

THE PRACTICE REVIEW



THE ELECTRONIC MEDICAL RECORD: RISK MANAGEMENT ISSUES FOR PSYCHIATRISTS

The shift from paper to electronic medical records has lagged far behind other digital leaps. Now, propelled by government incentives, this technology is poised to mount, if not a sweeping revolution, then a slow and steady advance. The transformation is expected to both benefit and complicate the practice of medicine, with perhaps the greatest challenges facing those in the field of psychiatry.

According to the previous and current presidential administrations, the electronic medical record (EMR) has the potential to improve clinical outcomes and forms the very basis of healthcare reform. The government's commitment to this endeavor is reflected in the American Recovery and Reinvestment Act of 2009, which allocated billions of dollars in incentives to clinicians and hospitals who implement certified EMR systems beginning in 2011.

Providers may receive up to \$44,000 under Medicare and up to \$63,750 under Medicaid over ten years. Eligibility is determined by a series of criteria released in July 2010 by the Centers for Medicare & Medicaid Services. These criteria define the minimum requirements that a provider must meet to demonstrate "meaningful use" of electronic records.

These initiatives are expected to accelerate the widespread adoption of EMRs in the United States and bring new

opportunities for physician liability. This article will provide an overview of the potential benefits and perils of EMRs to the practicing psychiatrist, followed by recommendations to manage the risks of this evolving technology.

A CLOSER LOOK AT THE EMR

The electronic medical record, also commonly referred to as the electronic health record (EHR), consolidates each patient's relevant medical information into a unique, digital storehouse. Clinical findings, diagnostic testing, treatment plans and outcomes can be documented in pre-existing templates. Decision prompts based on clinical practice guidelines are provided and electronic submissions to the pharmacy can signal alerts of patient drug allergies and potential interactions with previously prescribed agents.

The primary goal of EMR technology, however, is the exchange of medical information across clinical settings and specialties. Fragmented patient data sequestered in files of individual specialists at separate locations can be consolidated into a single electronic record and relayed across an expanded digital network. The result will be a comprehensive picture of the patient's health status that can be accessed by authorized clinicians at any point of care.

Clearly, the expected benefits of the EMR over the standard paper record

extend well beyond improved legibility. A better informed physician can make better decisions, with expected improvements in both treatment and outcomes during routine patient care. When faced with a psychiatric emergency or unresponsive patient, instant access to the medical record can be life saving.

Further, improved clinical efficiency is expected to reduce healthcare costs and malpractice claims due to medical errors. Indeed, important safety measures exist, but increased use of EMRs is expected to usher in liability concerns unprecedented in the era of the paper record. Ironically, it is the most critical function of the EMR – interconnectivity – that underlies the most significant risks associated with its use.

BREACH OF PATIENT PRIVACY

Privacy is paramount to the practice of psychiatry and the psychiatrist is primarily responsible for protecting confidential patient information. The psychiatric medical record includes psychiatric and sexual history, details of the diagnosis and treatment, and financial and other personal data. The records of children and adolescents are expanded to include confidential information about the parents, guardians and other family members.

The Privacy Rule under the Health Insurance Portability and Accountability

Act (HIPAA) was enacted in 1996 to help preserve the confidentiality of private patient information. Incorporated into the privacy rule is the Security Rule, in effect since 2005, which requires safeguards pertaining to the security, storage and transmission of electronic medical information. Despite these federal mandates, security simply cannot be guaranteed, especially in the electronic age.

ESCALATING THREATS

By design, the confidential information in a patient's EMR is available to a wider audience; including physicians, staff and administrative personnel in clinical settings and insurance companies. The EMR may also be subject to unauthorized access, a risk compounded at each stop on its digital path. Examples include accidental exposure following the inadvertent emailing to the wrong address or theft of physician laptops, flash drives or other storage devices.

Intentional, malicious access can also occur. Private information may be viewed on computer screens by unauthorized personnel as evidenced by highly publicized celebrity cases. Records can also be exposed through hacking. This risk that may be increased in smaller practices without advanced security systems; however, records housed in centralized servers outside of the clinical setting are also vulnerable.

This fact is underscored by the theft of confidential data from prestigious institutions such as the University of Miami Health System. The private medical information of more than two million patients was stolen from this institution's storage vendor, an event that was reported by the American Medical Association in 2008, three years after the enactment of the HIPAA Security Rule.

WITH A CLICK OF THE MOUSE

Once accessed, sensitive patient information can be sent skyrocketing across the internet and the consequences can be profound. The patient may experience overwhelming embarrassment and the loss of current and future opportunities. The psychiatrist may be subject to litigation for breach of privacy, regardless of whether it occurred through intended or unintended disclosure, hacking, or in some cases, defects in the EMR system.

Even if the worst never happens, some experts believe that the practice of psychiatry will be forever impacted by the lingering fear of exposure. The knowledge that their most personal psychiatric issues will be permanently etched into an electronic data base may deter patients from revealing private details. In turn, the psychiatrist may be hesitant to document stigmatizing disorders that may incur patient harm if disclosed. This imposes an additional burden on both patient and professional: to consider carefully the costs of unintended exposure of confidential information against the potential risks of withholding such information from the medical record.

ADDITIONAL RISKS

The implementation and use of an EMR system may expose psychiatrists to additional liabilities. While it is impossible to anticipate all potential risks, the following is a brief overview of the areas of greatest concern.

INFORMATION OVERLOAD

Many experts agree that the highest risk lies in the sheer volume of information contained in the EMR. With increased adoption of this technology, diagnostic and treatment summaries from each patient's previous visits with

multiple specialists will be accessible, and psychiatrists may be overwhelmed by the deluge of data. Because a careful review may require a time-consuming scroll through a series of crowded screens, a critical finding may easily be overlooked. This simple human error can lead to patient injury and exposes the psychiatrist to malpractice liability.

Time lost to information overload leaves less time to interact with the patient. This can impact patient care and diminish the quality of the therapeutic relationship. Patients who are dissatisfied with their treatment are more likely to initiate a malpractice claim if they view their interactions with the psychiatrist as unsatisfactory. This perception may be reinforced if the psychiatrist is distracted by the computer during the encounter.

SYSTEM USE AND DEFECTS

Time constraints may contribute to other factors that risk patient harm. A simple inputting error may send the wrong prescription to the pharmacy or propagate misinformation that can potentially alter therapeutic decisions at any future point of care. A physician may delay checking email and miss an update from a seriously-ill patient. System reminders regarding follow-up testing may be missed and complex templates and system protocols may further impede clinical work flow, especially during the transition from paper to electronic records.

The psychiatrist may elect to override computerized recommendations or alerts regarding patient care, especially if the prompts are frequent and distracting. Regardless of medical validity, each override is documented, forming an indelible electronic trail that may be used in court to support a claim of negligence.

“Protocols should be developed to manage security breaches and maintain the confidentiality of records during transmission to other specialists, and protocols developed to handle security breaches”

Interconnectivity allows for direct access to results of diagnostic testing by other specialists, which is an established benefit of this technology. Accordingly, the clinician may avoid duplicate testing, and choose to rely instead on prior results. However, this decision could increase liability risk in the event of poor treatment outcome or misdiagnosis, as could occur if the patient's condition worsened since the last evaluation.

A negligence suit may also result from liability related to product defects. Examples include patient harm associated with faulty equipment, the selection of a system known to be suboptimal, or continued use of a system found to be flawed after implementation.

MANAGING THE RISKS OF EMR TECHNOLOGY

It is impossible to measure the virtually limitless opportunities for patient harm that could result from the interplay of human error and computer malfunction as psychiatrists move from paper to electronic records. Accordingly, all potential liability risks to psychiatrists cannot be anticipated nor eliminated.

The most effective approach to risk management is through education. It is essential that psychiatrists stay abreast of changing government guidelines and consult their malpractice carriers for course offerings in risk management. Professional societies involved in EMR programs should be consulted on an ongoing basis. Such guidance is

invaluable in minimizing the factors that contribute to risks through the use of specific strategies, such as those outlined below.

SYSTEM SELECTION

The first and perhaps most essential step in risk management is the selection of an optimal EMR system. To qualify for government incentives and ensure the required functionality, the psychiatrist should choose a system that has been certified by a federally-recognized EMR certifying body such as the Certification Commission for Healthcare Information Technology (CCHIT).

Because start-up costs are often well in excess of \$20,000 and users require significant training during the transition from paper records, experts suggest that clinicians thoroughly investigate available options. Changing to another system down the road can be complex, time consuming, decrease clinical efficiency and increase security risks.

Consideration should be given as to whether the system should be based in the clinician's office or on the internet, where records stored on a vendor-owned server are accessed through a web browser. Each has important advantages and disadvantages. With local systems, records are stored within the clinician's office and may be more secure; however, computer malfunction or inadequate backup routines may lead to down time or data loss. With web-based systems, start-up costs

are lower and records are routinely backed up and can be accessed online from any location. However, as discussed previously, the storage of records on centralized servers controlled by outside vendors may increase risk of data loss or theft.

Recommendations should be sought from other psychiatric practices where EMRs have been in use for several years or more. Clinicians should study the advantages and limitations of each system and ensure adequate vendor support and training over time. Once installed, the clinician should allow adequate time for authorized staff to learn all relevant functional and safety features, especially during the transition period, when errors are most likely to occur.

PROTECTION OF PATIENT PRIVACY

From the moment the EMR system is up and running, securing the privacy of patient records will be a continuing challenge. Key individuals should be selected to be solely responsible for security. Protocols should be developed to manage security breaches and maintain the confidentiality of records during transmission to other specialists, and protocols developed to handle security breaches.

Access to the system and patient records should be limited to authorized staff. Patient records should be encrypted and guarded with complex passwords that are changed on a regular basis. Screensavers and privacy screens

should be used on computer monitors in public areas, such as reception and the psychiatrist's office.

PROTOCOLS FOR EMR MANAGEMENT

It is essential to remember that the psychiatric medical record is not only a chronicle of patient care, but a legal document. Good documentation remains the best defense against a malpractice claim. To provide optimal patient care and minimize the risk of liability, psychiatrists and their staff should become proficient in EMR management.

Office protocols should be established regarding all aspects of system use; including data access, input, backup, and transmission. Storage and preservation of patient records and emails are especially critical in the event

of a malpractice claim, as both are subject to the rules of discovery. Protocols should be established for managing system crashes and other malfunctions.

The psychiatrist should establish routines for reviewing and managing EMRs. To minimize the risk of overlooking vital data, this process should include the careful review of every screen contained in the record. The psychiatrist should avoid over reliance on prior diagnoses and testing. All new findings should be carefully added to the record and checked for accuracy, especially if entered by staff or other providers as signing off constitutes agreement. Careful consideration should be given when responding to or ignoring clinical decision reminders, prescription alerts, or laboratory notifications. The electronic imprint that

results could provide a powerful defense against a claim of negligence.

FINAL THOUGHTS

It will likely be years before all medical and legal ramifications of EMRs are revealed. Given the greater expectations of confidentiality in the psychiatric setting coupled with the increased threats inherent in this technology, securing electronic records and minimizing related risks will be an enduring concern for the practicing psychiatrist.

To this end, psychiatrists considering transitioning to electronic bookkeeping should become active in professional societies and state and local programs involved in EMR initiatives. This will provide them with the tools needed to manage ongoing risks as this technology continues to evolve.

– Susan Daubman

“The Practice Review”, published by the American Professional Agency, Inc. is provided as a risk management tool for psychiatrists and other mental health providers. This document is advisory in nature. It is offered as a resource to be used together with your professional insurance advisors in maintaining a loss prevention program. No liability is assumed by reason of the information this document contains. This publication will present brief overviews of liability exposures.

American Professional Agency, Inc.

Is the endorsed provider of the
American Psychiatric Association
Malpractice Insurance Program



95 Broadway, Amityville, NY 11701
(800) 421-6694

www.americanprofessional.com