's opinion that the plaintiff's damages were worth significantly less money, the parties discussed the possibility of mediation. Although the plaintiff agreed to mediation, the carrier for the co-defendant general surgeon declined to participate in this process. Despite that, MLMIC proceeded to mediate the case on behalf of the defendant plastic surgeon. An initial offer of $350,000 was made to the plaintiff. Unfortunately, because little progress was made, the mediation process ended without resolution of the case. However, settlement discussions between MLMIC and the plaintiff continued over the course of the next several weeks. The matter was finally resolved for $725,000 on behalf of the MLMIC defendant plastic surgeon. The case against the co-defendant general surgeon by the plaintiff, however, continued.

A Legal & Risk Management Perspective

Donnaline Richman, Esq.
Fager Amsler & Keller, LLP
Counsel to Medical Liability Mutual Insurance Company

There were numerous risk management and legal issues which contributed both to the plaintiff's injuries as well as the need to settle rather than defend and litigate this lawsuit.

The key deficit in this plaintiff's care, according to the physician experts who reviewed the case, was improper patient selection. The plaintiff was 69 years old and had diabetes and hypertension. Her weight also made her a less than ideal candidate to undergo an abdominoplasty. The MLMIC defendant plastic surgeon should have seriously considered all of those factors prior to accepting the plaintiff for this surgery. In fact, the patient had not even requested abdominal surgery. She had come to the defendant to discuss breast reduction surgery. When a patient is improperly selected for a surgical procedure, or is influenced to undergo a procedure other than what was originally sought, it increases the possibility of the patient suffering a serious complication. Merely because a patient wants plastic surgery or another procedure does not mean that the physician should accede to the patient's wishes. Poor patient selection often leads to increased risk and physician liability. Further, possible undue influence to choose one procedure over another, which the patient had requested, could potentially result in disciplinary action by OPMC.

Compounding the problem, the defendant apparently did not provide nor document a detailed informed consent discussion in either the pre-operative office or hospital notes. He should have discussed with the patient the risks, benefits, and alternatives, including not undergoing this procedure, as well as the risks of the alternatives, and documented that this discussion had taken place. The defendant should have specifically noted that he advised the patient that she was not a good candidate for this surgery.

According to the experts who reviewed this case, the defendant's overall documentation was extremely poor. If he had documented fully and accurately in his record, it may have been possible to defend this suit. However, the pre-operative notes were both sparse and poorly written. Although the operative report was well-written and highly detailed, it was not at all credible because the defendant delayed dictating the operative note for 6 weeks. By that time, the patient had already suffered the surgical complications. Thus, the notes were written in a highly defensive manner because the defendant well knew what problems had occurred. Further, it was highly unlikely that, after 6 weeks, all of the information contained in the post-operative report was accurate. The prolonged delay between performing and documenting a procedure diminishes the credibility of the documentation. Post-operative notes must be dictated contemporaneously with the procedure.

In addition to the documentation issues which concerned the experts, apparently, the written forms used by the defendant for documenting patient history and physical

continued on page 14

Popular MLMIC CME Modules Available Online

As part of our ongoing efforts to educate our member policyholders on current healthcare law and risk management issues, we are pleased to announce that we have made available through MLMIC.com four of our most highly rated risk management CME modules: *An Interview with a Plaintiff's Attorney – Parts 1 & II* and *High Exposure Liability: Delay in Diagnosis of Breast Cancer – Parts I & II*

In *An Interview with a Plaintiff's Attorney – Parts 1 & II*, a prominent plaintiff's attorney provides his perspective on a number of issues related to medical malpractice claims and litigation, including:

- Why do patients sue?
- How important is the deposition?
- How should the defendant physician prepare for cross examination?

These questions, and many more, are addressed in great detail in this video presentation.

High Exposure Liability: Delay in Diagnosis of Breast Cancer – Parts I & II feature a defense attorney, a plaintiff's attorney, physician risk management experts, and a senior MLMIC claims professional addressing the continued high frequency and severity of claims alleging a delay in diagnosis of breast cancer. They share their experiences in handling breast cancer claims, focusing on the key issues that can impact the outcome of these cases while offering suggestions to help prevent future claims.

To learn more about MLMIC's CME modules, including how to register and view them, please visit MLMIC.com or call MLMIC's Risk Management Department at (212) 576-9601. ❖

entity." Covered entities include healthcare providers who conduct certain electronic financial and administrative transactions (i.e., electronic claims submission).[2]

Unfortunately, PHI can become compromised in an instant: lost or stolen laptops, jump drives, iPhones, and other external portable devices; misdirected faxes, emails, and regular mail; workforce members improperly accessing (a/k/a "snooping") PHI within an organization; posting PHI without authorization on social media; texting patient photos; conversing about patients in public places; and the list goes on and on. When protections fail and the PHI is compromised, HIPAA requires covered healthcare providers to notify affected patients, the Secretary of Health and Human Services (HHS), and, if the breach involves 500 or more individuals, the media. Similarly, a covered entity's "business associate" must notify the covered entity of such breaches.[3]

Before proceeding, it is critical to distinguish between "use" and "disclosure." Simply stated, a "use" of PHI occurs within the organization and a "disclosure" occurs when PHI is released or transferred outside the entity holding the PHI.[4] Breaches can occur involving both uses and disclosures, and knowing the difference is essential to determine how to approach a breach risk analysis.

Responding to a Suspected Breach

The first and most important piece of advice is to prepare now, before a breach occurs. A medical practice, hospital, or other covered entity should already have a process in place requiring staff to immediately notify the organization's privacy official (or other designated personnel) of any suspected breach of PHI. The organization's culture should be one in which staff are comfortable bringing HIPAA concerns to senior leadership's attention without fear of retaliation. Policies and procedures must be in place now to perform a breach risk analysis and to provide breach notification, if and when required.

Once an issue is reported, the covered entity must determine rather quickly whether a reportable breach has occurred, since not every violation of HIPAA amounts to a breach of PHI. Only a breach of "unsecured" PHI must be reported. Unsecured PHI means that the information has not been made unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology specified by HHS in published Guidance.[5] However, if PHI is secured in a manner set forth in the Guidance (by encryption, for example), then no breach notification is required following an impermissible use or disclosure.

A reportable breach is one where the unauthorized acquisition, access, use, or disclosure of PHI compromises the security or privacy of PHI.[6] However, three instances are specifically excluded from the definition of a "breach" and you must determine whether any of these exceptions apply to a given situation:

2. To determine if your organization is a HIPAA covered entity go to: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/AreYouaCoveredEntity.html.
3. A business associate is generally defined as a person or entity who, on behalf of a covered entity, performs certain activities involving the use, access, disclosure, maintenance, of the covered entity's PHI. The term "business associate" does not include members of the covered entity's workforce. 45 CFR 160.103.
4. "Use" means the sharing, employment, application, examination, or analysis of PHI within an entity maintaining the PHI, whereas "disclosure" is defined as the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. (45 CFR 160.103).
5. http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.
6. Prior to March 26, 2013, whether a breach occurred depended on whether there was a risk of reputational, financial or other harm to the patient as a result of the unauthorized use or disclosure of the PHI. That standard has been repealed and replaced with an analysis of whether the PHI has been compromised. (Effective date for the new standard was March 26, 2013, with a compliance date of September 23, 2013).

1. Unintentional acquisition, access, or use of PHI by an employee or other person acting under authority of the covered entity (or business associate) if such acquisition, access, or use of PHI was made in good faith and within the course and scope of the employment relationship with the covered entity/business associate and such information is not further acquired, accessed, used, or disclosed by any person.
2. Inadvertent disclosure of PHI from one person authorized to access PHI at the covered entity to another similarly situated person at the covered entity, as long as the PHI is not further acquired, accessed, used, or disclosed without authorization.
3. Unauthorized disclosures in which an unauthorized recipient of the PHI would not reasonably have been able to retain the PHI.

Even if an event falls within one of the exceptions, you must fully investigate the situation to determine exactly what happened. You may not have to provide breach notification if an exception applies, but in a robust HIPAA compliance program, preventing similar occurrences is key, for the next time you may not be so lucky.

Conducting the Breach Risk Analysis

Prior to September 23, 2013, breach notification was required only if a covered entity concluded that an unauthorized use or disclosure of PHI posed a risk of reputational, financial, or other harm to the patient. This arguably subjective analysis is no longer the legal standard. Now, the focus is on the data itself, and the sole question is whether the PHI has been "compromised." More to the point, an acquisition, access, use, or disclosure of PHI in a manner not allowed under HIPAA is presumed to be a breach unless the covered entity shows there is a low probability that the PHI has been compromised.

Hypothetical #1: *It is a particularly busy day for your primary care practice. An employee intends to fax patient information to a local hospital's outpatient clinic. Unfortunately, in haste, the wrong fax number is used and the document is faxed to the wrong party. Later in the day, the unintended recipient calls to tell you of the mistake, explaining that after she glanced at the fax, she realized it was not hers.*

What do you do if faced with this situation? Clearly, the misdirected fax does not fall within one of the three exceptions outlined above. Moreover, the faxed information is "unsecured PHI." You must decide whether you are required to notify anyone of the breach.[7] Your obligation hinges on whether there exists a "low probability" that the PHI has been compromised, in which case breach notification is not required. Therefore, you must perform a breach risk analysis with consideration of at least the following four factors to determine whether or not there is a "low probability" the PHI has been compromised:[8]

1. **The nature and extent of the PHI involved, including the types of identifiers and the likelihood the information can be re-identified.** In the above hypothetical, the practice would need to determine the type of information included in the fax. Did the fax include the patient's name and social security number (a high risk)? Or was the information limited to an appointment reminder to a general practitioner (arguably a lower risk)? Was medical information disclosed (in many instances, a higher risk)?
2. **The unauthorized person who used the PHI or to whom the disclosure was made.** Who is the unintended recipient of the fax? For example, if the fax was sent to another HIPAA-regulated entity,

7. Note: Because uses and disclosures of PHI in violation of HIPAA are presumed to be a breach, covered entities may proceed directly to breach notification without conducting a breach risk analysis. We generally do not recommend this approach, as it may result in alarming patients unnecessarily and may also expose the covered entity to increased liability.

8. 45 CFR 164.402.

continued on page 10

you may find a lower probability that the PHI has been compromised since the recipient of the information is obligated to abide by HIPAA and/or other privacy laws. On the other hand, if the unintended recipient has no such obligation, it may be more difficult to find a "low probability" that the information has been compromised.

3. **Whether the PHI was actually acquired or viewed.** In our hypothetical, the unintended recipient reported glancing at the fax—so put a check mark next to this factor. In some situations, however, the covered entity may determine that although PHI was provided to the wrong person, he or she could not have viewed or acquired the information. For example, if during the hospital discharge process, a nurse inadvertently hands patient A's discharge instructions to patient B but quickly realizes the mistake and immediately retrieves the document, it may be reasonable to conclude that patient B did not have time to review the other patient's PHI.
4. **The extent to which the risk to the PHI has been mitigated.** In our hypothetical, this might involve reaching out to the unauthorized fax recipient to obtain satisfactory assurances (through a confidentiality agreement or similar means) that the PHI was not further used or disclosed but instead has been destroyed or returned in full to the covered entity.

The results of this analysis will determine whether breach notification is required in the above hypothetical. If, after your investigation, you determine that there is a low probability that the PHI has been compromised, no breach notification is required. If, on the other hand, you cannot substantiate a determination that there is a low probability, breach notification is required.

Not all breaches involve unauthorized disclosure of PHI. As mentioned above, misuse of PHI within a covered entity may also constitute a breach. Consider the following hypothetical:

Hypothetical #2: *A hospital employee discovers his neighbor recently presented to the hospital's emergency department. On a whim, and unbeknown to the hospital, the employee decides to take a peek at his neighbor's electronic medical record (EMR) for curiosity's sake. The hospital's privacy official learns of the employee's access through routine auditing and wonders why the employee (who works in an inpatient setting) viewed the records of a patient who was never admitted to the hospital. When confronted, the employee confirms that he had no official purpose for viewing the patient's EMR.*

Here, the employee's unauthorized access to his neighbor's EMR does not fall into one of the three breach exceptions discussed above. "Snooping employees" are not covered by any exception because their "access as a result of such snooping would be neither unintentional nor done in good faith."[9]

As no breach exception applies and the PHI is unsecured, a breach risk assessment in this hypothetical would reasonably conclude that the employee's unauthorized access likely compromised the patient's PHI. If so, a reportable breach has occurred. Keep in mind, the question is whether the PHI has been compromised, not whether there is a risk of harm to the individual.

Breach Notification Process

Once you have determined that you need to report, you must decide to whom a report should be made. A great deal of information on the breach notification process is contained on the HHS, Office of Civil Rights (OCR) website, at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/.

Notice to Individuals

When a reportable breach is discovered, a covered entity must generally notify the affected individual(s) (or their personal representatives) without unreasonable delay and in no event later than 60 calendar days from the date of discovery, except in the event of a "law enforcement delay" as explained below. You should treat the breach as "discovered" on the first day the breach is known or should reasonably have been known to any of your employees or agents other than the person who committed it.

The concept of "without unreasonable delay" is important. You should not delay reporting for sixty days if a shorter time frame was possible. For example, if a laptop containing PHI is stolen, you may find it difficult to defend waiting more than a few days to report. Also, be aware that New York State breach notification laws, discussed in more detail below, may require you to report breaches of computerized data much sooner than is required under HIPAA, depending on the circumstances.

Notice to the patient must be in plain language and include a brief description of what happened, including: the date of the breach and the date it was discovered; a description of the types of PHI involved; steps the individual should take to protect him/herself from potential harm; a brief description of the actions taken by the covered entity to mitigate the harm and protect against future breaches; and contact procedures for the individual to ask questions.[10] Note that the "type" of PHI means a general description, not the actual specific infor-

9. Federal Register Vol. 78, January 25, 2013 at 5640.

10. Contact procedures include a toll-free telephone number, an e-mail address, website, or postal address. 45 CFR 164.404.

mation. For example, the covered entity would explain in the notice that a SSN or date of birth was disclosed, but would not include in the breach notification letter the actual SSN or date of birth. Do not include actual PHI in the breach notification letter in the event the letter is read by someone other than the patient or his/her personal representative.

First class mail is generally the method of notification, although you may use e-mail if agreed to by the individual. The regulations do not require the use of certified mail, but you may elect to do so depending on the circumstances. If your contact information is insufficient or out of date, you may use substitute notice, including telephone, website, or local print or broadcast media to provide notice of a breach.

Notification to the Media

If the breach affected more than 500 residents of a state or jurisdiction, the law requires you to notify major local media outlets. This, again, must be done without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, except in the event of a law enforcement delay. The content of the notice is generally the same information required for individual notice. Of course, no identifying patient information may be disclosed to the media. Notice to the media may be in the form of a press release.

Notification to the Secretary of Health & Human Services

For breaches affecting fewer than 500 individuals, the covered entity must provide notice to the Secretary of HHS annually within 60 days of the end of the calendar year in which the breaches were discovered. The notice to HHS is submitted electronically via http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

For breaches affecting 500 or more individuals, the covered entity must provide notice to HHS without unreasonable delay, and in no case later than 60 days from the discovery of the breach, except in the event of a law enforcement delay.

HHS publishes all breaches of 500 or more individuals on its website at: http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html.

Prior to publishing information about such breaches on its so-called "wall of shame," OCR will likely contact the covered entity to confirm the details. Should your organization have the unfortunate experience of a large breach, be prepared for the conversation with OCR. You should consult with legal counsel experienced in these matters prior to having a conversation with OCR so that you will be prepared and informed of the process.

Law Enforcement Delay

In rare circumstances, law enforcement may request a delay in breach notification. If a law enforcement official states to the covered entity that a required breach notification would impede a criminal investigation or cause damage to national security, the covered entity will need to delay such notification for the time period specified, if the request is in writing, or for no longer than 30 days from the date of the request if made orally. Note: if the law enforcement request is made orally, the covered entity must document the request, including the law enforcement official's identity.

Documentation

All breach-related activities and investigations, and especially the risk analysis, must be thoroughly and timely documented. Retain this information for at least six years in your organization's HIPAA compliance or similar files. Do not place it in the patient's medical record.

Penalties

HIPAA violations can lead to substantial monetary penalties and jail time in criminal cases. Penalties are tiered based on culpability ranging from "did not know" to uncorrected "willful neglect" that a standard has been violated. Within this tiered approach, amounts per penalty range from $100 to $50,000, with a maximum for all violations of an identical standard in a calendar year capped at $1.5 million. This means that a covered healthcare provider may be exposed to multimillion dollar penalties based on non-compliance with the various HIPAA standards and for breaches of unsecured PHI. With respect to breach notification, you are at risk for penalties if you do not have and/or do not follow an appropriate breach risk analysis process, if you fail to report a breach as required by HIPAA, if you do not adequately train staff, and so on. However, even where you appropriately notify the patient and OCR that a breach of unsecured PHI has occurred, you may nonetheless be subject to penalties levied by OCR, depending on the extent of the breach and the particular circumstances.[11]

New York State Breach Notification Law

As mentioned above, New York State has additional notification requirements for breaches of computerized data.[12] The following is a very brief summary of the state law requirements.

Healthcare providers and others conducting business in New York (persons or businesses) must disclose any

11. Case examples and settlements with OCR can be found here: https://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html.
12. See Section 208 of the State Technology Law ("STL") for state entities and Section 899-aa of the General Business Law for the private sector.

continued on page 12

breach of computerized data containing "private information" by notifying the affected NYS resident(s), the NYS Attorney General, the NYS Police, the Department of State's Division of Consumer Protection, and, if the breach involves 5000 or more individuals, consumer reporting agencies. Certain state entities have slightly different reporting obligations.

For purposes of the NYS law, "private information" means personal information combined with a certain data element(s), when the personal information or the data element is not encrypted. The data elements include the person's social security number, driver's license or non-driver identification card, or an account number, credit or debit card number with the security or access code. The time frame for making the required notification is "the most expedient time possible and without unreasonable delay." HIPAA's outside time frame of 60 days may be too long for purposes of New York law. For more information and for a link to the data breach reporting forms, refer to: http://www.dhses.ny.gov/ocs/breach-notification/.

Lessons Learned

The following are recommendations to lower the risk of breaches and to manage your organization's HIPAA compliance obligations and initiatives:

- Conduct a security and privacy risk assessment now before any breach occurs. You should also perform periodic updates. A government security risk assessment tool kit designed for small to medium sized practices can be found at: http://www.healthit.gov/providers-professionals/security-risk-assessment-tool.
- Designate a privacy and security official.
- Strongly consider encryption for PHI at rest and in motion.
- Understand how external portable devices containing PHI are used in the organization. If risks are uncovered, correct them as soon as possible.
- Educate staff on privacy and security frequently (include training on your policies regarding social media, text messaging and the use of digital photos).
- Review, revise and update your HIPAA policies and procedures.
- Monitor access to your EMR.
- Keep informed of OCR's HIPAA-related publications, including the widely anticipated (but not yet released) further guidance on breach risk analysis.
- In the event of a suspected or actual breach or patient privacy complaint, be sure to document your investigation, response, efforts to mitigate and resolution. This documentation will be vital in the event of an OCR investigation and/or audit.

The consequences of a breach of unsecured PHI are severe, including an investigation by OCR, potential for substantial fines and penalties, and, significantly, damage to your organizational or professional reputation. The steps you take now to safeguard PHI will hopefully prevent breaches from occurring in the first place.

Finally, you should remain HIPAA informed. The information OCR provides on its website referenced above is a good place to start. Remember, this is a constantly evolving area. You should continually check for the most recent guidance to remain HIPAA compliant. ❖

Laurel E. Baum is a Partner in the Health Law Department of Hancock Estabrook, LLP in Syracuse, New York, focusing her practice on providing advice and legal counsel to healthcare providers, including hospitals, nursing homes and physicians. Ms. Baum is also a registered nurse with past experience in pediatrics, adult critical care, and nursing management. Further, she was formarly a compliance officer for an academic medical center.

LEGAL Update

PICC Line Concerns

Interventional radiologists often place *peripherally inserted central catheter* (*PICC*) lines and other central lines for use by physicians for the treatment of various medical conditions. These lines can be quite troublesome for the interventional radiologist, the treating physician, and facilities when patients have PICC lines placed. For example, patients with drug addictions who have had PICC lines inserted for antibiotic therapy frequently leave the hospital or physician's office against medical advice. The patient then uses this line to give him/herself illegal controlled substances. These patients often fail to return to the physician for follow-up and/or removal of the line, unless or until the line causes an infection or becomes blocked.

Another concern is the patient who receives antibiotic treatment through a PICC line but fails to return to the treating physician's office to have the line removed, because of relocation or transfer of care to another physician. On occasion, the treating physician may lose track of the patient and fail to arrange to have the PICC line removed.

Patients who are noncompliant with returning to have these lines removed must first receive a telephone call and then a letter to return to see the physician. The letter must warn the patient of the risks of leaving the PICC line in for an extended time beyond that indicated for treatment. The letter, marked "personal and confidential," should be mailed at the post office via first class mail to the patient's last known address. A "certificate of mailing" showing the date the letter was accepted by the post office should be purchased. The certificate proves that the letter was mailed at the post office and it is delivered in the same manner as other regular, first class mail. A copy of the letter and the certificate of mailing should be kept in the patient's medical record. If the first class letter with proof of mailing from the post office is not returned as undeliverable, it may be assumed the patient received the letter.

Even if the patient has relocated or sought treatment from another physician, it is the obligation of the original treating physician to appropriately follow up with the patient to arrange for removal of the PICC line by a physician or facility equipped to do so. After making several reasonable but unsuccessful attempts to urge the patient to return to the office because of the serious risks to life and health in not having the PICC line removed, the treating physician should consider whether it is safe to discharge the patient for noncompliance.

Finally, there is the question of which physician, the interventional radiologist or the treating physician, is responsible for removal of the PICC line after treatment has been completed. The interventional radiologist who inserts the line generally does not necessarily have a duty to follow up with the patient and/or remove the line because that care is transient and only intended for that one time. Usually, removal of the line is the responsibility of the treating physician since he/she has the ability and duty to follow up with the patient and provide continuity of care. However, we do recommend that the interventional radiologist remind the treating physician and the patient that the catheter requires changing at specific intervals. Further, the interventional radiologist can offer to remove and, if necessary, replace the catheter at appropriate intervals. The radiologist should also remind the patient's physician at an appropriate interval about the proper care of the line. The radiologist must document all such reminders in the patient's medical record for his/her own protection.

Updated Notices of Privacy Practices Are Available on the HHS Website

Frances A. Ciardullo, Esq.
Fager Amsler & Keller, LLP

The HIPAA Privacy Rule requires each covered healthcare provider to develop and distribute a Notice of Privacy Practices (NPP) that provides a clear, user friendly explanation of individual rights with respect to patient personal health information, and how that information may be used and shared by the healthcare provider. The U.S. Department of Health and Human Services Office for Civil Rights has published model NPPs in four different formats using plain language. The can be found at http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html. The model NPPs are available in English and, most recently, in Spanish. Covered entities may adopt and customize the NPPs by typing in their own information. These templates also reflect the 2013 regulatory changes of the HIPAA Omnibus Rule. For example, they highlight the new patient right to access electronic informa-

continued on page 15

RISK MANAGEMENT Tip

Tip #17 – Communicating with Low Health Literacy Patients

The public often has limited knowledge and understanding of medical diagnoses and terminology. Low health literacy is a significant problem in the United States. Only 12 percent of U.S. adults have the health literacy skills needed to manage the demands of our complex healthcare system.[1] A patient's ability to understand medical information also may be compounded by stress, age, illness, and language or cultural barriers.

Effective communication with patients may improve compliance with treatment regimens, enhance the informed consent process, and increase safe medication use. Healthcare organizations and physician office practices can improve patient safety and satisfaction, and reduce potential liability exposure, by employing the following tactics:

1. Use lay terminology whenever possible. Define technical terms with simple language. Patient education materials should be written in plain language, avoiding the use of medical jargon.
2. Verbal instruction may be reinforced with visual aids and printed materials that are easy to read and include pictures, models, and illustrations. Consider using non-printed materials, such as videos and audio recordings, as indicated.
3. Offer to assist your patients when completing new patient information or any other practice documents. Provide this help in a confidential way, preferably in an area that is private and conducive to this type of information exchange. Encourage your patients to contact you with any further questions. Additional assistance and/or the use of interpreters may be indicated for patients who are not fluent in the English language.
4. Use open ended questions rather than yes/no questions to further assess patient understanding. At the end of an encounter, instead of asking "Do you have any questions?" try asking "What questions do you have for me?"
5. Providers and staff should be familiar with and utilize the principles of "Teach Back" when reviewing new medications or treatment plans with patients: teach a concept—then ask the patient to repeat back the information they just heard using their own words.
6. Patients and family members may be embarrassed by, or unaware of, their healthcare literacy deficits. An empathetic approach to understanding patient health literacy will enhance your physician-patient relationship. ❖

1. AHRQ Health Literacy Universal Precautions Toolkit: 2nd edition. January 2015. Agency for Healthcare Research and Quality, Rockville, MD. http://www.ahrq.gov/professionals/quality-patient-safety/quality-resources/tools/literacy-toolkit/index.html.

Case Study *continued from page 7*

examinations did not belong to the defendant. Rather, these forms displayed the names of other practitioners with whom the defendant shared office space. These physicians were not surgeons, were not his partners, nor even his employees. The defendant's use of these forms appeared deceptive, sloppy, and unprofessional. It is highly irregular for physicians to use forms belonging to another practice. Further, the defendant might well have implicated the physicians listed on the forms in the litigation. This seeming lack of professionalism was further exacerbated by the defendant inviting the patient to his home to discuss the proposed surgery. All professional discussions should have taken place in the privacy of the defendant's office in order to avoid possible HIPAA violations and ensure patient confidentiality. Further, office discussions would more likely have resulted in contemporaneous documentation.

Despite the fact that all of the expert reviewers felt that the complication suffered by the plaintiff was rare, there were additional concerns with the plaintiff's post-operative care. First, the defendant failed to recognize the plaintiff's serious complications in a timely manner. Second, the defendant's proposed plan to address the complications was inappropriate. A dispute then arose between the co-defendant general surgeon and the defendant. The co-defendant had the patient transferred to a facility better equipped to handle the plaintiff's needs and then emergently loosened the abdominoplasty sutures to alleviate the patient's abdominal compartment syndrome. Because the co-defendant performed this emergent surgery without the benefit of a specialist in plastic surgery, the patient sustained increased scarring.

The co-defendant's initial post-operative note had documented that the abdominoplasty and hernia repair were uneventful. However, when the co-defendant was interviewed by defendant's counsel, he was extremely critical of the care the defendant provided. Because it was obvious that there would be finger-pointing between the two defendants, which would only serve to benefit the plaintiff, settlement by the MLMIC-insured defendant was strongly pursued by counsel. This case was finally settled on behalf of only the MLMIC defendant for the sum of $725,000. The lawsuit against the non-MLMIC insured co-defendant, however, continued to be defended by his insurer. ❖

UNDERWRITING Update

Lost Income Reimbursement Policy Benefit

Robert Pedrazzi
Assistant Vice President, Underwriting
Medical Liability Mutual Insurance Company

Being named as a defendent in a lawsuit can be a trying experience. Adding to the overall stress of such circumstances is the potential for loss of income that may occur from your having to cease practice in the event you need to attend a trial. Fortunately for MLMIC PSE Policy insureds, the policy provides physicians, surgeons, and extenders with an added benefit to help address this concern by protecting you from potential loss of income under such a scenario. The Policy's Supplementary Payments provision can be found in 9.b. "Other Costs We Will Pay" under "SECTION I. INSURANCE COVERAGE PROVIDED BY THIS POLICY". This provision provides for reimbursement of up to $500 per day (subject to a cap of $5,000 per trial) for lost income due to the suspension of an insured's practice in order to attend a trial in which you are being defended under the policy.

The provision pertaining to this coverage appears in the policy as follows:

"In addition, we will reimburse you, the natural person, up to $500 a day for the income you, the natural person, lose because you, the natural person, have suspended your practice in order to attend a trial in which you, the natural person, are defended under this policy; however, this payment will not exceed $5,000 per trial."

Equally beneficial to our PSE Insureds is the fact that this Supplementary Payment benefit is in addition to their policy's Limits of Liability, meaning that their available coverage limits are not reduced by any payments made under this provision.

If you have any inquiries concerning this policy benefit that pertain to either a current or past case of yours, please contact your assigned claims examiner. Otherwise, for general inquires, or to obtain a copy of the policy, please feel free to contact an underwriter in the regional office nearest you. ❖

Updated Notices of Privacy Practices *continued from page 13*

tion held in an electronic health record held by a healthcare provider.

Covered entities in New York should not adopt a model NPP without a thorough review of all its provisions. Some of the language in the national model will not apply in New York because of New York's stricter privacy rules. In particular, the model NPPs recite that personal health information can be shared for law enforcement purposes and with law enforcement officials, although that is not the law in New York. Providers who wish to review what disclosures are permissible in New York would be well advised to compare the language in the federal models with the NPPs published by the New York State Department of Health, available on the DOH website at https://www.health.ny.gov/regulations/hipaa/notices/. ❖

MLMIC Offices

2 Park Avenue
New York, NY 10016
(800) 275-6564

2 Clinton Square
Syracuse, NY 13202
(800) 356-4056

90 Merrick Avenue
East Meadow, NY 11554
(877) 777-3560

8 British American Boulevard
Latham, NY 12110
(800) 635-0666

Fager Amsler & Keller's attorneys are available during normal business hours to assist MLMIC insureds with a wide range of legal services, including, but not limited to, advisory opinions concerning healthcare liability issues, liability litigation activities, lecture programs, and consulting services.

Healthcare law, regulations, and practices are continually evolving. The information presented in Dateline *is accurate when published. Before relying upon the content of a* Dateline *article, you should always verify that it reflects the most up-to-date information available.*

MLMIC
Medical Liability Mutual Insurance Company
2 Park Avenue
New York, NY 10016

PRESORT STANDARD
U.S. POSTAGE
PAID
PERMIT #1174
NEW YORK, NY

MLMIC.com

Reflections on Being a Defendant *continued from page 1*

it, and to discuss it openly. I did this to counteract the common feeling among physicians that being sued is like a piece of dirty laundry, to be hidden from colleagues. Instead, it's part of the professional and personal life of so many doctors in today's world. When sharing my experiences with other physicians who had been sued, they felt relieved that they were not alone and often went on to describe their own experiences.

My personal experience of the courthouse is that it's a somber, depressing place. Everyone seems to be trying to take advantage of everyone else, and the truth be damned. That may not be how it is, but that's sure how it felt to me. Nothing starts on time. Few seem to be working hard. You do feel terribly alone. It's not like our medical offices. You can't talk to your own experts, and the only person who has your back is your attorney.

I vastly underestimated the effort and passion that attorneys put into these cases. My attorney knew the case as well as I did. He woke up at night, with a pad and pen by his bed, writing when he had a thought about the case that he didn't want to forget by morning. He lived the case, along with me. I can't imagine how these attorneys can go from one trial to the next, without feeling emotionally and physically exhausted. It's as tough as anything I've ever done. They deserve our gratitude.

So what were the toughest times for me as a defendant? The first is certainly at the end of the plaintiff's case, when you have been called a liar, a falsifier of records, deceitful with the patient, and incompetent. No one has spoken up for you yet, except you, and even then, the plaintiff's attorney won't let you just tell the story, as you would to a colleague. They purposely say things they know will be stricken from the record, but the jury hears anyway. You begin to have doubts about yourself and the fairness of this process. Am I a competent physician?

Hearing your colleagues defend you feels so much better. I would have hugged them all if I could, and when I learned about how they had to juggle their schedules to accommodate the judge's timetable, I was even more appreciative.

The second worst time is after the plaintiff's summation, as they get the last word. You just hope the jury remembers what your attorney said (my attorney's closing was brilliant). After closing remarks, defendants can lose objectivity and want to bail out. My attorney helped me maintain my objectivity. We declined a settlement offer made by the plaintiff, and went on to win the case.

I have come away from all this with a visceral appreciation of the importance of what we all do as doctors on a daily basis, and with a new appreciation of the protection provided by my liability insurer, MLMIC, and their defense counsel. ❖