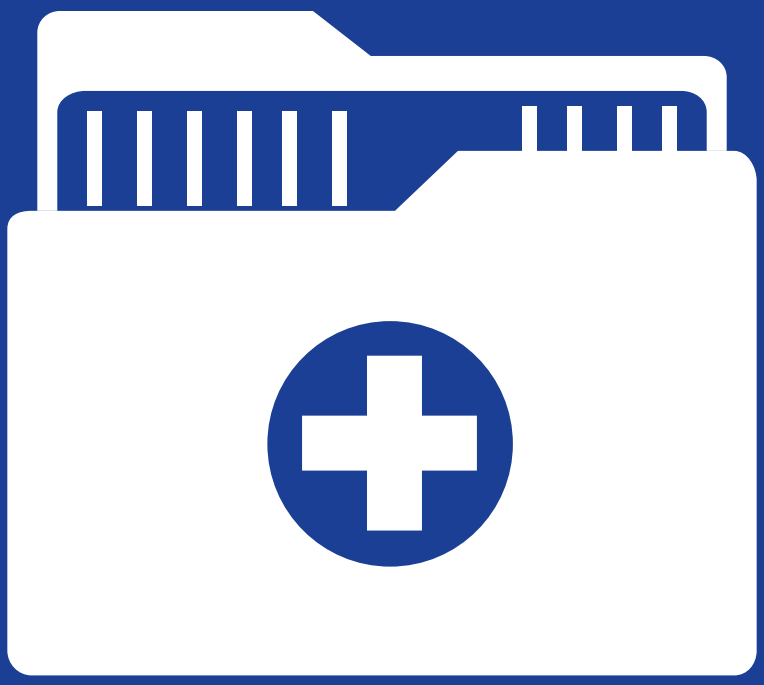
Rx FOR RISK IS A PRMS PUBLICATION

2017 | Volume 25 | Issue 2

Rx FOR RISK

Addressing risk management issues and concerns in the field of psychiatry

Documentation



Reading Rx for Risk on a screen?
Click on the page numbers below to be taken directly to that section of the newsletter!

Table of Contents

MYTHS & MISCONCEPTIONS: A PERFECT RECORD

Myth 1: It is possible to create a perfect record.

Truth: There is no such thing as a perfect record. As with most aspects of psychiatric practice, documentation remains a lifelong learning process, a perpetual skill-in-progress that must continually be reassessed in order to respond to changing demands and considerations.

A psychiatric record does not have to be "perfect," but it should be "good enough." What does that mean? While the specific *content* of a psychiatric record may vary, the *purpose* of documentation remains constant. A good record accomplishes several things: it substantiates your clinical judgment and choices, demonstrates the knowledge and skill you exercised during treatment, provides a contemporaneous assessment of the patient's needs and behaviors, and documents significant events, revisions to the treatment plan, and explanations of your decisions.

Myth 2: Unless you have a perfect record, you cannot win a lawsuit.

Truth: You do not need a "perfect record" to win a lawsuit, but you need to have one that is "good enough." It is true that documentation plays a vital role in the defense of a malpractice lawsuit; without adequate documentation it may be very difficult to demonstrate that you provided appropriate care. However, an experienced defense attorney can work well with a cooperative clinician and a "good enough" record. [See above for what constitutes a "good enough" record.] You should not become complacent, though; the reality that perfection can never be obtained should not prevent you from striving to create as complete and supportive a record as possible.

There is one *absolute* with regard to records and professional liability . . . NEVER ALTER A RECORD. Altering a record destroys your credibility in a lawsuit, could compromise your professional liability insurance coverage, could lead to sanctions from your medical licensing body, and will destroy your professional reputation. In addition, altering a record may be considered a criminal act.

YOUR MEDICAL RECORD HAS **THREE ESSENTIAL PURPOSES**:

1. To support good clinical care
2. To use in your defense and show compliance with legal requirements
3. To substantiate your billing and demonstrate your adherence to payer guidelines

PRACTICAL POINTERS FOR PSYCHIATRIC RECORDS

The importance of records in malpractice litigation cannot be overemphasized. A good psychiatric record accomplishes several things: It substantiates clinical judgment and choices; it demonstrates the knowledge and skill exercised during treatment; it provides a contemporary assessment of the patients' needs and behaviors; and it documents explanations of the provider's decisions, significant events, and revisions to the treatment plan.

Set forth below are risk management tips regarding psychiatric records.

DO know your state's laws regarding the creation and maintenance of patient records. Most states have statutes and/or regulations governing the creation and maintenance of patient records. Even when such requirements are absent, it is the standard of care to create and maintain a record for each patient.

DO review and be familiar with contractual obligations regarding record creation and maintenance in all provider contracts.

DO remember that there is no "statute of limitations" for disciplinary actions by licensing/medical boards or for ethics proceedings. Absent state and/or federal or contractual requirements, legal experts advise keeping records indefinitely and, *at a minimum*, until your state's statute of limitations runs. Remember, there are generally no statutes of limitations imposed on disciplinary actions by licensing/medical boards or on ethics proceedings.

DO establish separate sections within a record for clinical documentation, patient billing information, correspondence regarding the patient and records received from other health care providers or institutions. *Communications with personal counsel or the Risk Management Consultation Service (RMCS) should be kept separately in a personal administrative file.*

DO establish separate records for each and every person attending a patient's session. This will assist with maintaining confidentiality and will facilitate your ability to process requests for information in a timely manner.

DO keep records somewhere safe, accessible only to those who have authorization.

DO back-up computerized records and information daily, at a minimum. Be aware that if you choose to use a given technology, you will be held to the standard(s) associated with that technology. Consult equipment and software professionals for information about your system's back-up standards and capabilities.

DO document legibly. The record should be legible not only to the writer but to others, as well.

DO NOT wait to write or dictate record entries. Avoid waiting until the end of the morning/afternoon/day to make entries, because essential information can be forgotten.

DO date and sign or initial record entries. Keep a permanent listing of all past and present employees for reference. Include their names, signatures, and initials.

DO maintain the integrity of the entire record.

DO record identifying patient information on each page of the clinical documentation so that if it becomes separated from the record, it can be re-filed correctly.

DO NOT alter, amend, or expand a record. Altering records, especially to avoid looking bad, can be fatal to a case and may lead to a forced settlement due to the damage such changes would do to your credibility in court. Any alteration of medical records could jeopardize coverage under the terms of your professional liability insurance policy.

DO use accepted methods for correcting mistakes or omissions in a record. In situations where there is legitimate cause to correct a record, be sure that you carefully date the correction, clearly note that you are correcting an error, and sign or initial the correction. Make corrections using single line strike-through and date & initial the corrections. For corrections which involve more that a word or phrase, amend the original entry with a statement about where to find the correct information. Then, make a new entry (in current chronological order) indicating that a correction is being made and giving the correct information. Date and sign or initial both entries.

DO document dates (and length) of service, pertinent history, assessments, and prescriptions.

DO document informed consents, release of information authorizations, consultations with other health care providers, relevant correspondence, etc.

DO document psychological testing, physical examinations, laboratory data, etc.

DO document late shows, no shows, and appointment cancellations.

DO document what treatment options/actions were considered, what options/actions were chosen and why, and what options/actions were rejected and why.

DO document prescriptions and prescription refills.

DO document the discharge summary, if relevant.

DO document the termination of treatment process.

DO document phone calls between patients, third-parties, and the office.

DO document objectively and professionally. Documentation of the psychiatrist's thought process is an essential part of the record. S.O.A.P. notes or some variation thereof are preferable.

DO establish written policies and procedures to ensure that lab tests, consultations, and referrals have been completed, the subsequent reports have been received, reviewed, and initialed by you, and all paperwork has been filed appropriately. This system should also capture information received after an office visit regarding allergies, medications, and information received from patients' other health care providers. The timely filing of phone messages, lab slips, consultation reports, etc. greatly enhances the credibility of the record.

DO NOT include personal comments about patients, names of third parties, or other extraneous references which do not serve a therapeutic purpose.

DO NOT document contacts with personal counsel or the RMCS in patients' records. Consultations regarding legal or risk management issues should be maintained in a personal administrative file. No identifying patient information should be included.

DO NOT release information without proper authorization. Proper authorization usually means either a signed release authorization or a court order.

DO educate staff regarding the handling of records. Stress confidentiality. Ensure that all requests for release of information/records are reviewed by you for determination of proper authorization, identification of the specific information to be released, and analysis of the potential impact upon the patient(s) and others.

10 THINGS PLAINTIFF ATTORNEYS LOOK FOR

1. Documentation of informed consent/refusal
2. Documentation of a psychiatrist's thought process
3. Reasons for off-label prescribing
4. Self-serving/late entries
5. Documentation of any termination procedures
6. Finger-pointing/jousting
7. Documentation of prescriptions/refills
8. Documentation of follow-up efforts
9. Documentation of contacts with/regarding patients
10. Altered records

RETAINING AND DISCARDING PSYCHIATRIC RECORDS

It should go without saying that a patient record exists for a reason -- it exists *primarily* to support good patient care. A good patient record accomplishes several things: It substantiates clinical judgment and choices; it demonstrates the knowledge and skill exercised during treatment; it provides a contemporary assessment of the patients' needs and behaviors; and it documents explanations of the provider's decisions, significant events, and revisions to the treatment plan. In short, it allows someone else (e.g., another physician) to know and understand what has happened during treatment and why.

A secondary benefit derived from a good patient record is the ability to provide a defense in an adversarial situation such as litigation or an administrative or ethics complaint. The importance of patient records in these types of situations cannot be overemphasized.

RETAINING RECORDS

How long should records be kept? There is no clear answer. Due to the variety of statutes, regulations, legal principles, and professional obligations affecting psychiatric records, the best risk management advice

dictates that records should be kept for as long as possible. The safest and most conservative option is to keep records indefinitely. Perpetual maintenance may seem excessive, but there are many reasons your records may be needed in the future. If records cannot be kept indefinitely, they should be kept as long as possible.

How long am I "legally" required to keep records?

Many states have statutes and/or regulations governing the creation and maintenance of patient records, including the time period for which records must be kept. Federal statutes and/or regulations may also address record maintenance. The time periods mandated in these statutes and regulations represent the length of time you are "legally" required to keep patient records, *at a minimum*.

In addition to statutory and/or regulatory requirements, there may be contractual obligations regarding record creation and maintenance in provider contracts, both explicit and implicit. Frequently, provider contracts include provisions mandating how long records must remain available to patients and insurance companies. If a contract requires you to keep records for a different amount of time than is laid out in the relevant statutes and/or regulations, then you should keep the records for whichever time period is the longest, at a minimum.

Absent explicit requirements, records should be kept *at least* until well after your state's statute of limitation for medical malpractice actions and/or statute of repose have run. The statute of limitations laws and/or the statutes of repose establish the time period during which a legal action may be brought against you. However, you cannot absolutely rely on these statutes to protect you from litigation. Depending on the nature and wording of a complaint, an action may be brought against you even though it is not brought within the limitation periods. In addition, statutes of limitations or repose do not apply to disciplinary actions by licensing/medical boards or to ethics proceedings. Professional complaints may be made against you at any time.

Why should I keep records indefinitely?

1) Continuity of Care

One of the most important reasons for retaining records is continuity of care. Patients may receive care from a patchwork of healthcare providers over time, and the psychiatric records may be necessary to ensure that patients continue to receive the care they need. Patients who find that they are unable to obtain their medical information whenever requested can initiate complaints with professional and licensing bodies. Increasingly, medical boards and state/federal regulators are starting to insist that patient records be available *whenever needed*.

2) Potential Lawsuits

Another reason records may be needed is litigation. In a legal proceeding against you, the record is the primary means of supporting and defending the care that was given. As mentioned above, your state's statute of limitations laws and/or statutes of repose exist to limit the time period during which an action may be filed, however there are exceptions to these statutes. For example, state law usually also contains provisions for "tolling" the statute of limitations in cases where the patient (i.e., prospective litigant) is a minor or suffers under some other legal disability or incompetence. This means that for some patients, the time in which a suit can be filed is extended.

Additionally, your state's statutes of limitations that limit the time during which malpractice actions may be filed against physicians may not limit the time litigation resulting from allegations involving fraud, conspiracy,

or criminal acts may be brought against you. Furthermore, these laws are not applicable to professional and ethical complaints or allegations involving federal laws, rules, and regulations (e.g., Medicare billing complaints).

3) Other Situations

There are other situations in which a record may be needed, besides defending you. For example, a patient may need the record to support his case against another individual (e.g., another healthcare professional or an employer) or to back-up a claim for disability benefits. Custody proceedings are another common example.

How do I store records?

Records should *always* be stored somewhere safe and secure, and should be accessible only to authorized individuals. All psychiatrists are ethically obligated to keep the psychiatric record secure. There may also be legal requirements under state law, as well as federal law. For instance, per HIPAA's privacy and security regulations, covered providers must comply with standards to ensure security and prevent unauthorized disclosure. Remember that the duty to maintain the confidentiality of patient records does not diminish over time, nor does it cease to exist upon the death of the patient.

Should you choose to keep your records indefinitely or for an extended period of time, you may want to consider using a professional records storing company. Such companies may be found online or through the records department of the local hospital or medical society. Your personal attorney or accountant may also be able to suggest a company.

If a storage company is used, it should have experience handling confidential medical information, guarantee the security and confidentiality of records, and allow access by authorized individuals. You should have a written agreement with the storage company. Topics which should be addressed specifically in the written agreement include but are not limited to confidentiality and privilege, release of information, time in which it will take to retrieve records, and destruction of information. If you are a covered provider under HIPAA's Privacy Rule, you will need a "Business Associate Agreement" with the storage company. All contracts should be reviewed by personal counsel.

DISCARDING & DESTROYING RECORDS

If, after careful consideration, you do decide to discard and destroy patient records, there are some important considerations to keep in mind. Primarily, you should develop and implement a retention schedule and destruction policies and procedures. Records involved in open litigation, investigation, or audit should *not* be destroyed.

How do I discard & destroy records?

Should you choose to discard and destroy records, it is *imperative* that you establish and follow written policies and procedures for doing so. Following an established procedure may help to mitigate potential allegations that a record was destroyed in order to conceal unfavorable information. It *cannot* be guaranteed to protect you from situations in which you need the record; the absence of a record is problematic in any type of proceeding.

Some jurisdictions require that you notify patients that their records will be destroyed. Even if not required, notifying patients is always prudent. Patients may want copies forwarded to them or their current physician for future use. Remember to always obtain a proper release authorization prior to releasing any information.

Destroy *completely* all records and copies of records selected for discarding. Different media require different methods of destruction: shred, burn, or pulverize paper records; recycle or shred microfilm or microfiche; purge and destroy computerized records. Whatever method is used, ensure that third parties cannot discern or reconstruct patient information from destroyed records.

Retain a log of what records were destroyed, how and when they were destroyed, the inclusive dates covered, what method of destruction was used, a statement that the records were destroyed in the normal course of business, and the signatures of the individuals supervising and witnessing the destruction. Maintain destruction documentation permanently.

In addition, you may want to consider keeping an abbreviated patient record containing basic information, including the intake form, dates of treatment, diagnosis, release of information forms, termination forms, and case summaries, etc.

Who else can I contact for information?

For additional information on retaining and discarding records, contact your state medical board, your local medical society, your local APA district branch, and other professional medical organizations to which you belong. The American Health Information Management Association (AHIMA), a professional healthcare information organizations, is an invaluable resource.

Risk management tips for retaining & discarding psychiatric records.

DO review and be familiar with statutory, regulatory, and contractual obligations regarding records creation, retention, and discarding. In addition to federal law, including HIPAA, most states have statutes and/or regulations governing the creation, maintenance, and discarding of patient records. Even when such requirements are absent, it is the standard of care to create and maintain a record for each patient. The safest and most conservative option is to never destroy patient records.

DO understand that you cannot absolutely rely on your state's statute of limitations for medical malpractice or the statute of repose to protect you from legal actions. Depending on the nature and wording of a complaint, a legal action may be brought against you even though it is not brought within the limitation period.

DO understand that the records of minors and patients with some other legal disability or incompetence may fall under statutory tolling provisions. This means that for some patients, the time in which a suit can be filed is extended.

DO understand that your state's statutes that limit the time during which malpractice actions may be filed against physicians would not be applicable in litigation resulting from complaints or allegations involving fraud, conspiracy, criminal acts, or federal laws, rules, and regulations. For example, your state's statute of limitations laws would not apply to allegations of Medicare billing fraud.

DO remember that there is no "statute of limitations" or "statute of repose" for disciplinary actions by licensing/medical boards or for ethics proceedings. Absent state and/or federal or contractual

requirements, legal experts advise keeping records indefinitely and, *at a minimum*, until well after your state's statute of limitations for medical malpractice and/or statute of repose have run.

DO keep records somewhere safe and accessible only to those who have authorization.

DO consider using a professional records storage company. Since you are responsible for ensuring the confidentiality of your patients' records, make sure that the records storage company agrees to protect patients' confidentiality in your agreement/contract with the company. If you are a covered provider under HIPAA's Privacy Rule, the confidentiality agreement with the records storage company is a "Business Associate Contract", containing all the elements required under that regulation

DO develop and implement a retention schedule and written policies and procedures for destroying records. Following an established procedure may help to mitigate future potential allegations that a record was destroyed in order to conceal unfavorable information. It *cannot* be guaranteed to protect you from situations in which you need the record.

DO NOT destroy records involved in open litigation, investigation, or audit.

DO destroy *completely* all records selected for discarding. Different media require different methods of destruction. Ensure that third parties cannot discern or reconstruct patient information from destroyed records.

DO retain a log of the destruction. Include information about what records were destroyed, how and when they were destroyed, the inclusive dates covered, what method of destruction was used, a statement that the records were destroyed in the normal course of business, and the signatures of the individuals supervising and witnessing the destruction. Maintain destruction documentation permanently.

Additional Resources:

American Health Information Management Association (AHIMA): www.ahima.org

American Psychiatric Association (APA): www.psych.org

American Medical Association (AMA): www.ama-assn.org

American Hospital Association (AHA): http://www.aha.org

EHRS AND DOCUMENTATION

Many psychiatrists are either now using or are contemplating the use of electronic health records. The first thing to remember is that no matter how good the system, what you get out of it will only be as good as what you put in. In other words, garbage in, garbage out. If you have not been thorough with your documentation in the past, your EHR system might make your record look "prettier" but it will not in and of itself create a record that supports good patient care and would be useful in your defense in a claim or a lawsuit.

TRANSITIONING FROM **PAPER TO ELECTRONIC RECORDS**

Unless you are starting your practice from day one using an EHR system, you are going to have a period of transition. It is during this time that you must be particularly vigilant to avoid documentation errors and gaps. Courts and licensing boards will not "cut you any slack" during your transition/learning period. You will be expected to practice to the same standard of care and are responsible for implementing procedures a reasonable provider would implement to avoid errors. To that end, you should recognize, and take steps to minimize, the following risks:

- Documentation gaps – how will you maintain and refer to your paper charts?
- Mental fatigue from treating patients while learning a new system
- Inadequate training/inconsistent use among staff leading to errors

Concerns about patient safety and the use of electronic health records have been in the news for years. As the use of this technology has grown so have these concerns. In 2015 ECRI Institute listed errors associated with EHR use among its Top 10 Patient Safety Concerns and the Joint Commission issued a Sentinel Event Alert on the Safe Use of Health Information Technology.

DOCUMENTATION SHORTCUTS

Documentation shortcuts were created with the intent of allowing physicians to create a more complete record in less time. Ironically, it is often these shortcuts that pose the greatest risks to patient safety and physician liability.

Box Checking

A written record often contains seemingly extraneous information that can become extremely important to a physician's defense. For example, who was present when a patient was informed of the risks associated with a certain medication and what questions were asked and answered, or what comments the patient made regarding her adherence to treatment. Unfortunately, some EHR systems don't provide a mechanism for users to include this information and instead they are limited to checking boxes. The absence of the ability to write a complete narrative is a frustration many physicians report with EHR use.

Templates

As will be discussed more fully in a moment, template use is an area that is undergoing scrutiny by CMS and other payers. Templates are used to easily provide additional detail to a note but may not accurately reflect treatment – for example, they may misstate a patient's age or gender. The result is often a record filled with a large number of identical notes which call into question whether the physician truly did a thorough evaluation of the patient at each encounter. If a template is used for informed consent, it may not capture all of the information you need to establish that the informed consent discussion actually took place, e.g., who was present.

Autopopulation

Some systems will automatically populate entries with information from previous visits. On occasion the system will erroneously enter information from the previous *patient*. It is often impossible to determine whether data was entered by a clinician or by the system itself. Relying on default data can cause you to make false assumptions about a patient's condition and making inaccurate default data a part of your record will cause you to lose credibility in any subsequent litigation. Further, some state medical boards have written position statements cautioning licensees against relying upon software that pre-populates fields.

Copy and Paste Functionality or Note Cloning

As with template use, this function which allows a provider to copy and paste portions of previous entries into a new note is undergoing scrutiny by CMS. While intended to improve the thoroughness and ease of documentation, this function may be misused leading to problems both for the physician and the patient. Risks include:

- The possible perpetuation of erroneous information leading to incorrect diagnosis/treatment
- The potential for copying and pasting the note to the wrong treatment date or even the wrong patient's record
- The inability to identify the author of the original note and the date of that note
- Duplication of information not relevant to the current encounter

In its *Report of the Committee on Ethics and Professionalism in the Adoption and Use of Electronic Health Records*, Federation of State Medical Boards recommends:

> *"If a provider is satisfied that copying and pasting information into a new record entry is permissible in a given instance, he or she must include the appropriate citation in the record and verify that the copied information is current. Generally, it is inappropriate to copy and paste or otherwise document an entry that is not derived from a patient encounter at the time of the visit, unless the provider makes a clear notation that the information is copied and pasted from another record. Copy and paste is only appropriate when the content is verified."* [1]

THE FALSE CLAIMS ACT (FCA)

The Federal False Claims Act (FCA) protects the federal government from being overcharged or sold substandard goods or services and imposes civil liability on anyone who knowingly submits, or causes to be submitted, a false or fraudulent claim. "Knowingly submits" includes acting in deliberate ignorance or reckless disregard of the truth or falsity of the information related to the claim. Penalties for violation of the FCA include fines up to three times the amount of damages sustained by the government plus $11,000 per claim filed, or jail, or both.

One example of "knowingly submitting" a false claim might be a situation involving "upcoding" where a provider bills for a higher code than is appropriate for the service actually furnished which then results in a higher payment. The use of templates or note cloning in an electronic health record may lead to upcoding which puts the physician at risk – even if the upcoding was unintentional. In September of 2012, HHS and the Justice Department sent a letter to the American Hospital Association and others advising that the use of templates and note cloning would thereafter be under scrutiny.

If you choose to use documentation shortcuts such as templates and the copy/paste function you must remember that it is you who will be responsible for insuring that the encounter is billed using the appropriate code. Though the system may create documentation that meets the coding requirements for the highest code, it does not mean that you should bill at that code. Medical necessity is the key to accurate coding – even if a coding tool suggests a higher level of service.

TOO MUCH INFORMATION

Another issue to consider is whether so much information is being captured and stored that users cannot find relevant information. This can be problematic in emergency situations as well as routine treatment. One practical solution to this dilemma is to periodically print out a patient record and evaluate it for adequacy. A good medical record is one in which a subsequent provider or an expert witness would be able to understand what happened during the treatment relationship and why.

METADATA

Metadata is literally data about data and provides an audit trail of everything that occurs within the electronic record. What this means is that every time you sign onto an electronic health record system, you leave a trail of your activity including what patient records and what portions of those records were viewed, the actual time the record was viewed, how much time was spent looking at the record (including how long it took to view and override a safety alert or other clinical support tool), what entries were made, and any changes that were made to the record. And, as with all other parts of the medical record, metadata may be discoverable in a medical malpractice lawsuit.

"In addition to affecting the risk of a lawsuit, implementation of EHRs may affect the course of malpractice litigation by increasing the availability of documentation with which to defend or prove a malpractice claim."[2] No longer will juries have to rely upon a physician's recollection as to what occurred. There will be no question as to whether a physician reviewed a lab finding or whether he or she made a self-serving entry after an adverse outcome. Any dispute may now be resolved by simply examining the metadata.

In addition to its use in malpractice litigation, metadata may also be utilized to monitor access to patient records and to uncover HIPAA violations. Another potential use is by third-party payors who wish to analyze it to determine whether physicians have actually performed the services for which the payors are being billed.

CLINICAL DECISION SUPPORT SYSTEMS

Clinical decisions support systems are designed to assist physicians by making recommendations about possible diagnoses from a set of signs and symptoms, provide alerts on possible drug interactions or critical lab values, or to question a physician's medication dosage or other orders.[3] Unfortunately these systems tend to produce alerts that are not relevant and in such a large number that they've prompted at least one author to refer to them as the electronic version of the little boy who cried wolf. In other instances, the alerts may be based on out-of-date information. In fact, your EHR vendor likely will not even stand behind them as many include in the limitation of warranties section of their vendor agreements a statement that they are not responsible for the accuracy or completeness of the alert.

A 2009 study published in the Archives of Internal medicine found that of more than 200,000 alerts generated by an outpatient electronic prescription system, physicians accepted only 9.2% of drug interaction safety alerts and only 10.4% of "high severity interaction alerts."[4]

Further, a Department of Veteran's Affairs funded study published in the April 2012 Issue of the International Journal of Medical informatics found that often prescribers were unsure of why the alert was generated or that it pertained to a group of individuals , e.g., diabetics or pregnant women, as opposed to the specific patient in question.[5]

Alerts are often seen as such a waste of time that some practices have elected to have that feature turned off if possible while others have purchased software that allows them to screen alerts for relevance. While it is true that many alerts are not clinically relevant it is also true that there are some that are and therein lies the problem. Physicians can become so accustomed to seeing alerts that are not relevant that they tend to not notice when an alert is relevant which is known as alert fatigue.

Unfortunately, a jury will not be sympathetic should you miss an alert that might have prevented patient harm. As presented by a plaintiff attorney, they will only see that you were told of potential patient harm and ignored the warning. Because the plaintiff attorney will also have access to metadata, he will be able to show how rapidly you clicked past the warning seemingly without consideration.

RISK MANAGEMENT REMINDERS

- Ensure templates used are appropriate for the specific patient
- Consider disabling the cut and paste function or use with extreme discretion and require author identification for each entry
- Do not allow autopopulation
- Periodically print out a copy of your record to look for
  - » Technical glitches
  - » Ability to pass a billing audit
  - » Ability of a subsequent treater (or an expert witness) to understand what you did and why
- Understand metadata
- Ensure appropriate security protections on hardware and software
- Ensure compliance with federal and state confidentiality law
- Prevent inappropriate access by employees – training is key

1 Federation of State Medical Boards. Report of the Committee on Ethics and Professionalism In the Adoption and Use of Electronic Health Records, April 2014.

2 Mangalmurti SS, Murtagh L, Mello MM. Medical malpractice liability in the age of electronic health records. N Engl J Med 2010 Nov 18; 363(21): 2060-7.

3 Berner, ES. Ethical and Legal Issues in the Use of Clinical Decision Support Systems, J.Healthc Inf Manag. 2002 Fall; 16(4):34-7

4. Arch Intern Med. 2009; 169(3): 305-311

5. Russ, AL, et al. Prescribers' interactions with medication alerts at the point of prescribing: A multi-method in situ investigation of the human-computer interaction. International Journal of Medical Informatics, Volume 81, Issue 4. 232-243.

MYTHS & MISCONCEPTIONS: PSYCHIATRIST'S SIGNATURES

Q: In my place of work I work with a team of healthcare professionals that provide mental health services. I am often asked to sign various forms related to patients that I have not seen. Are there any guidelines that govern the signatures on forms by psychiatrists?

A: Yes. The American Psychiatric Association has issued a resource document titled *Guidelines Regarding Psychiatrists' Signatures*. (APA Resource Document 890002, June 23, 1989.) These guidelines govern the circumstances under which a psychiatrist may sign medical records and insurance forms and provide guidance as to what the psychiatrist's signature signifies.

The signature on a diagnostic or treatment plan signifies that the psychiatrist has reviewed it, agreed with the diagnosis and approved of the plan. It does not necessarily mean that the psychiatrist has seen the patient or performed an evaluation. The psychiatrist should clarify their role by writing an annotation immediately before their signature that includes information about the role they served. Examples include: "Reviewed by (name)" or "Under the supervision of (name)" or "Team Leader Approval."

The signature on insurance forms for billing purposes signifies that the patient received the billed-for treatment. The psychiatrist must carefully check the wording of the form and make clear with an annotation the services rendered by him or her. This can be accomplished by writing in before the signature a phrase such as: "Under the supervision of (name)" or "Reviewed by (name)" or other such clarifying annotation. A psychiatrist's signature for quality assurance, peer review or other administrative review should include what was reviewed during the evaluation and approximately how long the review took.

Have any comments or questions about an article?

We would love to hear from you!

Editor@prms.com

(800) 245-3333

PsychProgram.com