MEDICAL MALPRACTICE:
ASSESSING ELECTRONIC MEDICAL RECORDS STRATEGICALLY

By: Franklin D. Beahm, Esq.
Jeremy P. Robichaux, Esq.
Beahm & Green
145 Robert E. Lee Blvd, Suite 408
New Orleans, LA 70124
frank@beahm.com

As everyone is abundantly aware, the cost of healthcare in the United States increases every year, however the overall health of our growing nation is not necessarily improving at the same rate as other countries. To combat this growing concern, the United States government wanted to transform our nation's healthcare delivery system with the use of electronic health record (EHR) technology. To achieve this goal, the 111th Congress passed the American Recovery and Reinvestment Act, and President Obama signed it into law on February 17, 2009 with the main purpose of strengthening the health information technology infrastructure through the Health Information Technology for Economic and Clinical Health (HITECH) provision.

What is HITECH and what does it do?

-The HITECH ACT of 2009 provides specific incentives designed to accelerate the adoption of EHR system amongst providers.

-Allows for a provider to transmit protected information in electronic form upon proper authorization, doing away with the archaic practice of paper coping each patient's medical chart

-Widens the scope of privacy and security protections available under HIPAA by holding business associates liable for failure to comply with

HIPAA and HITECH requirements

-Increases the potential legal liability for non- compliance

-Enhanced Authority

-Authorizing State Attorney General to file an action against covered entity on behalf of his or her residents; and requires HHS to conduct periodic audits of covered entities and business associates

-Mandatory Breach Notification

I. ELECTRONIC HEALTH RECORDS DEFINITIONS

An Electronic Health Record (EHR) is an electronic version of a patient's medical care that is maintained by the provider over time, and may include all of the key administrative clinical data relevant to that persons care under a particular provider.

Examples: Demographics; Progress notes; Medications; Vital signs; Past medical history; Immunizations; and Laboratory data and radiology reports.

The EHRs allows access to information and has the potential to streamline the clinician's workflow. The EHRs also have the ability to support other care-related activities directly or indirectly through various interfaces, including evidence-based decision support, quality management, and outcomes reporting. EHRs are the next step in the continued progress of healthcare that can strengthen the relationship between patients and clinicians. The data, and the timeliness and availability of it, will enable providers to make better decisions and provide better care. The benefits of EHRs are as follows:

-Real time access to complete patient records at the point of care which can improve the efficient of patient care in transition from one provider to another;

-Produce clinical alerts and reminders that reduce and prevent medical errors'

-Diagnostic support, and elimination of repetitive tests;

-Reliable e-prescribing with reduced medication errors;

-Reduction in voluminous and redundant paperwork;

-More efficient coordination of patient care;

-Legible records;

-Improved coding and billing

EHRs offer multiple improvements over paper charts; however, they can also pose concerns such as:

-Security and privacy issues;

-System interoperability; and

-Documentation overload;

II. HIPAA AND ELECTRONIC HEALTH RECORDS

Whether you represent a hospital, physician, insurance company, or an individual personal injury victim, you should be aware of a patient's rights to privacy, and the rules and regulations governing the transmission of their **"protected health information."**

The Health Insurance and Accountability Act

-Creation and History

-August, 1996: HIPAA passes Congress and signed into law.

-August, 1999: Congress fails to pass health information privacy law.

-January, 2001: Absent Congressional action, DHHS was authorized to produce

administrative regulations.

-April, 2001: DHHS finalizes its Privacy Rule with President Bush's approval.

-April, 2002: Bush administration modifies the original Privacy Rule.

-April, 2003: The rule becomes effective for most **"covered entities."**

-April, 2004: DHHS Privacy Rule is fully effective for all covered entities.

-2013: the Omnibus Rule revised some provisions and added new ones.

-Added a requirement to report information breaches to patients

-Made business associates directly liable under HIPAA

-Increased civil penalties

-Structure of HIPAA: Privacy and Security

-Privacy Rule- Provides standards for maintaining the privacy of identifiable health information: "A Covered Entity" may not use or disclose an individual's protected health information, except as otherwise permitted or required by law.

-Security Rule- establish a national set of security standards for protecting certain health information that is held or transferred in electronic form**.**

Two key components to HIPAA are **"Covered Entities"** and **"Protected Health Information."**

Covered Entities (CE):

-Health Plans;

-Health Care Clearinghouses;

-Health providers that exchange identifiable health data electronically; and

-Business Associates

-Claims or data processors

-Billing Companies

-Quality assurance reviewers

-Lawyers

-Accounts

-Financial service providers

Protected Health Information

-Any individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.

Examples:

-The individual's past, present, or future physical or mental condition;

-The type and mode of health care to the individual;

-The past, present, or future payment for any health care provided to the individual;

-Name, address, date of birth, or social security number.

-The following are permitted uses and disclosures under HIPAA's Privacy Rule:

-Authorization (specific written authorization from the individual);

-Treatment, Payment, and Health Care Operations;

-Incident to an otherwise permitted use and disclosure (Minimum necessary rule-provider should disclose the minimum information necessary to achieve a particular purpose);

-Public Interest and Benefit Activities (e.g. child abuse, public health

tracking, judicial proceedings); and

-Limited data set for purposes of research, public health or healthcare operations (direct identifiers removed)

-Covered Entities may rely on professional ethics and best judgments in deciding which of these permissive uses and disclosures to implement.

-HIPAA's Security Rule applies to a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form. The Security Rule requires all Covered Entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting all electronically stored or transmitted protected health information. The purpose of HIPAA's Security Rule is to:

-Ensure the confidentiality, integrity, and availability of all electronic protected health information they create, receive, maintain or transmit;

-Identify and protect against reasonably anticipated threats to the security or integrity of the individual's protected health information; and

-Protect against reasonably anticipated, impermissible uses or disclosures by ensuring compliance of a Covered Entity's workforce.

-To safely secure and ensure compliance with HIPAA's Security Rule, health care providers and business associated should be aware of security features and available safe guards, and utilize them when creating, maintaining or transmitting electronic protected health information (including EHR):

Administrative Safeguards- perform risk analysis that includes, but not limited to,

the following:

-Evaluate the potential risks associated with electronic protected health information;

-Implement appropriate security measures to address the risks identified in the risk assessment (securing networks, implementing firewall protection, encrypting data files);

Physical Safeguards:

-Create policies and procedures for secure use of and access to an individual's electronic protected health information at workstations;

-Create policies and procedures for secure transfer, removal, disposal, and use of an individual's electronic protected health information via electronic media

-Physical locations where electronic protected health information is maintained via data servers should be locked with highest access restrictions

Technical Safeguards:

-Password protect files to ensures only appropriate or authorized users can access certain protected health information

-Implement hardware, software, and/or procedural mechanisms to record and tract access or other activity in systems that contain or use electronic protected health information

-Example:

-Edits, audits, and system logs should be enabled to track all

persons accessing and editing any and all electronic protected health information (More on this in the Medical Malpractice Section)

-Electronic protected health information should be backed up to control the risk of data loss from natural disasters

Recent Developments:

HIPAA ENFORCEMENT UNDER A NEW ADMINISTRATION

-Both the Department of Health and Human Services and President Trump's budget for fiscal 2018 suggest the same for HIPAA enforcement, "Less is more." This notion is a result of a dramatic drop off in HIPAA enforcement actions brought by the Office of Civil Rights. With President Trump and HHS's focus of "minimizing duplication and burdensome requirements" and "eliminating outdated and obsolete restrictions" for 2018, it is unlikely to see an increase in HIPAA enforcement.

HIPAA REGULATION AND ENFORCEMENT BY INDIVIDUAL STATES? MAYBE.

-An additional regulatory priority documented by the HHS is to "enhance regulatory flexibility so state and community partners are able to tailor their programs to fit the needs of the people they serve." Today, the world is focused on cyber-security and data breaches, and each State is developing their own cyber-security and breach notification protocols; however, there still remains federal preemption when it comes to HIPAA regulations. Could it be possible that the current administration and HHS give the states more rights to enforce the

security and use of medical information? The change would not be favorable with industry participants as it would change what is greatly accepted as a uniform rule which would in turn look different from state to state if regulations of protected health information were enforced through state authority. With the current administration focused on reducing federal regulation and giving more regulatory power to the states, one cannot help to think if HIPAA regulations would be abandoned in lieu of state regulations.

III. Electronic Health Records In Medical Malpractice Litigation

Prior to the mass production of personal computers, all medical records, including physician and nurse progress notes, were written by hand. For legal purposes, whenever an attorney needed to review medical records for medical malpractice cases, he or she would have to rely on the hand writing of doctors and medical staff personnel to understand more about the medical condition of each patient, which more the likely is illegible for most non-health care professional. However, it has now become easier than ever for attorneys to determine if a particular physician or health care provider breached or maintained the standard of care by way of Electronic Health Records or Medical Records.

Electronic Health Records not only affect the risk of a potential lawsuit, but the conversion from paper to electronic health records can also affect the course of malpractice litigation by increasing the availability and volume of information an attorney may use to prove or disprove an alleged malpractice claim. An added benefit for attorneys using EHRs is its function in recording all electronic transactions, including the

input of all physicians' orders and time stamps of all clinical activity. This information is called Metadata, and it provides an electronic fingerprint that can be used to track all health care provider activity in real time.

Under Federal law, (FRCP 26(b) & 34(a)), Metadata similar to electronically stored information, are discoverable in civil trials, meaning defendants must produce them to any requesting attorney during discovery as long as they are relevant and reasonable attainable. However, State law governs most malpractice litigation, and whether Metadata is discoverable and permissible varies from State to State.

Possible Scenarios dealing with Metadata

-In a malpractice case, the documentation within EHRs can establish a provider's liability, whereas in other matters it may serve to help defend a health care provider from potential liability.

Examples:

1. A patient undergoes extensive repair surgery to his jaw that resulted in a favorable operative outcome. The patient sues his surgeon for negligence in a malpractice action. Following a thorough review of the EHRs (including the metadata contained therein) from the operating room, the patient's attorney discovers a gap of more than ninety minutes in the anesthesia record. The attorney amends his pleading seeking legal action against the anesthesiologist to uncover the reason for the discrepancies in the anesthesia record, and its possible correlation with the patient's operative outcome.

-Result- Though it may be unclear or require additional expert testimony that the missing entries in the anesthesia record were indicative of an error in the patient's treatment, the discrepancies in the anesthesia record would be difficult to defend. The metadata in this instance (and not just the medical records themselves) could ensure settlement or a positive outcome at trial.

Metadata can also be used to verify or authenticate an EHR was modified at the time of treatment rather than later, which would typically solidify a defendant's ability to rely on the EHR when disproving any alleged negligence for delayed treatment. However, if the medical record was edited or modified at an inappropriate time, metadata can give rise to claims of potential falsification of records, or professional negligence.

2. In referring to the scenario above, the metadata also revealed the Anesthesiologist wrote his *post-operative note* within minutes after the operation *began* (and well before the completion of the procedure).

Result- Reviewing the metadata in addition to the actual records themselves revealed another glaring deficiency in the anesthesiologist's practice because the entry of his post-op report was time stamped. In this instance, reviewing the time stamped activity from the audit trail will bolster the plaintiff's negligence claim, making any defense of the anesthesiologist's negligence nearly impossible.

New Developments and Tendencies

With the increasing implementation of EHRs by health care providers, attorney's representing injured patients are now more than ever drawn to the audit trails of the EHRs. These EHR audit trials may reveal information undocumented by the health care provider providing at times the long sought after "Smoking Gun." Audit trails are **computer metadata** that document every change or addition to a patient's EHR, and can tell you which health care provider input or accessed which record and when, and in most cases, if any modifications have been made.

Examples:

1. Attorney Smith represents a patient who was admitted to New Jersey Hospital for complaining of increased pain around her surgical wound from the prior week. Doctor Strange evaluated the patient and noted no signs of redness or swelling at the surgical site and no fever. Despite sending specimens to pathology for testing, Dr. Strange failed to note it in the medical records. The plaintiff was admitted to New Jersey Hospital a week later with fever of 103.0 and an infected non-healing surgical wound. Despite a thorough review of his client's medical records, Attorney Smith could not find any evidence to show his client's infection was present upon her prior visit to Dr. Strange. Several weeks before trial, Attorney Smith realized New Jersey Hospital failed to produce

the metadata or audit trail for his patient's office visit. Following a court order for production of the metadata, Attorney Smith was able to locate pathology slides for his patient that had never been disclosed nor existed in any of the patient's medical records or billing except for the audit trail.

-Result- This evidence revealed Dr. Strange failed to follow up with pathology and discharged the patient based solely on her physical symptoms. This bolstered Attorney Smith's claim for negligence, and further prompted him to amend his pleading for Spoliation of Evidence as the New Jersey Hospital failed to produce the Metadata/Audit Trail.

2.-Patient X underwent a routine jaw surgery and suffered subsequent brain damage not evidenced until the patient seized several months later. Attorney Smith reviewed the case; at a glance, the EHR contained little evidence to connect the unfortunate result to any malpractice of the surgeon. However, a glaring discrepancy during the surgeon's deposition changed everything. During the surgeon's deposition, Attorney Smith discovered the medical record the surgeon was reading from contained an interpretation of the patient's CT scan that was not included in his copy of the medical records. Following the deposition, and after reviewing the audit trail carefully (which was

voluminous), he discovered Patient X's medical record had been altered. Attorney Smith's copy of the medical records was printed 11 months following the surgery, and the surgeon's copy was printed 2 months following the surgery.

Result-The evidence presented from careful review of the audit trail made defending the physician who altered the record after the fact a near impossibility. The case went from a slam dunk for the health care provider to a costly settlement.

The above examples exemplify the importance of reviewing the EHRs and the Metadata or Audit Trial by both plaintiff and defendant attorneys alike. Taking the time to review hundreds or even thousands of pages of metadata may be your client's saving grace or the final nail in your opponent's coffin. Improving the quality of patient care was and is the main goal of all health care reform and the implementation of EHRs and Audit Trails will at the very least deter any health care provider from the temptation of altering a patient's medical records at the risk of a potential lawsuit or even losing their medical license.

IV. EHRs AND There EFFECT ON THE STANDARD OF CARE

In a medical malpractice action, the plaintiff has the burden of establishing the applicable standard of care, proved the healthcare provider acted negligently and breached the standard of care, and the healthcare provider's negligence or breach caused the plaintiff or patient harm. However, due to the mass adaptation of electronic

health records systems by healthcare providers, EHRs may possess the power to reshape or reform health care provider liability by restructuring the way courts and juries view the “standard of care.”

-Traditionally, each side in a malpractice suit presents expert testimony to establish the applicable standard of care to the facts of the instant suit.

-Example

-Plaintiff alleges orthopedic surgeon botched his/her surgery, then each side with present an expert witness who specializes in orthopedic surgery to testify and establish the standard of care for applicable to the defendant physician.

To establish the applicable standard of care, an expert may rely solely on their own judgment and experience and/or produce acceptable medical standards through medical journals or guidelines to show customary care (American College of Orthopedic Surgeons). Any departure from the accepted standard of care would be used as evidence of negligence.

-As mentioned above, the implementation of EHRs were established to improve patient care, and reduce costs on the medical community. But consider, should implementing EHR systems become a standard of care for the health community in and of itself rather than a financial incentive from the government, and would failure to comply with said standard create health care provider liability where it doesn’t exist today.

1. In *Laskowski v. United States Dept. Of Veteran Affairs*, 918 F. Supp. 2d

301, 306 (M.D. PA. 2013), a veteran filed a medical malpractice action against the VA Hospital for failure to treat his PTSD. The case revolved around the health care provider failing to implement EHRs, resulting in a breakdown of communication between medical providers as to which provider had done what. The Court found in favor of the Plaintiff and awarded 3.5 million dollars in damages for failing to treat his PTSD.

While EHR systems have many errors further discussed below, the Court above clearly found implementation of the EHRs would have increased the chances of properly treating the plaintiff, and increased efficient communication between multiple providers.

V. **MAJOR PITFALLS AND RISKS ASSOCIATED WITH EHRS**

Technology has had a major impact on the health care industry for both patients and providers, and one of the advances is EHRs. EHRs have increased the efficiency of modern medicine. EHRs are now in use in 90% of hospitals and 80% of physician's offices as a result of the Federal Mandate issued through the American Recovery and Reinvestment Act, requiring public and private health care providers to adopt and demonstrate meaningful use of EHRs by January 1, 2014 to maintain Medicare/Medicaid reimbursements. This method of tracking patient information has made staff more productive in facilitating communication between patient care teams and providers. But like anything that sounds too good to be true, there are drawbacks and risks associated with EHRs, and such errors associated with EHRs have increased in recent years.

User Errors Associated With EHRs

Keeping records electronically carries some inherent risk for the users of the EHR system and therefore the patients being cared for by those users.

1. *Alert Fatigue*- this is the number one error of EHRs that result in patient harm and malpractice lawsuits. The software that operates the EHR system is designed to spot and alert providers to potential drug-drug interactions in the patient's medical records. These alerts can be frequent and disruptive, and alerts are often overridden or disabled by physicians, which is potentially harmful to a patient.

2. *Copy and Paste Function*- Copy and paste is a helpful tool through EHR systems when a patient's condition remains the same, but any slight change must be accurately recorded. Copying and pasting a patient's history and medical information from prior visits to current visits is a common practice that creates high risks when used for progress notes and physician examinations. Copying and pasting notes can obscure the new clinical information with less relevant information or worse, prevent treatment of the patient's current ailment aggravating said condition to a degree beyond repair.

3. *Drop Down Menu*- This function of EHR systems is a frequent source of errors involving EHRs. They exist to facilitate data entry by the provider, but it is easy to choose the wrong field on a drop

down list, including the medication above or below the appropriate selection. Once an error has been entered into an EHR, it can quickly spread throughout the system and become difficult to correct.

4. *Lack of Training on new Systems*- While some user errors can come from laziness or time restrictions, others come from a lack of training and cause substantial harm to a patient.

> Example: On a new EHR system, Nurse Betty assumed the drop down function of the new system was the same as the old EHR system she had been trained on. Nurse Betty would check the Patient X's bed sores twice a day and indicate such by selecting "Complete" from the drop down menu. But with the new EHR system, selecting "Complete" from the drop down menu copied the description of the bed sore from the last entry if not manually changed. As a result, Patient X's condition worsened but was not noted in the record because the system was continuously copying her original note, showing the condition was the same. The patient got worse, and was transferred to ICU. Patient X sued the hospital and nurse.

5. *Information Overload*- The implementation of EHRs has increased the length of a patient's medical chart by 3x to 5x. This

information overload can cause providers to miss-key pieces of information required to treat or diagnosis the patient. The influx of information creates a temptation for providers to rely on previously recorded patient histories, test results, and clinical findings from a previous visit rather than conduct a new examination and update the record.

System Errors Associated With EHRs

In addition to user errors, poor technology design can also cause issues with EHRs and negatively impact patient care. The transition from paper charts to electronic health records has the potential for documentation gaps.

1. *Missing Information*- Missing information such as tests results or imaging inhibits the provider's ability to make a proper patient diagnosis. When a provider cannot access radiology studies during the patient visit, this can result in a delayed diagnosis.

2. *Field Deficiencies*- when a certain field is inadequate for the actual size of the information to be added. For example, the COMPLAINT field was too small to record "sudden onset of chest pain w/ burning epigastric pain" so the complaint was shortened automatically by the system to "epigastric pain." This mismanaged work up resulted in a subsequent cardiac event.

3. *System Design*- Poorly designed EHR systems are also a

frequent problem seen with providers. Drop down menu designs are often problematic. For example, when what a provider wants to enter is not an option and no “Other” option is available to manually enter a particular complaint, symptom, of diagnosis, providers tend to select something similar that is available in the drop down menu.

4. *Critical Alert Failures*- The failure of critical alerts such as prescriptions or clinical decisions can and have caused unnecessary harm to patients. These alerts are necessary for triggering steps in treatment plans, often times serving as a built-in warning system. When it fails, it can alter a patient’s treatment plan and expected recovery, resulting in misdiagnosis or delayed diagnosis, adverse effects from unintended prescriptions including patient death.

HOSPITAL EHR DATA SECURITY

Ransomware is a growing concern and threat to Covered Entities and Providers who have implemented EHRs in their practice. Ransomware is a type of malware that prevents an organization from accessing certain parts of its system.

-Crypto Ransomware- malware that encrypts the data in a provider’s system with password protection;

-Locker Ransomware- malware that completely locks a provider out of its system denying access to the stored data

Health care provider ransomware attacks could be devastating to a Covered Entity. A provider's failure to access a patient's medical records could delay or render care insufficient causing potential harm or death.

For liability purposes, it is important for Covered Entities to implement the necessary security measures such as advanced updated malware protection, anti-virus software, firewalls, and email/internet security.

Recent Ransomware Attacks

-Hollywood Presbyterian Medical Center- Crypto malware attack, paid $17,000.00 to regain access

-Hancock Health Hospital, Greenfield, IN- Crypto malware attack, paid $55,000.00 to regain access;

-Erie County Medical Center, IN- Refused to pay the $30,000.00 ransom, causing the provider to completely shut down the health care systems mainframe to reboot and restore the system from a backup server. This process took two weeks, and cost the Health care system 10 million dollars.

There are many ways the EHR system has improved patient care such as helping doctors make critical decisions and help nurses carry out effective treatment plans, but no system is error free. Mistakes in medical records have the potential to seriously harm patients, and providers have a duty to do everything possible to prevent them.

VI. MITIGATION STRATEGIES TO REDUCE MALPRACTICE CLAIMS INVOLVING EHRS

The following are mitigation strategies physicians and all covered entities should

employ to help avoid or reduce the risk of malpractice claims and improve patient care:

-Physicians are liable for the data to which that have access to; therefore, they should review all available data and information prior to treating a patient;

-Make sure your health care providers adhere to any alerts within the e-prescribing module of the EHR and document any treatment given;

-Do not disable or override any alerts in the EHR because alert fatigue is a growing problem among providers and they can be held liable if they disable an alert that could have prevented and adverse event;

-Avoid copying and pasting in the EHR except when addressing the patient's medical history, and make relevant, and current notations;

-Review all information auto-populated by the EHRs and contact your IT head to make necessary changes;

-Providers should be aware that Metadata is as important then the EHR as it time stamps all activity in the EHR and is discoverable. The time stamp avoids the allegation of inaccurate or falsified records (Additions, edits, etc.);

-The convenience of drop-down menus for adding prescriptions and such can create over reliance and lead to submitting erroneous information if not properly and timely checked prior to submission;

VII. Electronic Health Record Abuse And Enforcement

From its inception in 2012, the EHR initiative has been under scrutiny by the

HHS Office of the Inspector General for potentially abusive and erroneous practices by some health care providers. Congress intended the EHR incentive program to be a mechanism to encourage its adoption, not an avenue for cheating the system to generate a financial gain. Below are examples of how some providers use multiple functions in the EHRs to inflate payments from Medicare and Medicaid.

Identical Documentation

- This may occur due to use of template based records creation, which can lead to overly standardized documentation. While a standardized documentation system is beneficial, documentation must be clinically relevant and appropriate to the patient, and properly support claims to Medicare and Medicaid for services rendered. Identical documentation also occurs from the overuse or inappropriate use of the "copy and paste" function. This may lead to issues with Medicare and Medicaid billing compliance, and documentation errors.

Medicare Medicaid Fraud

- Providers should examine their EHR documentation practices to ensure that claims are properly supported in the record. In particular, providers should scrutinize any "copy and paste" practices and consider limiting them to certain approved text or even prohibiting it completely to prevent any potential allegation of fraud by the OIG.

Providers should also implement compliance program policies that guide clinicians on documentation issues that could give rise to claim for fraud and abuse as well as ensure

its EHR system vendor is continuing to ensure the system meets the government's certification standards.

VIII. Electronic Medical Record Production During Discovery

Discovery is the legal process by which attorneys gather information and potential evidence relevant to their case. While discovery rules and deadlines vary from state to state, most states derive their discovery procedures from the Federal Rules of Civil Procedure. For example, in Louisiana,

> *"Discoverable evidence includes any matter, not privileged, which is relevant to the subject matter involved in the action. The information sought need not be admissible at trial as long as it appears reasonably calculated to lead to the discovery of admissible evidence."*

However, as mentioned above, because medical records (paper chart or EHR) are protected health information that requires compliance with HIPAA in order to be produced during discovery. For discovery purposes, EHRs are produced if:

> -HIPAA Compliant Authorization form signed by the patient, and addressed to a specific health care provider;
>
> -By Court Order and Subpoena

EHRs produced in compliance with HIPAA regulations still create issues for practitioners. It is well known by any healthcare defense attorney the difficulty of producing a complete, uniform and consistent copy of a patient's EHRs for litigation purposes upon request by a party. The nature of the EHR system and the complexities involved in obtaining a printed copy of voluminous health records intended to be read on

a computer screen are well recognized in the legal community.

EHR PRODUCTION REQUESTS

-Varies based on a state's discovery rules and procedure

-Example

-Virginia Sup. Ct. R. 4:9A(c)2 provides for the production of electronically storied information from a non-party provider when the information is reasonably accessible and does not create an undue burden or costs.

-FORMATS OF EHRS FROM PROVIDERS

-Nothing in HIPAA requires a health provider to have or allow access through a portal of any type, let alone a provider portal (access to review EHRs at the provider's office).

-HIPAA recognizes the right of a patient to access their medical records, but it does not grant access to that information in whatever format if that format creates an undue burden on the provider.

-In Lewis v. Kushner, 95 Va. Cir.50 (1/4/2017), the patient's attorney asked the court to enter an order requiring a non-party provider to make an employee available for the purpose of guiding counsel through EHR maintained through the "provider portal." The court cited Va. Code § 32.1-127.1 in its denial of said request:

-Health care records are required to be disclosed shall be made available electronically only to the extent and manner authorized by

HITECH and HIPAA. Notwithstanding any other provision to the contrary, a health care entity shall not be required to provide records in an electronic format if :(1) the electronic format is not reasonably available without additional costs to the health care entity; (2) the records would be subject to modification in the format requested; or (3) the health care entity determines the integrity of the records could be compromised in the format requested.

-The Court held, “The statutory language confirms the plaintiff is not entitled to her son’s health records in the format that she requested. Access to the “provider portal” is not reasonably available without additional costs to the provider because an employee authorized to use the system must accompany plaintiff’s counsel. And the employee’s presence is also needed because the records would be subject to modification or could be compromised.

-Based on this analysis, the court found the requested format is not reasonably accessible without undue burden, and the provider is not required to allow access through the provider portal.

CERTIFICATION OF EHRS

-Requesting a Certified Copy during discover

-Via affidavit of the records custodian, usually the first page of the record sent to the requesting attorney

-By testimony of the records custodian, provider administrator, or

treating physician at trial

-Certifying EHRs at trial

-Will vary from state to state

-In Louisiana, if the health record is a certified copy of the chart or record of any hospital, signed by the administrator or the medical records librarian of the hospital, shall be received into evidence as *prima facie* proof of its content, provided the party against whom the chart is sought to be used may summon and examine those persons making the original as a witness under cross-examination. *See,* LSA-R.S. 13:3714.

-Any health records which are stipulated to by all parties are considered certified or authenticated for trial use.