CLM 2015 Medical Legal Summit
June 3, 2015 in Chicago, IL

Electronic Medical Records: Problems, Liability Issues Related to ACA Requirements and HIPAA

I. The Age of Electronic Medical Records is Upon Us

What Exactly is an EMR?

Gone are the days where the world is ruled by paper. Society is continuously evolving to a paperless environment, and healthcare is certainly no exception. Many hospitals and doctors offices have migrated to an electronic format in their data and records. In a perfect world, this could one day streamline the healthcare system nationally – even internationally. Patients would be able to walk into any doctor's office or hospital and the physician would have nearly instant access to entire records, charts, and other important data. While we are still quite a ways away from perfecting that system, it is enough of a reality that it needs to be discussed in this day – particularly their role in the legal industry.

Advancement of EMR Culture Resulting from ACA

In 2010, President Obama signed the Affordable Care Act. Under this act, comprehensive insurance reforms rolled out over the course of the last five years. So what role does electronic health information play in this? As of October 2012, in an effort to reduce paperwork and administrative costs, a series of institutional changes have been put in motion to standardize billing as well as requiring the implementation of rules for the secure, confidential, electronic exchange of health information. By eliminating as much paper as possible, as well as reducing administrative tasks – costs will be cut, errors will be reduced and ultimately the quality of care across the board will improve.

Technology Concerns: How Secure is Electronic Data?

Understandably, some are concerned over the possible security issues that anything electronic is faced with. Having entire patient history information available electronically can be especially attractive to potential hackers. More often than not, it's not the actual health history that the cyber criminal is interested in. Whether or not you

broke your leg six years ago and had to visit an orthopedic surgeon does not translate into anything valuable to a hacker. Confidential information that would be specific to one's identity is the primary security concern. Establishing a secure enough system technologically as well as personnel-wise is crucial in protecting the private data that an electronic medical record contains that limits the possibility for identity theft. It is estimated that to date, nearly 41.5 million people have had their protected health information (PHI) compromised in a reportable privacy or security breach, according to recent Department of Health and Human Services (HHS) data.

II. Breaking Down the EMR

Benefits of Electronic Health Information

When the Affordable Care Act was signed, the role of electronic health records or EMRs, is substantial to the desired outcome of the intention of this act. Beyond the reduction of paperwork and administrative duties, there are plenty of other benefits that result from the continued implementation of electronic information. Quality and convenience of care is predicted to increase noticeably. Being able to be treated anywhere, efficiently and accurately is something that patients of the past have not been able to experience.

While this certainly affects the patients positively, it also proves to be a benefit for folks in the legal and insurance industry as well. Through secure electronic storage and transmission, these records can be shared with much greater efficiently than the days of old where thousands of pages of hard copy files had to be exchanged in order to settle a claim or litigate a case.

Challenges of the Electronic Environment

As previously mentioned, one of the biggest concerns involving electronic medical records is the security involved with the protected health information. Privacy is by far the biggest concern with making all this information electronic. While privacy of records has always been an issue – even in a paper environment, the ability to do widespread damage is potentially intensified in an electronic space. Fortunately, there are preventative measures to take on many different fronts that can limit any type of undesired event.

Beyond the privacy issue, another general concern is how possible a complete transition into electronic data truly is. It is an unprecedented undertaking to convert all data to paperless information, and that shift is not expected to take place fully for some

time. However, in the midst of that transition, information of individual patients may still be in multiple locations and may initially cause confusion.

Future Outlook

As of 2013, it was estimated that the majority of practicing physicians as well as most hospitals had adopted some variety of electronic health records into their practices. What these ultimately evolve into, and how soon is still to be determined. What is clear is that they are here to stay – and this form of data needs to be respected. It could be said that the initial phase of EMRs was an "implementation phase" and was introduced into the healthcare system out of necessity from the ACA. We are now progressing into an "optimization" phase, where the power of the EMR will be fully unleashed and we will see next-level health IT through this electronic data.

III. Real World: HIPAA Breaches

Alaska – Mental Health Organization

Anchorage Community Mental Health Services has agreed to pay a relatively low fine considering of $150,000 to the Department of Health and Human Services as a settlement to a breach reported in March 2012. After extensive investigation, it became clear that while the ACMHS had appeared to adopt the appropriate HIPAA security policies and procedures, they had fail to consistently follow the guidelines that they themselves had implemented in order to avoid breaches.

Nearly 3000 individuals were affected by a malware breach that could have likely been avoided if the proper technological updates were performed. Seemingly simple measures such as updating software and making sure internal systems are up to date would have avoided the compromising of this data as well as the settlement bill.

Tennessee – Insurance Plan Subcontractor

A Dallas-based medical testing and screening company had to notify over 60,000 individuals that their protected health information was compromised. It was brought to officials' attention that hackers had as much as three months access to the system without any notice. The individuals affected were members of the Tennessee State Insurance Plan.

Perhaps even bigger than the actual breach itself, was how long it took the officials to inform the individuals who had been affected. Fortunately, social security numbers were not obtained in this scenario – however member names, birth dates, addresses, etc. were indeed accessed. While there has been no reported identity theft in

conjunction to this event, the length of time that passed between the notifications is much longer than what is considered responsible.

Massachusetts – Third Party Vendor

Serious HIPAA breaches are not always the result of a malicious or criminal intent. Sometimes, the breach is completely unintentional and accidental. That does not mean that it goes without consequence. Boston Medical Center had to fire a third party transcription vendor last year after it was uncovered that 15000 different patients had their health records and demographic data posted to the vendor website without password protection. While it is unknown both how long the information was accessible, as well as who, if anyone actually accessed it – the hospital had to take necessary action and terminate their relationship with said vendor.

IV. Preventative Measures: How to Limit the Chances of a Breach

Minimizing Technological Snafus and Lapses in Human Judgment

In the first example of the Anchorage Community Mental Health Services, the event may have been avoided if two different preventative measures were taken more seriously. Educating your employees on what needs to be done to avoid breaches, as well as driving home what level of consequence may be in store for the individual, the company, and all potential victims may create a higher level of respect towards the system.

In this scenario, it appears that there was a plan for technological security but not one that was consistently maintained. Simple maintenance and continuous updating to software that was specifically created to prevent these types of snafus goes a long way. Regularly subjecting employees to HIPAA training will at the very least provide you with facts to back-up that you have at least taken all appropriate measures to attempt to avoid any breach.

Don’t Delay: Notifying All Appropriate Parties

Unlike the four month waiting period that was illustrated in the example of the Tennessee insurance victims, reporting breaches to the appropriate channels accurately and efficiently is the most responsible avenue that will be most likely to limit punishments as well as the damage done.

Nothing is too small to be reported. Having a HIPAA Compliance Officer on staff is crucial – report anything to him/her and they can then direct to the appropriate parties

depending on the severity of the potential breach. This can be done anonymously and must be emphasized that there is never a situation where keeping a breach or potential breach silent is more beneficial than communicating it. Once appropriate individuals or entities are notified, action can take place to prevent further damage – but until then, there is little to no control.

Vendor Relationships – Establishing Trust

When an entity such as an insurance carrier hires a third party vendor to perform some sort of administrative task externally, many factors are taken into consideration. Level of service, reasonable pricing, pre-existing relationships – these are all very common factors in choosing an outside vendor. Adherence to HIPAA, as well as a thorough and secure internal prevention plan must not be overlooked. Understanding what the company does to make sure they avoid any breaches as well as establishing that they have the same vested interest in your organization's security as you do is key.

With more and more services being performed electronically, whether the dealings are with medical records, depositions, or any other kind of electronic data – a mutual commitment to this type of security is a factor in a third party relationship that should not be neglected.