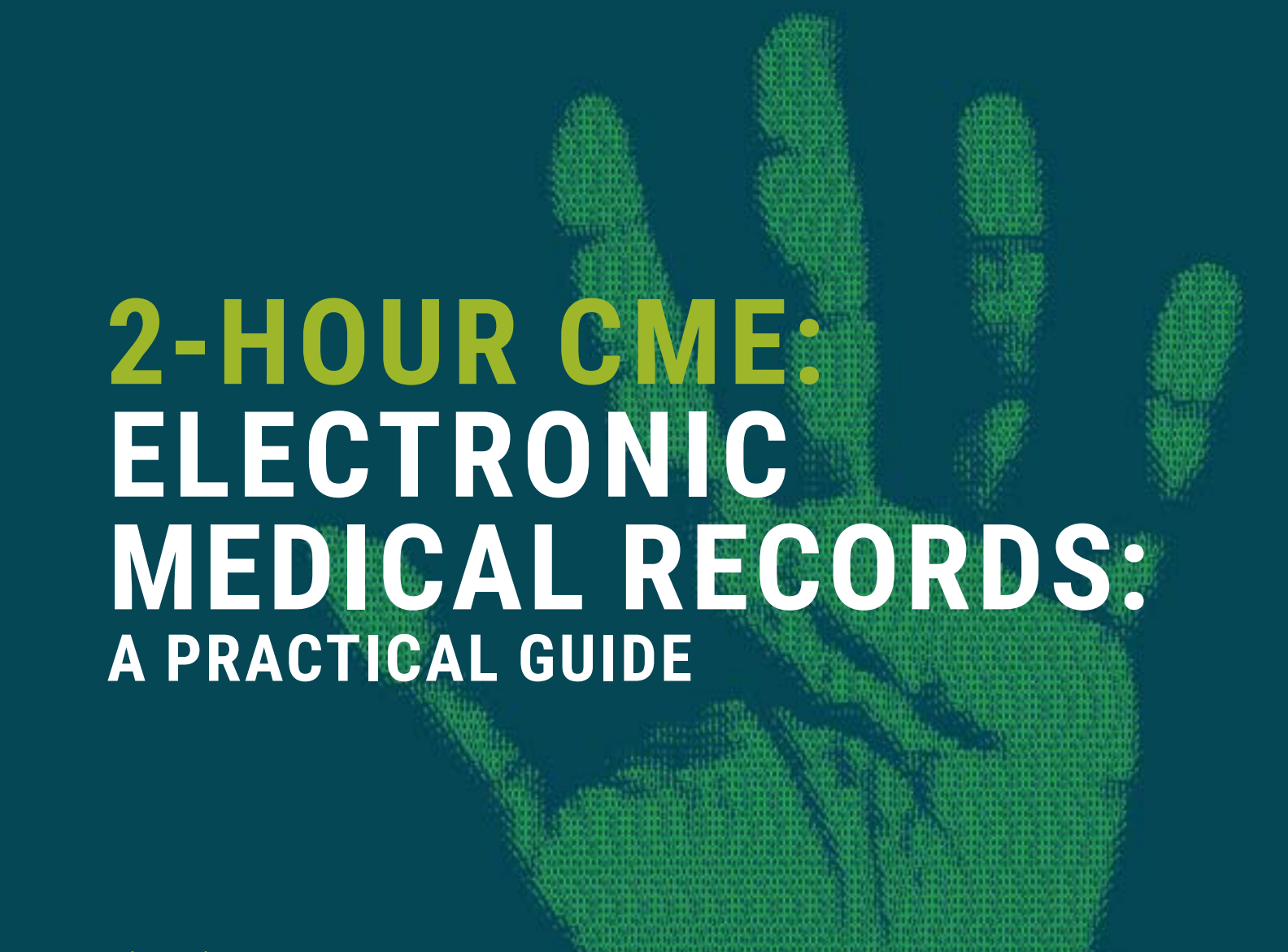
LONE STAR ALLIANCE
A RISK RETENTION GROUP

the REPORTER



2-HOUR CME: ELECTRONIC MEDICAL RECORDS: A PRACTICAL GUIDE

Also in this issue:

- **Wearable health technology: Risks, rules, and defenses**
- **Closed claim: Failure to monitor medication and order testing**
- **Closed claim: Delay in treating stroke**

Q2
Quarter 2, 2022

2-HOUR CME - ELECTRONIC MEDICAL RECORDS: A PRACTICAL GUIDE

by Karin Zaner, JD
with additional material by Laura Hale Brockway, ELS, Vice President, Marketing

OBJECTIVES

Upon conclusion of this course, the physician will be able to:

1. list potential advantages and disadvantages of using an electronic medical record (EMR);
2. identify the federal laws in place to protect patient privacy and personal health information;
3. discuss how to select an EMR for use in their practice; and
4. apply risk management strategies when using an EMR.

COURSE AUTHORS

Karin Zaner, JD of Zaner Law PC, represents Texas physicians and physicians in training. She earned her Bachelor of Arts with special honors in the Plan II Honors Program at The University of Texas at Austin, before earning her law degree from the UT School of Law. Ms. Zaner is a member of the Dallas Bar Association Health Law Section, serves on both the College of Liberal Arts Advisory Council and the Plan II Advisory Council at The University of Texas at Austin, and is a member of the College of the State Bar of Texas.

Laura Hale Brockway is the vice president of marketing at Texas Medical Liability Trust.

DISCLOSURE

Karin Zaner and Laura Hale Brockway have no relevant financial relationship(s) with ineligible companies to disclose. TMLT staff, planners, and reviewers have no relevant financial relationship(s) with ineligible companies to disclose.

TARGET AUDIENCE

This 2-hour activity is intended for physicians who are interested in practical ways to increase patient safety and reduce the potential for medical liability.

CME CREDIT STATEMENT

The Texas Medical Liability Trust is accredited by the Accreditation Council for Continuing Medical Education (ACCME) to provide continuing medical education for physicians.

The Texas Medical Liability Trust designates this enduring material for a maximum of 2 *AMA PRA Category 1 Credit(s)™*. Physicians should claim only the credit commensurate with the extent of their participation in the activity.

PRICING

The following fee will be charged when accessing this CME course online at http://lonestara.inreachce.com.

Policyholders: $25
Non-policyholders: $100

ETHICS CREDIT STATEMENT

This course has been designated by TMLT for 1 credit in medical ethics and/or professional responsibility.

TEST

To receive CME credit, physicians should complete the test questions that follow the activity. A passing score of 70% or better earns the physician 2 CME credits.

INSTRUCTIONS

the Reporter CME test and evaluation forms must be completed online. After reading the article, go to http://lonestara.inreachce.com. Follow the online instructions to complete the forms and download your certificate.

ESTIMATED TIME TO COMPLETE ACTIVITY

It should take approximately 2 hours to read this article and complete the questions and evaluation form.

RELEASE/REVIEW DATE

This activity is released on June 1, 2022 and will expire on June 1, 2025.

CME DISCOUNT

Lone Star Alliance policyholders who complete this program may earn a 2.5 percent discount that will be applied to their next eligible policy period.

DISCLAIMER

The closed claim study included in this article is based on an actual medical malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physician led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physician and the patient.

INTRODUCTION

As a practicing physician, you most likely spend a significant amount of time documenting the medical care and treatment provided to patients in the medical record. This usually means doing so in an electronic medical record (EMR) system.

Even if you do not have an EMR system in your office, you may be required to use an EMR at a hospital or other health care facility (HCF) where you have privileges. A physician may be required to attend hours of training on specific EMR systems (which may or may not be compatible) and spend time after-hours inputting patient information into the EMR. Otherwise, a "suspension of privileges" can occur if certain electronic records are not completed in a timely manner.

Gone are the days of simple paper charts, with their inconsistencies, disorganization, and reliance on how legible a physician's handwriting may be. Replacing these old concerns are newer challenges found with EMR use — challenges that can be substantial and many times

unforeseen. This article offers physicians a practical guide for making better decisions and avoiding risk exposures when using an EMR.

BASIC DEFINITIONS

The terms "electronic medical record," "electronic health record," and "personal health record" are often bandied about and used interchangeably. But what do they mean? How are they different? The following definitions can help clarify what actions are being discussed or what records are being accessed in a busy health care environment.[1]

Generally, the term "electronic medical record," or EMR, refers to digital versions of the paper charts found in clinician offices, clinics, and hospitals that contain "notes and information collected by and for the clinicians in that office, clinic, or hospital." Used mostly by providers for diagnosis and treatment, EMRs are arguably more beneficial than paper records because they "enable providers to track data over time, identify patients for preventive visits and screenings, monitor patients, and improve health care quality."

In contrast, the term "electronic health record," or EHR, usually refers to an electronic record that "contains information from all the clinicians involved in a patient's care and all authorized clinicians involved in a patient's care can access the information to provide care to that patient." An EHR may also share information and access with other health care providers, such as laboratories and specialists so that it can "follow patients – to the specialist, the hospital, the nursing home, or even across the country."

A "personal health record," or PHR, contains the same types of information as EHRs—diagnoses, medications, immunizations, family medical histories, and provider contact information—but are designed to be set up, accessed, and managed by patients. Patients can use PHRs to maintain and manage their own health information in a private, secure, and confidential environment. PHRs can include information from a variety of sources including clinicians, home monitoring devices, and the patients themselves.

With electronic prescribing, or "e-prescribing," health care providers can enter prescription information into a computer device, like a tablet, laptop, or desktop computer, and securely transmit the prescription to pharmacies using a special software program and connectivity to a transmission network. When a pharmacy receives a request, it can fill the medication right away.

Generally, e-prescribing is considered more convenient, cheaper, and safer and can improve health care quality and patient safety by reducing medication errors and checking for drug interactions.

A "patient portal" is a secure website that provides patients with access to their own health information online. Using a secure username and password, a patient can view their health information, such as recent doctor visits, medications, lab results, immunizations, discharge instructions, and other useful information. Patient portals may also allow a patient to securely update their contact information; download and complete forms and consents; send messages to a health care provider; request refill prescriptions; view or download educational materials; schedule appointments; check benefits and coverage; and make payments.

EMRs: A BRIEF HISTORY

The first EMR system was developed in 1972 by the Regenstrief Institute, a not-for-profit health care research organization. Due to high costs, this first EMR system was primarily used by the government and other big institutions instead of individual physicians. It was not until the 1990s, when personal computers became more available and affordable and internet use exploded that the concept and widespread use of EMRs became more feasible.[2]

Since then, federal health IT budgets and laws have expanded, encouraging the industry-wide adoption of EMRs. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was amended in 2009 to include the HITECH/Enforcement Rule, which provided specific requirements for the adoption of EMRs in the U.S.

The vehicle for HITECH was the American Recovery and Reinvestment Act of 2009. This act provided additional funding and incentives to encourage the adoption of EMR systems. The Office of the National Coordinator for Health Information Technology (ONC) leads these efforts, as the "principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information."[2, 3, 4]

Federal EMR adoption incentives to individual physicians who were able to demonstrate "meaningful use" of an EMR were up to $44,000 under Medicare or up to $65,000 over six years under the Medicare and Medicaid EHR Incentive Program. "Meaningful use" refers to specific objectives that eligible physicians and hospitals were required to achieve through their use of an EMR to participate in incentive programs.[5]

Along with financial incentives, these programs also incorporated penalties for failure to adopt and use an EMR by 2015. These penalties took the form of decreased reimbursements to providers under the same federal programs.[5] In 2018, CMS overhauled the meaningful use program and transitioned to the Merit-Based Incentive Payment System (MIPS).

In 2017, the federal government figures on EHR adoption showed that nearly nine in ten (86 percent) of U.S. office-based physicians (non-federal, and excluding radiologists, anesthesiologists, and pathologists) had adopted an EHR. In addition, nearly four in five (80 percent) office-based physicians had adopted a "certified" EHR. A certified EHR system meets the requirements adopted by the U.S. Department of Health and Human Services.[6]

ADVANTAGES AND BENEFITS OF EMRs

In concept, a properly structured and functional EMR (as opposed to a paper chart) includes many features that can increase patient safety and quality care. Various core requirements of "meaningful use" illustrate the many useful and significant capabilities that may be applied to each patient record when using an EMR. These capabilities include:

- using computerized order entry for medication, laboratory, and radiology/imaging orders;
- implementing drug-drug, drug-allergy checks;
- enabling electronic prescribing;
- recording demographics, such as gender, race, ethnicity, preferred language, and date of birth;
- maintaining an up-to-date problem list of current and active diagnoses;
- maintaining an active medication list;
- maintaining an active medication allergy list;
- recording and charting changes in vital signs;
- recording smoking status for patients 13 years or older;
- implementing and tracking compliance with a "one clinical decision" support rule;
- reporting ambulatory quality measures to the Centers for Medicare & Medicaid Services (CMS) or to individual states;
- providing patients with an electronic copy of their health information upon request;
- providing clinical summaries to patients for each office visit;
- being able to exchange key clinical information electronically among providers and a patient's authorized entities;
- protecting patients' electronic protected health information (ePHI) through implementing technical authentication, access control, and authorization measures;
- implementing drug-formulary checks;
- incorporating clinical lab-test results into a certified EHR as structured data;
- generating lists of patients by specific conditions to use for quality improvement, reduction of disparities, research, and outreach;
- sending reminders to patients for preventative/follow-up care;
- providing patients with timely electronic access to their health information, including lab results, medication lists, allergies, and immunizations;
- identifying patient-specific education resources and providing them to the patient, via certified EHR;
- recording advance directives;
- performing medication reconciliation;
- providing summary care record for transitions in care or referrals;
- having the capability to submit electronic data to immunization registries and actual submissions; and
- having the capability to submit electronic syndromic surveillance data to public health agencies and actual transmission.[7, 8]

When EMRs are configured with these "meaningful use" attributes, physicians can access updated and consistent patient information, such as medications, past and new test results, allergies, medical history, and diagnoses in multiple care settings. Providers can also enter orders and prescriptions electronically for immediate fulfillment.

EMRs encourage compliance with the most up-to-date best practices, as well as provide decision-support services such as preventing adverse drug interactions. EMRs also allow for electronic scheduling and response systems, such as automated appointment scheduling and reminders and responding to patients through patient portals, as well as other efficiencies in administrative services. And of course, EMRs allow secure electronic communication among providers and patients.

On a grander scale, EMRs allow for relevant de-identified data to be stored, accumulated, and analyzed for population and community research as well as for reporting patient safety and disease surveillance efforts.

Use of EMRs can also help decrease fragmentation of a patient's health care. For example, EMRs could potentially organize and even integrate a patient's protected health information (PHI) to facilitate instant distribution to authorized providers involved in a patient's care. This functionality is important for patients receiving treatment in an emergency setting, seeing multiple specialists, or transitioning to another provider and/or HCF. The immediate availability of updated EMRs can reduce medical errors and unnecessary tests, as well as ensure that a provider remains informed of a patient's condition while being seen by different specialists.

In addition, EMRs may encourage patients to participate more in their own care. EMRs allow patients access to their chart as well as to their current health information and updated disease management tools and resources. With EMRs, providers can schedule specific patient services such as blood pressure monitoring and control for patients with hypertension; blood testing for patients with diabetes; and breast cancer screenings as needed. Patients and physicians who share access to EMRs can better communicate and collaborate to determine the cause of a

Continued on page 8

Closed claim study: Ordering incorrect dose of corticosteroid

The following case study illustrates the importance of reviewing orders or emails before signing off with an electronic signature in an EMR.

PRESENTATION
A 50-year-old man was referred to a nephrologist for renal insufficiency. The patient had a history of ankylosing spondylitis and scleroderma. He had an elevated serum creatinine, low creatinine clearance, anemia, and proteinuria. The patient had previously been prescribed 5 mg of prednisone daily for treatment of his renal disease.

PHYSICIAN ACTION
The nephrologist felt there was no evidence of an acute scleroderma crisis to account for the patient's renal failure. He placed the patient on an ACE inhibitor. After 10 weeks on the ACE inhibitor, the patient's creatinine did not improve and his proteinuria was still significant.

The nephrologist believed the patient had an undefined connective tissue disorder characterized by probable membranous glomerulonephritis renal lesion. He followed the patient for several weeks. In the interim, the patient was seen by his rheumatologist, who increased the prednisone to 10 mg daily.

When the nephrologist next saw the patient, he documented that he discussed the possibility that renal replacement therapy would be needed. The patient indicated he did not want to go on dialysis because he was afraid it would impair his ability to work. The patient's kidney function continued to deteriorate.

During the next visit, the nephrologist decided to place the patient on 120 mg of prednisone every other day to see if renal function would improve. The physician sent an email to his nurse stating, "Kidney function is slightly worse. As a last-ditch effort to keep him off dialysis we need to have him take prednisone 120 mg every other day."

The next day, the nurse called the prescription in to the pharmacy for prednisone 120 mg every day and completed the medication summary in the chart to reflect 120 mg daily.

Using the practice's EHR, the nurse emailed a copy of the prescription back to the nephrologist, which reflected 120 mg daily. When the nephrologist, who had been out of town, returned 10 days later he simply signed off on several emails (including the prescription) without opening them. He clicked a signature box and deleted the prescription from his email list.

The pharmacy's computer flagged the prescription because the dosage was too high. The pharmacist called and spoke to the nurse, who confirmed the dosage. The patient's wife also questioned the dosage and was told by the nurse that the dosage was correct. (The nurse later testified that she confirmed the dosage in the computer system by looking at her documentation rather than the actual physician's original order.)

Nine days after beginning the daily prednisone, the patient came to the clinic for an epoetin alfa injection. He reported tremors, esophageal burning, hiccups, stomach pain and swallowing problems. The following day, the nurse emailed the nephrologist, who had just returned to the office, and told him of the patient's condition. The physician never saw this email and may have clicked it off his email list as he had done the prescription.

Eight days later, the patient called and spoke to the nephrologist, who was unaware of the prescription error. The patient said he was not feeling well, and the nephrologist advised him to drop his prednisone dose back to 10 mg per day. An appointment was scheduled for the next day.

When the patient arrived the following day, he had extremely low blood pressure, elevated heart rate, and was going into shock.

The patient was admitted to a nearby hospital where he was diagnosed with severe dehydration, gastrointestinal bleeding, and symptoms of sepsis. Despite treatment from several specialists, the patient died two days later.

An autopsy performed on the patient did not identify a cause of death. However, chronic gastritis was identified with angio-invasive GMS positive micro-organisms most consistent with aspergillosis. Multiple ulcers were found in the colon with full penetration through the muscular wall with reactive peritonitis. The center of the ulcer showed prominent necrosis. The patient was also found to have interstitial lung fibrosis bilaterally.

ALLEGATIONS

A lawsuit was filed against the nephrologist alleging:

- prescribing a high dose of prednisone;
- failure to properly order prednisone in the correct dosage;
- failure to properly supervise staff in placing an order for prednisone;
- failure to monitor the patient's progress; and
- failure to give appropriate medical orders to stabilize and maintain the patient's deteriorating condition.

The nurse and the practice association were also named in the lawsuit.

LEGAL IMPLICATIONS

In reviewing this case, defense consultants were critical of the prescription error by the nurse and her failure to detect the error when questioned by the pharmacist and the patient's wife. There was further criticism of the nurse for not reporting the patient's symptoms of esophageal burning to a physician.

Regarding the physician's action in this case, defense experts expressed their greatest concern regarding the sign-off of the emailed prescription. The physician indicated that he did not read the email because the way he pulled it up on the computer screen did not show the text of the email.

Some experts believed the physician had a right to expect the prescription would be called in as ordered, and it was not necessary to read and confirm the email sent to him regarding the prescription. However, the physician did sign off on the prescription with an electronic signature in the record.

The plaintiff's experts were critical of the nephrologist's decision to initiate steroid therapy and related the patient's death to the prescription error. However, the defendant's decision to place the patient on alternate-day high dose steroids was very well reasoned. One of the plaintiff's experts agreed with this decision, as did defense experts.

Defense experts also agreed with the plaintiff's argument that daily high dose steroids likely contributed to the patient's death. Though most believed that the patient's underlying systemic sclerosis was the primary cause of his death, placing him on steroids likely caused him to become sufficiently immunocompromised that he could not fight the infection when the perforations in his colon occurred. This led to overwhelming sepsis and organ failure.

DISPOSITION

This case was settled on behalf of the nephrologist.

RISK MANAGEMENT CONSIDERATIONS

With either paper or electronic records, standards of care and documentation requirements remain the same. There were two opportunities for the nurse to confirm the prescription with queries from the pharmacist and the patient's spouse.

A third opportunity to intervene and stop the daily dose was in the nephrologist's hands when reviewing email and signing off on orders. Signing off on unread orders can jeopardize patient safety.

medical issue, as well as make informed decisions about treatment plans.

Instead of a phone call or an in-office visit, the EMR (usually through a patient portal) can allow quick and easy communication and may prompt earlier and more accurate recognition of symptoms, diagnosis, and treatment. These functionalities can also tie into telemedicine capabilities and allow a physician to connect with patients, even when patients are not physically present in the physician's office.

Patient participation is important in managing and treating chronic conditions such as diabetes, obesity, depression, and allergies. With specific attention and guidance, physicians can offer full and accurate information about medical conditions through a patient portal or an email after a patient visit. Follow-up information from an office visit or hospital stay (such as self-care instructions, alerts, reminders for follow-up care, and links to web resources) can be sent to a patient with the click of a mouse.

In addition to these advantages, EMRs may benefit a physician's business. While an EMR system requires an initial investment in technology and training, adopting an office EMR can increase practice efficiencies and cost savings in a variety of ways. Some of the most obvious are the reduction of transcription costs and costs of pulling, re-filing, and storing medical records.

EMRs can save time by allowing for centralized chart management that prompts condition-specific queries and other shortcuts. And the EMR can enhance a physician's communications with other clinicians, laboratories, pharmacies, and health plans by allowing easy access to patient information from any secured location. This includes expediting the:

- order and receipt of lab tests and diagnostic images;
- issuance and handling of prescriptions to the patient's chosen pharmacy;
- automated formulary checks by health plans; and
- sending and tracking of electronic communications to other clinicians, health care facilities, laboratories, pharmacies, and insurers.

As for billing, the EMR allows for quicker, more accurate billing and less time and resources spent on manual entry. Lost or non-optimized charges are also lessened. With more accurate electronic billing, charge delays and insurance denials associated with late filing may also be reduced.

EMRs may also inform a physician of the requirements for an insurance claim, such as required treatments that must be attempted before another treatment will be covered (such as physical therapy before surgery) or if a test must be performed at a certain frequency to be covered.

DISADVANTAGES OF USING AN EMR

For many physicians, the promise of a well-functioning EMR system has not always translated into reality. Significant and varied barriers to EMR adoption have manifested over recent years, including the cost of EMRs

being too high for smaller practices to justify. In addition, once an EMR system is purchased, how can a practice be sure that the EMR system will not become obsolete?

Once an EMR is established in a practice, numerous difficulties and negative unintended consequences can occur, many of which have been detailed in recent, compelling media articles. For instance, when a data compromise involving EMRs happens, it can be on an epic scale and affect thousands of patients.

EMRs can be encrypted, which means that safeguarding the confidentiality of a patient medical record should be simple and effective. However, technical glitches, lost computers, and stolen mobile devices are realities. Granted, compared to the paper medical record, an EMR allows secure organization, management, and storage of current as well as old medical records for a minimal cost.

Providing copies and transferring records to a third party is quick, easy, and inexpensive when all that needs to be done is to make an electronic copy. But this assumes that such tasks are performed without human error, and such errors can happen with clicking the wrong button or a simple oversight in securing or encrypting the record.

These realities, coupled with the existence of hackers, phishers, and other cyber criminals intentionally trying to steal patients' ePHI, may cause a physician to question whether a patient's medical record might be more secure as a hard copy in a locked file cabinet.

FEDERAL AND STATE PATIENT PRIVACY PROTECTIONS FOR EMRs

As mentioned, HIPAA and HITECH are the main federal laws that safeguard a patient's PHI, whether in EMRs or paper records. HIPAA's Privacy Rule gives patients rights with respect to their own health information and sets limits on how this information can be used and shared with others.

HIPAA's Security Rule establishes how PHI must be kept secure with administrative, technical, and physical safeguards. Both criminal and civil penalties can be imposed under HIPAA and HITECH. The standard for determining the specific penalty for a breach of PHI involves an analysis of intent (i.e., was the breach intentional or caused by negligence?).

The Department of Health and Human Services (HHS), Office of Civil Rights (OCR) administers and enforces the standards of HIPAA and HITECH. Part of this process includes compliance reviews conducted by the OCR to evaluate breaches and assess civil and criminal penalties for noncompliance.

So, how do HIPAA and HITECH apply to EMRs? Generally, these laws apply to EMRs in the same way as they apply to paper records. That said, there is at least one important practical difference — when compared to paper records, the size of the breach may be enormous when an EMR is involved.

Each state has specific legal requirements for patient privacy and medical records. In Texas, House Bill 300 was adopted in 2011 that expanded the definition of a "covered entity" under Texas law; imposed new regulations in addition to HIPAA and HITECH for safeguarding PHI; and created harsher sanctions.[9, 10]

In particular, Texas HB 300 defines a "covered entity" as any individual, business, or organization that engages in the practice of assembling, collecting, analyzing, using, evaluating, storing, or transmitting PHI; comes into possession of PHI; obtains or stores PHI; or is an employee, agent, or contractor of a person or entity described above that creates, receives, obtains, maintains, uses, or transmits PHI.[10]

This means that, in addition to business associates that may come into contact or handle PHI through a covered entity, any person or entity in Texas (including law firms) that handle PHI (whether from a client, an opposing party or a third-party even if such party) is a covered entity.[10]

This expansive broadening of the definition of covered entity affects physicians in Texas because HB 300 provides specific "breach notification" requirements detailing what a covered entity and/or business associate should do if PHI protections for patients are compromised.

STATE REQUIREMENTS AND LEGAL LIABILITY FOR MEDICAL RECORDS

Briefly, each state has specific legal requirements for medical records that must be reviewed and taken into consideration to protect patient privacy. For example, the Texas Medical Practices Act, which is administratively enforced by the Texas Medical Board (TMB), sets forth the requirements of medical records in Texas.[11]

If you practice outside of Texas, please consult your state medical board for patient privacy legal requirements in your state.

In addition, under the Texas Civil Practice and Remedies Code, a "health-care liability claim" is defined as a cause of action against a physician or health care provider for treatment, lack of treatment, or other claimed departure from accepted standards of medical care, health care, safety, or *professional or administrative services directly related to health care*.[12] This could translate into a risk of legal liability for medical record errors. There also may be liability for falsifying or not maintaining medical records,

for wrongful release of confidential information, and for refusing to release medical records.[13, 14, 15]

Of course, a physician can be liable for a variety of actions and inactions relating to the treatment of patients or the practice of medicine, all of which will be reflected in the medical records (EMRs or paper records).

CHOOSING AN EMR FOR YOUR OFFICE

If a physician is either looking to invest in a new EMR or upgrade EMR systems, it is important they understand certain factors when selecting the best EMR vendor. The Texas Medical Association (TMA) has various resources on its website to help providers understand the relevant issues, ask the right questions, and prudently negotiate with EMR vendors.[16]

In particular, the TMA suggests that a physician request the following from their EMR vendor:

1. **Version protection:** Many vendors discontinue software only to resell the newer version. Instead, the vendor should offer future releases, system updates, and new versions at no cost.
2. **Government mandates:** The vendor should stay in compliance with all government mandates and modify its software at no cost.
3. **Technical support:** A vendor should stipulate that support fees cannot be increased by more than the consumer price index.
4. **Contract validity:** Ensure that the contract is not valid until the vendor meets certain acceptance requirements, such as the system operating as promised.
5. **Warranty:** Ensure that the vendor will correct any malfunctions at its expense, and that support fees will be waived while the malfunctions are being fixed.
6. **Malfunctions:** Stipulate that malfunctions not corrected within an agreed upon time will result in a full refund.
7. **Source code:** The vendor should put the source code into an escrow account.
8. **Transferability:** The vendor should allow you to assign or transfer your contract to a new owner.
9. **Additional users:** Require that future users can be added at a reduced cost.
10. **Protection:** Cyber security protection should be at the vendor's expense.[17]

When budgeting for an EMR, request a detailed cost analysis from the vendor to determine actual implementation costs. Common cost add-ons to consider include:

- training costs (computer-based tutorials, hired trainers);
- additional office staff costs (while staff are in training, assisting with design, development and/or implementation);
- temporary labor (initial EMR data entry, scanning the paper-based medical records);
- temporarily reduced income (reduced schedule as the EMR goes live);
- office construction and required fixtures (e.g., shelves, counters, wall mounts, power outlets);
- technical upgrade of office infrastructure (i.e., wireless network, upgraded network connectivity);
- additional hardware and devices including networking devices, scanners, printers, or kiosk devices; and
- for larger practices, consultants or project manager to facilitate the implementation.

In addition, a physician's office should either create or update policies and procedures to include EMR use and security protocols. These policies may include:

- physical office security policies;
- document retention policies;
- workstation log in and access policies;
- network authorization parameters;
- email and calendaring policies;
- remote access safeguards;
- protocols for using mobile devices;
- cloud storage and/or document sharing agreements;
- portal access agreements; and
- policies for storage, re-use, and disposal of devices.

Once an office EMR is installed, a physician should pay close attention to its operation and ensure that their office is compliant with the various legal requirements and standards discussed above.

While it would be advantageous if there were interoperability between a physician's office EMR and the EMR system at the hospital where the physician has privileges, this is not always the case. A physician should be aware of this possible disconnect and troubleshoot as needed to ensure that the office EMR has what it needs to fully reflect the medical care given to each patient at any location where care is given.

A physician should be especially attentive when working with advanced practice providers, transcriptionists, or medical record scribes. If the person is not an employee of the medical practice, ensure an appropriate Business Associate Agreement (BAA) is executed to comply with HIPAA/HITECH and state patient privacy laws. A physician should carefully train and supervise these individuals to confirm that they are complying with these laws as well as inputting and interacting with the office EMR appropriately and accurately.

Any breach of HIPAA/HITECH and state patient privacy laws must be disclosed consistent with the "breach notification" requirements discussed in this article. Further, a physician should be mindful of any obligations

to timely gather and respond to any requests for patient records from the patient or the patient's authorized representative, others physician offices, the TMB, or courts of law (through subpoenas or other court orders).

INTERACTING WITH A HOSPITAL, TEACHING INSTITUTION, OR LARGE EMPLOYER'S EMR

A physician with clinical privileges at a hospital, surgery center, or teaching institution may be required to use an unfamiliar EMR system – different than the one in their practice or office.

In these situations, to maintain medical staff membership and clinical privileges, a physician will have to agree under the medical staff bylaws to the EMR being used and be initially and periodically trained on the specific EMR system.

When using an "outside" EMR, the physician should attempt to follow these steps to secure the health information of patients and help reduce liability.

- Determine how to timely complete medical records in the EMR, including when and how to "sign off" as a physician on each entry. Medical records privilege suspensions can be imposed if a physician does not complete all medical records on time.
- Adhere to the security protocols of the EMR established by the HCF, including safekeeping of passwords, encryption, and preventing unauthorized access, malware, and viruses.
- If there is a mobile device (owned by the physician or provided by the HCF) that allows access to the EMR, protect the device by maintaining physical control of the mobile device at all times, as well as other mitigation strategies such as using passwords, remote wipes, timed lockouts, and wi-fi protection.[18]
- Avoid accessing the medical charts of patients that you are not treating or consulting on, as an electronic trail will be left which can open you up to allegations that you were "trolling"— a potential violation of HIPAA/HITECH.
- Refrain from making any unauthorized recordings or taking photographic or digital images (audio or video) independently (e.g., on a mobile device like an iPhone). Doing so is likely a violation of HIPAA/HITECH in a health care environment.
- Take additional care when exporting or forwarding any of the EMR from an HCF to a third party. While a physician with privileges at an HCF and treating a patient at the HCF may cause an EMR record (like an operating report) to be sent to their medical office for inclusion in their office medical record, that physician must not forward an EMR record to any other third party without an appropriate HIPAA/HITECH compliant purpose and BAA relationship.

RISK MANAGEMENT CONSIDERATIONS WHEN USING EMRs

The following risk management considerations provide additional guidance for physicians when working with EMRs in their own practice or in other settings, and when creating policies and procedures for their office.[19]

- **Implement a strict policy regarding access and security.** Authorized users of an EMR system are given login credentials. The system associates the person who enters this information as the author of the entry in the patient's medical record. It is critical that credentials only be used by the individuals to whom they were assigned.

- **Staff members should not have access to the physician level of security.** This kind of access would allow any staff member to add or alter information as if they were the physician. Each staff member should have their own login credentials and level of security clearance based on their job functions.

- **Avoid sharing login credentials simply to make the entry of information easier.** This can offer staff members access to records that they should not be allowed to access. It also makes your records and identity more vulnerable to theft.

- **Not all employees need access to the EMR.** Consider limiting access to those in direct patient care, or only allowing non-clinical staff to view (not enter or edit) information in the EMR. When an employee leaves the practice, delete their EMR password immediately.

- **Ensure patient encounter records are locked.** Information entered into an EMR is likely to be more accurate if completed during or immediately after a patient visit. The author of each entry must confirm that the entry is theirs and that it is accurate. Once a patient encounter entry is completed, the author should sign it, date it, and lock it in the system. Note that not all EMRs are set to perform this task automatically; make sure you know how to finalize and "lock" your notes in the EMR system.

- **Clearly identify addendums.** If information needs to be added or comments made after an entry is locked, clearly identify the new entry as an addendum with current date, reference to the original entry date, the reason for the late entry, and electronic signature. Unclear, after-the-fact entries may be viewed as alterations to the medical record, which can create legal complications. Most EMR systems now allow for easy, transparent addition of addendums or amendments to the record. Again, familiarize yourself with how your system captures this information.

- **Take extra care when using templates in the EMR.** Most EMRs have been designed with templates for patient encounters. Many EMR templates allow the importation of historical data. While this functionality saves time, some EMRs re-populate the same data in the templates for each subsequent visit. If not well edited, the notes may include old or inaccurate information.

  For example, a physician sees a patient who has conjunctivitis and this is noted in the "review of systems" section. At the next visit, if the physician does not edit the "review of systems" section, the conjunctivitis is again noted. It will continue to be picked up from the templates, giving the impression that the treatment plan is not working or that the physician is not editing the record.

  Also, some programs may be set up so that specific complaints default to "resolved" if the physician or the patient does not renew that complaint on the next visit. Notes should be individualized for each patient encounter, and relevant sections reviewed to avoid importing incorrect, redundant, and irrelevant information.

- **Make EMR templates your own.** Most EMR systems allow physicians to edit templates. Review templates for areas that are frequently left blank or unused and consider what might be removed or added to make templates more appropriate for your specialty and practice. Before making permanent changes to templates, review required documentation and coding/billing elements.

- **Make sure physician sign off is clear.** Another potential weakness identified in some systems — it is not clear to an outside reviewer that the physician signed the record at the end of the visit, or the physician believes they have “signed off” on the note when closing it but they have not. While physician review and/or signature could most likely be verified somewhere in the system, it is beneficial if the note itself includes an electronic signature and date.

  Additionally, some programs do not allow each clinical staff member making entries to authenticate the entry with a signature or initial. It is recommended that each staff member electronically sign or initial all entries in the medical record.

- **Review orders or emails before signing off with electronic signatures.** Signing an order is an affirmation that the order is correct. Avoid auto-authentication techniques that do not require the author to review the entry. Do not "universally" approve or sign off on a series of orders, emails, or internal messages without reading them.

- **Enable tracking mechanisms.** Most software programs include an electronic order tracking system to help ensure that patients have completed recommended tests or consultant referrals. These tracking systems can provide ways to:
  - verify that a patient keeps an appointment or completes a test;
  - confirm receipt of a report;
  - prompt a call to the consultant, imaging center, or lab if a report is not received;
  - make sure the physician reviews the report;
  - prompt communication of results to the patient;
  - assist in scheduling a follow up appointment if necessary; and
  - document all these steps with dates and electronic signatures.

  It is strongly recommended that physicians use these tracking systems. Additionally, if you are planning to purchase an EMR, an electronic order-tracking system is a critical feature to look for during the selection process.

- **Establish a system to appropriately capture paper and other external clinical documents.** Optimally, all paper documents should be scanned into the electronic record for easy access. These documents could include paper records used before implementing an EMR, diagnostic test results, consultant reports, hospital reports, or records from other physician offices. Additionally, a process should be implemented to ensure that, once scanned, the paper documents are properly stored or destroyed.

  Alternatives exist for practices working with systems that have limited memory or scanning capability. While scanning a patient's entire paper record into the system is preferred, it is not always possible. Some patients' previous medical records can be hundreds of pages. In these cases, physicians can review the records, summarize them, and include that information in the patient's history within the EMR. Whatever process you adopt, it is important to develop a policy for capturing patients' previous medical records and follow it consistently.

- **Ensure prescriptions are reflected accurately in the record.** Prescriptions are not always appropriately captured in the EMR. E-prescribing can be very helpful if it saves the information as part of the patient's medical record. If physicians who use EMRs are not consistently e-prescribing, prescriptions should be captured by scanning

Continued on page 14

Beware of unfamiliar third-party EMRs

Sometimes, unfamiliar third parties contact physicians with offers of earning extra income by providing medical care from home via telemedicine. Not all of these companies are reputable. There have been instances of fraudulent telemedicine and other health care companies luring otherwise prudent physicians into these types of schemes, which often seem very legitimate. If you are contacted by a third-party telemedicine provider, use extreme caution and watch for any of these "red flags."

- The companies are new, unknown, or unfamiliar and may be connected to locum tenens or other placement companies, even reputable ones.
- All patient intake, interface, and billing functions are done for the physician. The physician has no control over these functions.
- The physician does not see or talk directly to patients. How can a patient/physician relationship be established?
- Independent contractor relationships are required, although employment and ownership opportunities may also pose risk.
- An online EMR portal is used that maintains all medical and billing records, and the physician is unable to access patient records without the portal.
- Payment is $25-100 per "consult" (or more).
- When credentialing, the physician must allow access to their NPI number and e-signature, which can be placed on prescriptions or other parts of the EMR without authorization.

The potential for fraud and abuse involving telemedicine has been building for years. In 2019, the Department of Justice (DOJ) issued indictments of physicians and others under "Operation Brace Yourself." This telemarketing/telemedicine scheme allegedly fooled Medicare beneficiaries into signing up for unnecessary genetic tests, durable medical equipment (DME), and prescriptions, causing billions of dollars of alleged losses to the federal government.[20]

More recently, "Operation Happy Clickers" resulted in similar types of DOJ indictments. In this alleged scheme, physicians were paid by "telemedicine" companies to review and sign orders as a "telemedicine" visit, and the orders were then sold to DME supply companies and laboratories.[21]

Even if a physician is not criminally indicted or called to be a witness due to involvement, participation in these schemes is usually detected by insurance providers, hospitals, or other health care entities. The involved physician will also likely be reported to their state medical board.

Fraudulent third parties often seek NPI numbers and e-signatures of physicians for use in EMRs. Do not trust an unfamiliar third party with this information. Even if the physician has worked with the locum tenens company, often such companies are "middlemen," who pair a physician with a third-party company and then contractually disclaim all responsibilities.

Unless the third party is an established hospital, surgery center, teaching institution, or large employer, a physician should conduct his/her own due diligence to ensure that the third-party HCF is completely legitimate before undertaking any work or signing any contracts.

the paper prescription into the EMR or fully documenting the name, dose, quantity, frequency, instructions, and refill amount. Documenting only the name of the medication does not meet the documentation guidelines set by the TMB. Potential side effects or risks should also be documented. The same is true when dispensing sample medications to a patient.

- **Ensure records are backed up reliably.** The HIPAA security rule has specific requirements regarding the backup of ePHI. Patient ePHI should be created and maintained in a method that ensures an exact copy can be retrieved should the data be compromised from a disaster such as a cyber-attack or system failure. Periodic testing to ensure complete data restoration should occur for all back-up types, including onsite data created on a local hard drive and offsite data stored with a remote data center or cloud service provider. Even if an EMR vendor is providing offsite back up, it is recommended that practices test and confirm that a retrievable, exact copy of ePHI is being maintained and protected, and that full restoration is possible.

- **Make sure the records are complete when printing or generating electronic copies.** Many physicians using an EMR do not regularly print a patient record, and they may be unaware that clicking the print button does not always provide a complete record. A patient or subsequent treating physician could receive an incomplete record as the result of the EMR printing or electronic generation protocols. If the records request came from an attorney, and that attorney received an incomplete record, this could cause the attorney to consider a malpractice claim based on incomplete information.

  After printing or generating an electronic copy of the record, confirm the following are included:
  - the physician's electronic signature and signature date in the progress notes;
  - entries made by staff as indicated by their initials or unique identifier;
  - all lab and consult reports with the physician signature and date indicating timely review;
  - all medications prescribed, refills authorized, and samples given (if relevant);
  - patient consent forms; and
  - patient telephone calls, portal messages, and other communications.

  In some EMRs, this information is available on the screen but does not show up on the printed record when the print button is clicked. It may be necessary to go to phone notes, prescription refills, etc. and print or generate electronically each element individually to ensure that they are included in the complete record as requested. Confirming that a complete record is sent is a prudent risk management practice.

  When implementing systems to have a patient's paper records scanned, test the print function to make sure it captures everything from the scanned documents.

CONCLUSION

Fully understanding your EMR system and making sure all EMR entries are accurate and timely requires training, attention to detail, and time. Until there is interoperability, a physician may need to learn multiple EMR systems in different venues of their practice. Therefore, it is crucial for physicians to become proficient in their use, and to meet all EMR entry deadlines and amendment procedures. Establish strict rules, policies, and procedures to follow when using an EMR system.

SOURCES

1. Frequently Asked Questions. What are the differences among electronic medical records, electronic health records, and personal health records? HealthIT.gov. The Office of the National Coordinator for Health Information Technology. Available at https://www.healthit.gov/topic/health-it-and-health-information-exchange-basics/frequently-asked-questions. Accessed May 13, 2022.
2. EMR: The Progress to 100% Electronic Medical Records. The University of Scranton website. Available at https://elearning.scranton.edu/resources/article/emr-the-progress-to-100-percent-electronic-medical-records/. Accessed May 13, 2022.
3. American Recovery and Reinvestment Act of 2009. U.S. Government Publishing Office. Available at https://www.govinfo.gov/content/pkg/PLAW-111publ5/html/PLAW-111publ5.htm. Accessed May 13, 2022.
4. About ONC. What we do. HealthIT.gov. The Office of the National Coordinator for Health Information Technology. Available at https://www.healthit.gov/topic/about-onc. Accessed May 13, 2022.
5. Federal Register. Part II. Department of Health and Human Services. Centers for Medicare & Medicaid Services. 42 CFR Parts 412, 413, 422, et al. Medicare and Medicaid Programs; Electronic Health Record Incentive Program; Final Rule. Wednesday, July 28, 2010. Available at https://www.govinfo.gov/content/pkg/FR-2010-07-28/pdf/2010-17207.pdf. Accessed May 13, 2022.
6. Office-based Physician Electronic Health Record Adoption. HealthIT.gov. The Office of the National Coordinator for Health Information Technology. Available at https://www.healthit.gov/data/quickstats/office-based-physician-electronic-health-record-adoption. Accessed May 13, 2022.

7. Department of Health and Human Services. Centers for Medicare & Medicaid Services. Section 495.6. Meaningful use objectives and measures for EPs, eligible hospitals, and CAHs. Available at https://www.govinfo.gov/content/pkg/CFR-2012-title42-vol5/pdf/CFR-2012-title42-vol5-sec495-6.pdf.
Accessed June 14, 2022.
8. Posnack, S. Meaningful Use Grids: Quick Reference to Navigation. February 24, 2011. HealthIT.gov. The Office of the National Coordinator for Health Information Technology. Available at https://www.healthit.gov/buzz-blog/meaningful-use/meaningful-use-grids-quick-reference-navigation.
Accessed May 13, 2022.
9. For physicians practicing outside of Texas, please consult with counsel licensed in your state as well as your state medical board for guidance as to any state.
10. Texas Health and Safety Code. Title 2. Health. Subtitle I. Medical Records. Chapter 181. Medical Records Privacy. Available at https://statutes.capitol.texas.gov/Docs/HS/htm/HS.181.htm.
Accessed May 13, 2022.
11. Texas Administrative Code. Title 22. Part 9. Chapter 165. Medical Records. §§165.1-165.6. Available at https://texreg.sos.state.tx.us/public/readtac$ext.ViewTAC?tac_view=4&ti=22&pt=9&ch=165&rl=Y.
Accessed May 13, 2022.
12. Civil Practice and Remedies Code. Title 4. Chapter 74. Subchapter A. Section 74.001.13. Available at https://statutes.capitol.texas.gov/Docs/CP/htm/CP.74.htm#:~:text=74.001.,or%20indirect%20parent%20or%20subsidiary.
Accessed May 13, 2022.
13. Baylor Scott & White, Hillcrest Medical Center v. Ruthen James Weems III. Available at https://casetext.com/case/scott-v-weems.
Accessed May 13, 2022.
14. TTHR, L.P. v. Coffman. Available at https://casetext.com/case/tthr-lp-v-coffman.
Accessed May 13, 2022.
15. Thilo Burzlaff, M.D., P.A. v. Janet M. Weber. Available at https://caselaw.findlaw.com/tx-court-of-appeals/1891200.html.
Accessed May 13, 2022.
16. *See* TMA white paper "EHR Buyer Beware: Issues to Consider When Contracting with EHR Vendors." Texas Medical Association. Electronic Health Records. Available at https://www.texmed.org/EHR/.
Accessed May 13, 2022.
17. Before You Sign: 10 Tips for Tech Contracts. Texas Medical Association. Updated August 31, 2018. Available at https://www.texmed.org/TexasMedicineDetail.aspx?id=48476.
Accessed May 13, 2022.
18. Fact sheet: Take Steps to Protect and Secure Information When Using a Mobile Device. HealthIT.gov. The Office of the National Coordinator for Health Information Technology. Available at https://www.healthit.gov/sites/default/files/fact-sheet-take-steps-to-protect-information.pdf.
Accessed May 13, 2022.
19. Brockway L. Potential pitfalls: Risk management for the EMR. Texas Medical Liability Trust Resource Hub. Available at https://hub.tmlt.org/risk-management/potential-pitfalls-risk-management-for-the-emr.
Accessed May 13, 2022.
20. Press release: Federal Indictments & Law Enforcement Actions in One of the Largest Health Care Fraud Schemes Involving Telemedicine and Durable Medical Equipment Marketing Executives Results in Charges Against 24 Individuals Responsible for Over $1.2 Billion in Losses. Office of Public Affairs. The United States Department of Justice. April 9, 2019. Available at https://www.justice.gov/opa/pr/federal-indictments-and-law-enforcement-actions-one-largest-health-care-fraud-schemes.
Accessed May 13, 2022.
21. Press release: U.S. Attorney Announces Criminal and Civil Enforcement Actions Against Medical Practitioners For Roles in Telemedicine Fraud Schemes. United States Attorney's Office. Western District of Michigan. August 24, 2021. Available at https://www.justice.gov/usao-wdmi/pr/2021_0824_Happy_Clickers.
Accessed May 13, 2022.

Karin Zaner can be reached at www.zaner.law.

Laura Brockway can be reached at laura-brockway@tmlt.org.

WEARABLE HEALTH TECHNOLOGY: RISKS, RULES, AND DEFENSES

by Wayne Wenske, Senior Marketing Strategist

As technology finds new, increasingly powerful ways to enter our daily lives, the public's appetite for new, more personalized tech products seems to grow in tandem. Some of the most popular consumer products are wearable health monitors (wearables), such as Fitbits and Apple watches.

Consumers rely on such wearables to help them lose weight, increase their fitness levels, and stay personally accountable for reaching fitness goals. Consumers also use these devices to track how many steps they take in a day, calories consumed, or when to take medications. These devices can also be used to monitor or detect irregular heart rhythms, blood oxygen levels, stress levels, sleep trends, and even notify users when to wash their hands.

According to a recent Pew Research Center survey, 21 percent of U.S. adults say they regularly wear a fitness tracker or a smartwatch. Market forecasters predict that 320 million consumer health and wellness wearable devices (including smartwatches and medical-grade wearables, such as "smart patches") will ship worldwide to consumers in 2022, with that number reaching 440 million by 2024. But for many physicians, questions remain about how these wearables can be used safely to enhance patient care.[1, 2]

INTEGRATING PATIENT DATA INTO AN ELECTRONIC HEALTH RECORD (EHR)

During the COVID-19 pandemic, technology use between physicians and patients grew dramatically through telemedicine, patient portals, and, yes, data from patient wearables. As physicians and health care systems adjust to a "new normal," data collected remotely will likely be incorporated into a patient's medical record for monitoring patient information or helping to support a diagnosis.[3]

To address the integration of new technologies in health care, physicians and health care systems are increasingly working with their EHR vendors to ensure that data from virtual visits and other online health services is easily and seamlessly integrated into the EHR. However, according to a Deloitte Global survey of U.S. physicians, only 10 percent of respondents reported that they had transferred data from patient's wearables into their EHRs.[2]

Several good reasons exist for this lack of integration. One being that many health care systems lack the necessary technology to pull data from patient devices into different EHR systems. These differences make it difficult for various devices and EHRs to "talk to each other" and transfer data, leading to a lack of system interoperability. However, third-party applications are being used to address interoperability issues and streamline communication between patient devices and EHR platforms. It may only be a matter of time before a more established and ubiquitous solution for system interoperability is introduced.[4]

Another reason physicians may be reluctant to integrate this data is the perception that the data is not accurate. For example, inaccurate results have been recorded from these devices, often from users not wearing them correctly or as instructed.

PROTECTING PATIENT DATA

But for many, the biggest reasons for hesitating to integrate this data are questions around when, how, or if the data is protected and regulated under the Health Insurance Portability and Accountability Act (HIPAA). As set forth by the U.S. Office for Civil Rights, HIPAA specifies what covered entities and their business partners must do to ensure the security of their patients' protected health information (PHI).

Much of the information collected by wearables and health apps would be considered protected PHI if collected in a health care setting and would be subject to restrictions set forth by HIPAA and the Privacy Rule. The HIPAA Privacy Rule directs what circumstances and settings a patient's PHI may be shared, such as in the coordination of care between physicians. The rule also outlines how to keep PHI secure using administrative, technical, and physical safeguards. This includes guidelines for the safe communication and storage of electronic PHI, via such methods as patient portals, online insurance or financial interactions, and emails.

If an individual is using a wearable to collect their own health data for personal use, HIPAA does not apply. However, once a physician requests this PHI or transfers the patient's data from the wearable to an EHR system, that exchange is subject to HIPAA compliance standards and the Privacy Rule. Whenever data is transferred there is an inherent security risk — and the lack of oversight and regulation on how this data is shared may be the biggest risk these devices represent. As interoperability grows between wearables, apps, and portals, so will the risks of data misuse and breaches.

HIPAA PRIVACY RULE NOW APPLIES TO DEVELOPERS OF WEARABLE DEVICES

There is a growing consensus that failing to expand HIPAA to protect the data collected by these wearables and other applications may mislead consumers about the privacy of their wearable data and how it could be used. Consumers may not be aware of where their collected health data is stored or how developers and manufacturers may use the data for marketing or other uses.[5]

To help protect consumers, the Federal Trade Commission (FTC) now requires developers of health apps and other wearable devices that collect customer PHI (such as fitness trackers) to comply with the FTC Health Breach Notification Rule. Established in 2009, this rule requires that vendors of personal health records and associated

companies must notify individuals if there is a breach of their health data. While this does not extend HIPAA's governance over these vendors, it does make these vendors accountable to consumers in the event of a data breach.[6]

RISK MANAGEMENT CONSIDERATIONS

To help protect the data collected by wearables and integrated into an EHR, consider taking the following steps. [7, 8]

- Enable data transfers only from wearables that use two-factor authentication, encryption, or other effective defenses. Consult with your IT professional or department on how to best protect the transferred data, best practices for transferring data from patient wearables, and which wearables may or may not be integrated with your system.
- Establish a "protected space," perhaps on a dedicated server, where a patient's data is submitted. The data is then encrypted, summarized, and transferred into the EHR.
- Inform your patients on where the data transferred from the wearable is stored in your practice and how it will be used. Execute a shared agreement with patients on what exactly is collected and how it will be used or shared.
- Research what privacy regulations exist at the federal and state level for the devices you are using or sharing with patients.
- Maintain a strong cyber security profile in your practice, including regular upgrades and training for your staff members. Update policies and procedures as needed, expressly for the protection of PHI.

SOURCES

1. Vogels, EA. About one-in-five Americans use a smart watch or fitness tracker. Pew Research Center. January 9, 2020. Available at https://www.pewresearch.org/fact-tank/2020/01/09/about-one-in-five-americans-use-a-smart-watch-or-fitness-tracker/. Accessed May 23, 2022.
2. Louks J, Bucaille A, Stewart D, et. al. Wearable technology in health care: Getting better all the time. Deloitte Insights. December 1, 2021. Deloitte. Available at https://www2.deloitte.com/xe/en/insights/industry/technology/technology-media-and-telecom-predictions/2022/wearable-technology-healthcare.html. Accessed May 23, 2022.
3. Abrams K, Shah U, Korba, et. al. How the virtual health landscape is shifting in a rapidly changing world. Deloitte Insights. July 9, 2020. Deloitte. Available at https://www2.deloitte.com/us/en/insights/industry/health-care/physician-survey.html. Accessed May 23, 2022.
4. Dinh-Le C, Chuang R, Chokshi S, Mann D. Wearable Health Technology and Electronic Health Record Integration: Scoping Review and Future Directions. JMIR Mhealth Uhealth. September 11, 2019. Available at https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6746089/. Accessed May 23, 2022.
5. Belfort R, Bernstein WS, Dworkowitz A, et. al. A Shared Responsibility: Protecting Consumer Health Data Privacy in an Increasingly Connected World. Manatt, Phelps & Phillips, LLP. June 2020. Available at https://www.ehidc.org/sites/default/files/resources/files/RWJFConsumerHealth.pdf. Accessed May 23, 2022.
6. Alder S. FTC Tells Developers of Health Apps and Wearable Devices to Notify Individuals About Data Breaches. HIPAA Journal. September 16, 2021. Available at https://www.hipaajournal.com/ftc-tells-developers-of-health-apps-and-wearable-devices-to-notify-individuals-about-data-breaches/. Accessed May 23, 2022.
7. The HIPAA Compliance of Wearable Technology. BlogMD. MicroMD. January 16, 2019. Available at https://www.micromd.com/blogmd/hipaa-compliance-of-wearable-technology/. Accessed May 23, 2022.
8. Bonderud D. Wearable Tech in Healthcare: Possibilities and Pitfalls. HealthTech. April 19, 2021. Available at https://healthtechmagazine.net/article/2021/04/wearable-tech-healthcare-possibilities-and-pitfalls-perfcon. Accessed May 24, 2022.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.

FAILURE TO MONITOR MEDICATION AND ORDER TESTING

by Wayne Wenske, Senior Marketing Strategist

PRESENTATION

On July 10, a 63-year-old man came to a catheterization laboratory to undergo a cardioversion procedure by his cardiologist (Cardiologist A). The procedure was intended to help control his atrial fibrillation.

The patient had a long history of severe atrial fibrillation, including two catheter ablation procedures performed five and three years earlier by Cardiologist B, an electrophysiologist. A cardioversion procedure was also performed around the time of the second ablation. The patient also had a history of gastroesophageal issues and smoking.

The patient's medication history included low-dose aspirin, dabigatran, and dronedarone, an antiarrhythmic medication. Dronedarone was first prescribed by Cardiologist B "for a few months" after the first ablation procedure, five years earlier. The patient was again prescribed dronedarone, 200 mg daily, after the second ablation and instructed to follow up with Cardiologist A twice a year.

This closed claim study is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physicians and the patient.

PHYSICIAN ACTION

Cardiologist A did not perform the cardioversion procedure due to the discovery of a thrombus. Cardiologist A noted that the patient would be treated with anticoagulants and brought back to the catheterization laboratory in three weeks to attempt the cardioversion procedure again.

On August 4, the patient returned to see Cardiologist A. Again, the procedure was cancelled, and the patient was instructed to return in another three weeks. Cardiologist A noted that the patient was taking dronedarone daily.

The patient's next office visit was not until September 13, in which the patient informed Cardiologist A that he had recently been hospitalized for a gastrointestinal bleed. At this appointment, he was given a prescription for pravastatin. The patient returned on February 1. Cardiologist A documented that the patient was still taking dronedarone and that the prescription was being discontinued.

In March, the patient was hospitalized with pneumonia. An internal medicine physician noted that he suspected the patient had dronedarone-induced toxicity. The patient's dronedarone was discontinued during his hospital stay.

On June 13, the patient returned to Cardiologist A. The medication list from this visit showed that dronedarone was still an active medication for the patient. Cardiologist A documented that he would "restart dronedarone for rhythm control." However, records do not indicate that a new prescription was written or filled. The patient was referred to Pulmonologist A for evaluation of shortness of breath.

One week later, Pulmonologist A examined the patient and noted her concern about possible aspiration pneumonitis and rheumatoid and dronedarone lung toxicity. She noted that the dronedarone had been recently discontinued and re-started.

Pulmonologist A discontinued the patient's dronedarone and ordered pulmonary function tests and biopsies. Test results showed the patient had 50 percent pulmonary function.

On July 13, Pulmonologist A diagnosed the patient with dronedarone toxicity with significant pulmonary fibrosis. She noted that the patient had "fairly advanced disease" and that she was not optimistic for the patient's outlook. The patient was prescribed dexamethasone and continued to be treated by Pulmonologist A.

Progress notes from Pulmonologist A in December describe the patient as using a wheelchair, experiencing intermittent solid food dysphagia and some intermittent aspiration pneumonitis aggravating his underlying pulmonary fibrosis. Pulmonologist A recommended continuous use of oxygen.

ALLEGATIONS

The patient filed a lawsuit against Cardiologist A and Cardiologist B alleging that his dronedarone-induced pulmonary toxicity was due to their negligence. Allegations included failure to:

- reconcile medications at appointments;
- administer annual pulmonary function testing, as appropriate with dronedarone prescriptions; and
- properly supervise employees who authorized dronedarone prescription refills.

LEGAL IMPLICATIONS

Cardiologist consultants who reviewed this case for TMLT noted that patients receiving dronedarone for extended periods should undergo annual pulmonary function testing, as pulmonary toxicity is a known risk of continued use of dronedarone. Annual thyroid function testing and eye exam are also recommended. These consultants were critical of Cardiologists A and B for not appropriately tracking the patient's medications, and for not obtaining annual testing.

One consultant noted that the prescribing physician is responsible for ordering any tests to monitor a medication's efficacy and potential side effects. In this case, Cardiologist B prescribed the dronedarone and instructed the patient to follow up with Cardiologist A, believing that the patient's primary cardiologist would take on the responsibility of reviewing the anti-arrhythmic medication. However, this consultant felt that it was more appropriate for Cardiologist B to maintain responsibility for this prescription as an electrophysiologist specializes in treating arrythmias.

Poor documentation was also a factor, as the patient's record clearly identified that he was taking dronedarone, but it was unclear how long he had been taking it, who prescribed/refilled it, and whether any surveillance testing had been ordered.

Consultants for the plaintiff were also critical of the poor documentation and communication between Cardiologists A and B. One consultant expressed that Cardiologist B breached the standard of care by failing to obtain surveillance testing. He believed that if early warning signs of pulmonary toxicity had been detected, the medication could have been stopped before damage became irreparable.

This same consultant stated that Cardiologist A breached the standard of care for not tracking the patient's extended dronedarone prescription. He felt that Cardiologist A should have consulted with Cardiologist B regarding the

continued prescription of dronedarone, to confirm if annual testing was being conducted, and to obtain test results.

DISPOSITION

This case was settled on behalf of the cardiologists in this case.

RISK MANAGEMENT CONSIDERATIONS

In this case, the cardiologists failed to communicate with each other about their individual roles and responsibilities in the care of the patient, specifically regarding prescriptions and follow up. Poor documentation also complicated the defense of this case.

This case emphasizes the importance of increased communication between providers and transparency of patient treatment plans and progress. If it is unclear who is undertaking primary management of a specific medication, physicians should communicate and determine a plan for medication management and monitoring.

Practice policies should include documentation requirements for the electronic health record (EHR) to ensure all patient information accurately reflects the patient's current medications and treatment status. Well-organized and complete medical records are necessary to maintain the integrity of a patient's care plan.

Medications should be reconciled with the patient at every encounter to monitor compliance, avoid adverse drug reactions, identify new medications or treatments since previous appointments, and determine the patient's tolerance of a medication. Document when patients are advised or required to complete any lab work or tests — and when the test results are received and read by the ordering physician.

Written and oral instructions about a medication should be provided to the patient when prescribed and throughout the patient's course with the drug. It is important that this education be in simple terms and include the risks and benefits of the medication. Instruct the patient to inform you immediately of any adverse reactions. In this case, there was no indication that the patient was educated about the dronedarone and its side effects.

In this case, the record was confusing about when the dronedarone prescriptions were refilled and who authorized them. Refills from the offices of both cardiologists were periodically obtained over three years but were not consistent.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.

DELAY IN TREATING STROKE

by Rachel Pollock, Marketing and Brand Specialist, and Wayne Wenske, Senior Marketing Strategist

PRESENTATION

A 60-year-old man came to his primary care physician (PCP) with fever, body aches, and blue discoloration of the hands and fingertips for one week. The PCP believed it to be Raynaud's Syndrome and recommended hospitalization due to the patient's fever and elevated antinuclear antibodies (ANA).

This closed claim study is based on an actual malpractice claim from Texas Medical Liability Trust. This case illustrates how action or inaction on the part of the physicians led to allegations of professional liability, and how risk management techniques may have either prevented the outcome or increased the physician's defensibility. This study has been modified to protect the privacy of the physicians and the patient.

PHYSICIAN ACTION

That evening, the patient was admitted to a local hospital. The consulting rheumatologist's (Rheumatologist A) impression was that the symptoms suggested a vasculitis process. A course of prednisone and an angiogram of the upper arms and hands were ordered.

The next day, a bilateral upper extremity angiogram showed the patient in good condition. Radiologist A documented his impression as:

> "Bilateral upper extremity angiogram demonstrates poor flow to the digital arteries pre administration of nitroglycerine, which improved post administration of medication. However, no focal stenosis or complete occlusions were noted. Several digital arteries appear to be hypoplastic following administration of nitroglycerine."

After the angiogram was completed and the patient was transferred to a stretcher, the patient experienced nausea and weakness in his left upper arm and left side of his face. A stroke code was called, and Radiologist A ordered an immediate head CT.

At 4:34 p.m., a CT scan was completed and did not demonstrate evidence of an acute stroke or hemorrhage. At 5:05 p.m., the PCP was notified of the results and ordered a neurology consult. The consultation report notes that Radiologist A contacted Neurologist A at 7:25 p.m., two hours and 20 minutes after the consult was ordered, more than three hours after the onset of symptoms.

Neurologist A completed his consult via telemedicine and recommended the patient be immediately treated with a tissue plasminogen activator (tPA), since it was still within the 3 to 4.5-hour therapeutic window for administration. The order to administer the tPA was given at 8:10 p.m., approximately 3.5 hours after the CT was completed.

Radiologist A had the patient moved from the PACU to the ICU to discuss the risks and benefits of the tPA with the patient. Radiologist A also expressed his concerns about hemostasis at the injection site to Neurologist A, citing the recent arterial puncture for the angiogram. However, the puncture site was compressible.

The patient consented to the treatment. However, transferring the patient to the ICU did not leave enough time for the tPA to be prepared and administered. At 8:50 p.m., while the tPA was still being prepared, Neurologist A cancelled the tPA order as it was then outside the therapeutic window.

The following morning, the patient continued to display left-sided weakness. An MRI showed a large acute to sub-acute cerebral infarction in the right middle cerebral artery territory. The patient was given prednisone and discharged five days later to a rehabilitation center for physical therapy.

ALLEGATIONS

A lawsuit was filed against the PCP, Rheumatologist A, and Radiologist A with allegations of failure to:

- appropriately and timely administer the tPA;
- timely obtain a neurology consult; and
- timely treat the stroke.

The patient alleges that these failures caused permanent weakness in his left arm. The patient now uses a wheelchair, is incontinent, has cognitive issues, and can no longer work.

LEGAL IMPLICATIONS

Radiology and neurology consultants for TMLT were critical of Radiologist A's involvement in the delay in administration of the tPA. They agreed that administration of the tPA to avoid stroke should have taken priority over the risk of hemostasis. An internal medicine physician who reviewed the case felt that the PCP could have been more active in expediting the neurology consultation, as this would have allowed more time for all of the physicians to express and resolve their concerns.

Two plaintiff experts stated that Rheumatologist A violated the standard of care by recommending an upper extremity angiogram, as they did not think there was sufficient evidence of Raynaud's Syndrome or that the patient was at substantial risk of losing a finger or developing ischemic ulcers. They further stated that if Rheumatologist A had not ordered the angiogram, the patient would not have experienced a stroke. In addition, if the patient had received the tPA in a timely manner, he may have shown significant improvement.

DISPOSITION

This case was settled on behalf of the PCP, Rheumatologist A, and Radiologist A.

RISK MANAGEMENT CONSIDERATIONS

Poor documentation and communication between the providers contributed to the outcome in this case. Neurologist A wrote an addendum to the patient's record stating that when he learned that the tPA had been delayed because the patient was being transferred from the PACU to the ICU, he explained to Radiologist A that the tPA should have been administered in the PACU to avoid such delays.

Neurologist A also noted that the initial neurology consult was ordered by the PCP as non-emergent, and that he encountered additional delays when attempting to attain an accurate history of the patient.

Radiologist A was criticized for inserting himself into the decision of whether the tPA should be administered, as he was not a member of the stroke team. However, Radiologist A noted that there was a gap of time (from 5:05 p.m., when the head CT was completed, to 7:25 p.m., when the neurology consult was ordered) when no action was taken by the stroke team. Radiologist A chose to contact Neurologist A at 7:25 p.m.

There was no documentation in this case of which physicians were on the stroke team; whether the hospital's on-call neurologist was consulted in this case; nor who was responsible for administering the tPA. Many consultants in the case noted that administering the tPA was outside the scope of practice for Radiologist A and that he should not have been expected to administer it.

Maintaining clear, complete, and contemporaneous documentation can benefit physicians in the event of a claim and increase the quality and continuity of patient care. When making clinical decisions outside a scope of practice or that contradict a specialist, it is important to document the rationale behind those decisions. Had Radiologist A documented more fully the reasoning for his concerns about excessive hemostasis or for transferring the patient to the ICU before the tPA could be administered, his defense may have been stronger.

The hospital also failed to establish and reinforce internal protocols, including the delineation of the roles and responsibilities of its physicians and specialists. There was also a lack of attention given to critical test results and consults. The patient's outcome in this case may have been improved with clearer assignments of physician roles and responsibilities and a higher level of communication for this patient's emergent care.

Rachel Pollock can be reached at rachel-pollock@tmlt.org.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.

the REPORTER

LONE STAR ALLIANCE RRG
P.O. Box 160140
Austin, TX 78716-0140
844-595-8866
www.lonestara.com

LONE STAR ALLIANCE
A RISK RETENTION GROUP