MLMIC

SPECIAL EDITION

Dateline

VOLUME 14

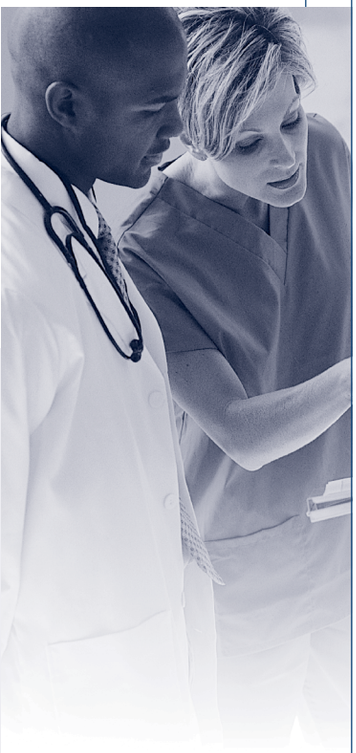
NUMBER 2

spring 15

A NEWSLETTER FOR MLMIC-INSURED PHYSICIANS & FACILITIES

This Special Edition of Dateline *was prepared in response to the increased prevalence of electronic health records and some of the possible issues that may be associated with their use. If you are a MLMIC insured and have any questions not covered in the following articles, please do not hesitate to contact the attorneys at Fager Amsler & Keller LLP, by calling the office nearest you, or by utilizing the Contact Us feature on MLMIC.com.*

1-877-426-9555 – *Syracuse* · 1-877-777-3560 – *Long Island* · 1-800-635-0666 – *Latham*



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.

Medical Identity Theft – The Crime That Can Kill

Joshua Cohen, Esq.
DeCorato Cohen Sheehan & Federico, LLP

Medical identity theft is not just a financial crime. It can kill. A patient receiving medical care fraudulently can lead to the real patient receiving the wrong blood type, prescription, or even being misdiagnosed at a later time. In 2013, there were an estimated 1.84 million victims of medical identity theft costing $12.3 billion.[1] This represented a 20% increase from 2012. There is no doubt that medical identity theft is one of the fastest growing areas of crime. Add in the momentum to move to electronic health records and the rise of cyber crime, particularly targeting healthcare providers, and many experts predict a rapid increase in medical identity theft. Hospitals, physicians, and other healthcare providers must recognize this threat and implement new policies and strategies to protect themselves and their patients from this evolving criminal epidemic.

Medical identity theft occurs when someone uses an individual's name, health insurance, or other personal information to fraudulently receive medical services, prescription drugs or devices, or other healthcare benefits. It has been used to commit false billing, to wrongly obtain credit card information, and to achieve other financial gains. In March 2014, a Florida woman was charged with filing $4 million in fraudulent tax returns by using personal information she illegally obtained from a local health department. In 2013, the healthcare industry experienced more data breaches than ever, accounting for 44% of all breaches, according to the Identity Theft Resource Center. It was the most for any industry. In contrast, the financial/credit industry experienced only 4% of data breaches.

Healthcare data breaches have doubled over the past 4 years. From April through June 2014, 4.5 million patient records were compromised from Community Health Systems by a Chinese cyber attack. Community Health Systems operates 206 hospitals in 29 states. The attackers obtained the names, social security numbers, and addresses of patients. The company, however, stated that no credit card, medical, or clinical information was compromised. The attackers exploited the Heartbleed vulnerability, a security weakness in a widely

1. Ponemon Institute "2013 Survey on Medical Identity Theft."

continued on page 2

Medical Identity Theft *continued from page 1*

used encryption software called OpenSSL that allows the stealing of protected information from applications such as web, email, instant messaging, and some virtual private networks. While patches were made available in April 2014, many systems remain vulnerable. There also are many other ways cyber attackers can infiltrate a system. The takeaway from this is that healthcare information is valuable and many people want to wrongfully access it.

In a recent study of 91 healthcare organizations, 90% reported having at least one data breach during the past two years. Of these, 38% reported having had more than five incidents during that time period. Data breaches can be very expensive. BlueCross BlueShield of Tennessee paid $1.5 million in penalties for a data breach in 2009 that affected more than 1 million individuals. The company stated that it spent nearly $17 million in investigation, notification, and protection efforts. A key element in many of these breaches is that the data was not encrypted. In the BlueCross BlueShield case, the theft involved 57 hard drives stolen from a data closet in their Chattanooga call center. The hard drives were not encrypted and contained audio and video recordings of telephone calls from providers and members that included personal information. Other data breaches have involved unencrypted backup tapes that were lost in transit to storage. In these cases, if the data had been properly encrypted, there would have been no breaches, thereby avoiding the expensive consequences and tarnished image that accompany them.

While most fraudulent activity, such as a wrong charge on a credit card statement or a bill for a credit card for which you did not apply, is identified early, medical identity theft can be insidious and can go unnoticed for years. In one case, a woman went to donate blood for the first time, but was denied without explanation. She later learned from the Red Cross that someone had used her social security number in another state to receive treatment at an AIDS clinic, rendering her ineligible to donate blood.

Even when the fraud is identified, if proper action is not taken, the real patient can suffer from the consequences. A woman in Florida received a bill from a hospital for amputating her right foot. Despite numerous calls to the hospital stating that she still had both of her feet, the hospital kept billing her. She finally went to the hospital and put her feet up on the desk of the chief executive of the facility. As a result, the hospital stopped billing her. However, a year later, she returned to the hospital to undergo a hysterectomy. A nurse asked her what medications she was taking for her diabetes, a condition she did not have. It quickly became apparent that the hospital had failed to remove the fraudulent patient's information from their computer system. Her medical record was contaminated by erroneous information. For example, the fraudulent patient had a different blood type and a blood transfusion would have likely killed the real patient. With the goal to make medical data more accessible among healthcare providers, wrong data such as blood types, medications,

continued on page 5

SAFER Guides for EHR Safety

Safety Assurance Factors for EHR Resilience (SAFER) Guides, available at http://www.healthit.gov/safer/safer-guides, enable healthcare organizations to address EHR safety in a variety of areas. The guides identify recommended practices to optimize the safety and safe use of EHRs. Interactive PDF versions of the guides can be downloaded and completed locally for the self-assessment of an organization's degree of conformance to the Recommended Practices. ❖

Responding to Requests for Electronic Copies of Medical Records

Frances A. Ciardullo, Esq.
Fager Amsler & Keller, LLP
Counsel to Medical Liability Mutual Insurance Company

Every healthcare provider or facility must respond to requests to produce copies of patient information. Both New York State and federal law (HIPAA) give patients the right of access to their protected health information. Most providers are accustomed to handling medical record requests in a paper-based environment. Now, however, many providers are utilizing electronic medical records systems (EMRs) and are starting to receive requests to produce patient information in electronic format. This article will discuss some unique issues involved in responding to such requests.

If the individual requesting the record is a "qualified person" under section 18 of the New York Public Health Law, the individual has a legal right to access the medical record. "Qualified persons" include the patient; the parent or legally appointed guardian of a minor; a health care proxy agent, if the patient lacks capacity; an individual who has power of attorney for the patient which grants the right to access records; the conservator or committee of an incompetent patient; a guardian appointed under Article 81 of the Mental Hygiene Law; the administrator or executor of a deceased patient; a distributee of the estate of a deceased patient; and an attorney at law who represents a qualified person.[1]

The New York Public Health Law requires that within 10 days of a written request for access to records, the provider must give the qualified person the opportunity to inspect the records.[2] You must also provide copies if requested. You must grant access to the medical record, regardless of ability to pay. You cannot withhold the record on the ground that there is a balance due on the patient's account. When patient records are requested in electronic format, questions arise as to how to comply with such a request, and what fees may be charged for providing the record.[3]

Must I provide a patient's record in electronic format?

Under HIPAA, covered entities that have EMRs must provide access in the form or format requested by the individual if it is readily producible in such format.[4] You are not required to purchase new software or systems in order to accommodate an electronic copy request in a specific form, provided that you are able to provide some form of electronic copy. If an individual requests a form of electronic copy that you are not able to produce, you must offer other electronic formats that are available on your system.

For those who have mixed media, i.e. paper and electronic records, there is no requirement to scan paper documents

1. Public Health Law § 18(g). Any qualified person who may access records on behalf of a patient under State law is a personal representative with a right of access under HIPAA. 45 CFR § 164.502(g).

2. New York's time limitation is more restrictive than HIPAA, and therefore providers must follow New York law.

3. The Department of Health and Human Services has published a helpful resource publication, entitled "The HIPAA Privacy Rule's Right of Access and Health Information Technology," which is linked as a PDF document on the HHS website at: http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/.

4. 45 CFR § 164.524(c)(2).

continued on page 4

and provide electronic copies of records held in paper form.[5] However, as a practical matter, it may be easier to scan and provide all records in electronic form rather than providing a combination of electronic and hard copies.

How should I comply with a request for electronic copies?

If the records are not readily producible in the form or format requested, access must be provided in some other readable electronic format mutually agreed upon between the covered entity and the requesting individual. Possible formats include MS Word, Excel, text, HTML, or text-based PDF.[6] If the individual declines to accept any of the electronic formats that you are able to produce, you must provide a hard copy as an option to fulfill the access request.

Electronic access may be granted by copying the record to a USB thumbdrive or a compact disc, or even via a direct-view portal. While a patient may ask you to copy the information on a flash drive he or she provides, you are not required to accept an external portable device provided by the patient if you feel it presents a risk to your system. You cannot, however, require the patient to purchase a portable medical device from your office. If the patient does not wish to receive the information on media you provide, he or she may opt to receive the electronic copy in an alternative form, such as through email.

If the patient requests that I send the information via an unencrypted email, am I allowed to honor that request?

You are permitted to send individuals unencrypted emails if you have advised the individual of the risk and the individual still prefers the unencrypted email. You are not expected to educate individuals about encryption technology and information security; rather, you are merely expected to notify the individual that there may be some level of risk that the information in the email could be read by a third party. If the individual is notified of the risks and still prefers unencrypted email, the individual has the right to receive the protected health information in that manner and you are not responsible for unauthorized access during transmission or upon delivery.[7]

May I deliver the information electronically to a third party?

The individual has a right to direct that you transmit an electronic copy of his or her protected health information in an EMR directly to a third party, provided that the designation is clear, conspicuous and specific. The request must be in writing, signed by the individual, and must clearly identify the designated person and where to send the copy. If you are disclosing information to a third party, a HIPAA authorization must also be provided.

What fees am I allowed to charge?

Fees for providing an individual with access to his or her protected health information are regulated by both federal and state law. Under HIPAA, the provider is allowed to charge a reasonable, cost-based fee for a copy of protected health information.[8] The fee may only include the costs of supplies and labor for copying the protected health information, and postage associated with mailing, if the patient has asked you to mail the information.[9]

The "reasonable, cost-based fee" means your actual costs for copying. You are not allowed to charge a search or retrieval fee.[10] There is little hard guidance as to how you should arrive at your actual costs for copying. The Department of Health and Human Services has stated that labor costs could include skilled technical staff time spent to create and copy the electronic file, such as compiling, scanning, and burning the information to media and distributing the media. The cost of supplies are also allowed, such as paper or the physical media (CD, flash drive) if the individual has asked that the copy be provided on portable media.[11] The commentary to the HIPAA rules states:

> In response to comments about the types of costs that are permitted in the reasonable cost-based fee to prepare and transmit data, we clarify that this may include both direct and indirect costs, including labor, materials, and supplies for generating, storing, retrieving, and transmitting the protected health information; labor and supplies to ensure the protected health information is disclosed in a permissible manner; as well as related capital and overhead costs. However, fees charged to incur a profit from the disclosure of protected health information are not allowed.[12]

On the other hand, costs associated with maintaining systems and recouping capital for data access, storage and infrastructure are not allowed as part of the "reasonable, cost-based fee" and cannot be apportioned to patients.[13]

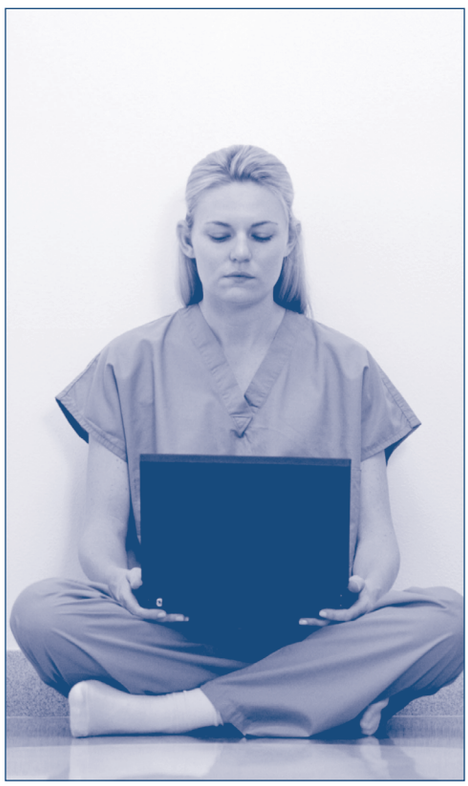
5. 78 Federal Register at 5633.
6. 78 Federal Register at 5631.
7. Id. at 5634.
8. 45 CFR § 164.524(c)(4).
9. If you are preparing an explanation or summary of the PHI at the request of an individual, you may charge for the labor cost of preparing the summary. Id. at 5635.
10. The charge for x-rays, photographs and videotapes must be the actual cost of duplication. In addition, a qualified person has the right to obtain original mammogram films. You may not impose a copy charge for original mammograms, but may charge the actual documented cost for furnishing the original mammogram. 21 CFR § 900.12 (c)(4)(ii) and (iii), New York Public Health Law § 17. Once the original films have been provided, you are no longer required to maintain a copy.
11. 78 F.R. at 5636.
12. Id. at 5607.
13. Id. at 5636.

How does HIPAA's cost-based fee requirement relate to the 75 cents per page rule under New York law?

Under HIPAA there is no maximum amount stated, as long as your fee represents your reasonable actual costs. Under New York law, however, providers are limited to up to 75 cents per page for paper copies.[14] Note that 75 cents per page is a maximum, and that you are permitted to charge up to this amount. Your charges must still reflect actual costs. In an electronic environment, you would estimate the number of printed pages the electronic record represents, and multiply that by 75 cents per page, as long as the total did not exceed your actual costs. For example, if you determine your actual costs for providing a medical record in electronic format is $15.00, you would be permitted to charge $15.00 for the first 20 paper pages of the record. If your record exceeds 20 pages, you would be limited to $15.00 since that would be your actual cost.

Can I charge a fee if I am asked to sign an affidavit certifying the record?

The cost of preparing an affidavit to certify the record is not a copying cost. You may charge the individual for preparing the affidavit and your charges are not subject to the reasonable, cost-based fee limitations. However, it is strongly recommended that you adopt a relatively nominal charge, and you may not withhold the record for failure to pay any fee you might impose.[15] ❖



14. NY Public Health Law § 18(e).

15. Id.

Medical Identity Theft *continued from page 2*

and allergies can lead to serious complications and death. This makes medical identity theft not just a crime, but also a quality care issue that must be addressed promptly by not only billing departments, but also the clinical and quality assurance departments as well.

Because medical information is becoming more accessible, medical identity theft is becoming easier to perpetrate and affects everyone. In Seattle, a couple celebrated the birth of their son. Three weeks later, they received a bill addressed to their son from a local clinic for a visit for a work related back injury and a prescription for OxyContin, despite the fact that the only labor their son had experienced was his own from birth. The bill even contained their son's middle name, which only close family and friends knew. It also included the hospital where he was born that filed the paperwork for his birth certificate, his home address, the parents' social security numbers, and the mother's maiden name. A call to the clinic revealed that someone using their son's identity obtained healthcare there within one week of his birth. While the clinic agreed to waive the charges for that visit, for many victims, the full impact does not immediately manifest until they are sick, need help, and are denied services because their health insurance is maxed out by a stranger.

Even if there is no physical harm to the real patient, medical identity theft often damages the trust and confidence a patient has in his or her healthcare provider. This results in a breakdown in the physician-patient relationship, the cornerstone of good medical care. There also is the very negative financial impact from being billed for services not received, the decreased credit scores, and the significant amount of time required to clear up the inaccuracies in a patient's medical and financial records. According to the Ponemon report, a staggering 39% of medical identity theft victims in 2013 reported losing their health insurance as a result of the fraud perpetrated on them. Others are denied life or disability insurance based upon erroneous information contained in the medical records.

Another form of medical identity theft is the "Robin Hood" fraud, where a family member or friend knowingly permits someone to use his or her identity to receive medical treatment or benefits. In 30% of these cases, the information was shared with the person using it. The most common reason cited for permitting

continued on page 6

this was that the family member or friend lacked insurance and could not pay for the needed treatment. In 28% of these cases, a family member took the information without the patient's knowledge. By contrast, data breaches account for only 7% of medical identity theft. Such allegedly altruistic sharing of one's medical identity still subjects the knowing provider to the same risks as those of patients whose identities have been stolen. They will likely need medical care from the same hospital or physician who treated their family member or friend. Thus, the provider will be relying on that other individual's medical history, such as known drug allergies, medications, etc., when treating the real patient. This is a prescription for disaster for both the patient and the provider.

Whether victims or knowing participants, it is often very difficult to get the erroneous information expunged from the real patient's record because of privacy protections that even protect the fraudulent patient. Healthcare providers and hospitals are required to maintain accurate records for all patients, even those with a false identity. Once it has been discovered that someone received treatment using fraudulent means, privacy regulations prohibit the healthcare entity from sharing the fraudulent patient's medical information with the real patient to determine which medical facts are not correct. This becomes even more problematic when the false patient's medical history is intermixed in the real patient's medical record, thus corrupting it. Without performing a line-by-line review of all of the information in order to delete what is incorrect, an entirely new medical record must be created. This is further complicated by the requirement to maintain an accurate medical record for the perpetrator, even if you know from the start that the patient's identity is not accurate.

Healthcare providers need to be educated about this growing problem and need to develop and implement policies and procedures to reduce their risk of being involved in medical identity theft. There are two basic approaches every healthcare provider and organization can take to avoid medical identity theft: patient identification and data protection. Most hospitals and physicians today require patients to show proper photo identification to receive medical care in a non-emergency visit. Many electronic health records allow the photo ID to be scanned into the chart, or allow the inclusion of another photo of the patient. Practices still using paper records should make a copy of the patient's photo ID and add it to the record. However, as a best practice, a government issued ID such as a driver's license should not be scanned into the patient's electronic health record because doing so would add unnecessary personal information to the record that could increase reporting requirements in the event of a breach. It is more important to document in the record that the patient's identity was verified using a proper form of identification, rather than incorporating unnecessary personal information. Then take a picture of the patient for inclusion in the EHR. Once the patient's identity has been verified, at subsequent visits, the photograph on file can be compared to the patient presenting for the appointment. This simple step greatly reduces patients using false information to obtain medical services.

Data protection is a more complicated issue, given the complexity of health information systems and the push to make information more available to providers who need it. In large hospital organizations with robust IT departments, a team approach is necessary to address the many potential areas of access. The team should include a privacy officer and representatives from corporate level administration, information technology, information security, compliance, finance, human resources, clinical departments, laboratory and imaging, and patient relations. Because it stores vast amounts of patient data, the larger the organization, the larger a target it becomes. Hackers may spend a year or more to gain access to these systems, but the financial reward to them is much greater if they can steal the information of millions of patients.

For individual or small practices, working closely with your IT specialist and electronic health record (EHR) provider is key. Whether your EHR is on a server located in the office or based in the cloud, you must know where your patients' data are being stored and how it is protected. Patients believe their physicians control and protect their healthcare information, whether there is a paper

record locked in a file room or an EHR. Physicians still control their patients' data, but now they have agreements with vendors and often do not know where the data is being stored nor how it is being protected. They rely on assertions from the vendors that the vendors are "HIPAA Compliant." However, if there is a data breach, it is the physician who is still responsible and most vendor contracts have no provision to protect the physician in the event of a breach. There is now "cyber insurance" available to help offset the costs of a breach and provide small medical practices with the resources to respond to a breach. When I had back pain, my doctor told me there were two types of people, those with back pain and those who will get back pain. I tell my physician and hospital clients there are two types of practices, those who have had a breach and those who will have a breach. The key is to be prepared.

At very little cost, physician practices can insure against a data breach and be ready for one by having a breach coach lined up to help them through all of the regulatory and state requirements, notification services to satisfy regulatory requirements, forensic services to identify and fix the breach, and ancillary services to remediate the effects of the breach and maintain the relationships forged with patients over years. For many practices, responding effectively to a breach means the difference between surviving, or not.

Whether you are a large hospital organization or a solo practitioner, prevention is crucial to preventing medical identity theft. Better firewalls, increased data protection, encryption, and information governance will definitely lower the risk of a breach. However, no matter how well technically you build a moat around your data, prevention starts with your staff. Whether they intentionally or negligently leak patient data, you are ultimately responsible for their actions. Therefore, know your staff and perform regular audit trails. Exercise care in hiring personnel who will have access to patient data. Your patients' data may be secured from an IT perspective, but may be readily available to those you entrusted to protect it. For example, a 35-year-old Los Angeles woman was recently sentenced to more than four years in prison for using information she obtained as a medical billing clerk to buy gift cards to pay for her tuition, hair extensions, and other items. In another case, a 51-year-old man from Brookhaven, Long Island, was sentenced to more than four years in prison for stealing the names, addresses, birth dates, and social security numbers of the patients of a community hospital where he worked and then selling them to co-conspirators to use as part of a tax fraud scheme. The bottom line is that you can spend a great deal of money and time to protect your IT infrastructure, but if you don't properly screen those who have access to the system, you are still at risk.

While prevention is the frontline against medical identity theft, detection is also integral to a fully implemented system to avoid this fraud and mitigate the threat to the quality of care provided to your patients. Detection starts with the obvious: a photo ID that does not match or appears forged; a social security number that is incorrect; discrepancies in the patient's demographics; and mail sent to the patient that comes back as undeliverable. These "Red Flags" of medical identity theft should alert the practitioner or their staff of a potential fraud problem. Both large healthcare systems and small practices must have written policies and procedures to address these discrepancies and determine whether there was a simple error or medical identity theft is being perpetrated. Larger systems can delegate prompt investigation of such a concern to various team members, such as the privacy officer. Small office practices can require that the office manager or provider be promptly notified. In

continued on page 8

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

MLMIC.com

Medical Identity Theft *continued from page 7*

either scenario, a reliable process must be followed to confirm that medical fraud is not being perpetrated while still meeting the needs of the patient.

Finally, if medical identity theft has been encountered, policies and procedures must be in place to quickly address the problem, ensure patient safety, establish the cause of the problem, and mitigate its effects on the patient and the practice. If the data breach involves numerous patients, a pre-arranged procedure should be followed to identify the breach, cure it, notify the patients, and assure them that every reasonable measure will be taken to protect their privacy and financial interests. Data breaches involving protected health information are required to be reported not only to the individual, but also to the US Department of Health and Human Services, and, in some cases, the media. If the breach involves computerized social security numbers, drivers' licenses, or credit card information, it is reportable to the individuals, the New York State Department of State Division of Consumer Protection, the office of the New York Attorney General, and the New York State Division of State Police.

Medical identity theft is clearly a growing problem for the medical community and has serious repercussions for both the healthcare provider and the patient. All healthcare institutions and providers must be cognizant of this rapidly increasing crime and enact measures to prevent and/or ameliorate it should it occur. It is not only a financial crime, but one that can have serious consequences to the health, safety, and finances of your patients, as well as your physician-patient relationship and the reputation of an institution or physician. ❖

Joshua Cohen is a founding member of DeCorato Cohen Sheehan & Federico, LLP, a firm dedicated to representing physicians and hospitals in healthcare litigation, professional liability, and administrative proceedings. He has taken a leadership role in electronic health records and electronic discovery in healthcare litigation. He is a former President of the New York State Medical Defense Bar Association and recently selected as a Top 100 Health Care Attorney in the State of New York by the American Society of Legal Advocates for 2015. He's listed in Who's Who in American Law and is AV Peer Review Rated by Martindale-Hubbell.