Practice Innovations

ISSN: 2377-889X
https://doi.org/10.1037/pri0000270

The Wild and Wooly World of Electronic Health Records (*Who Would Have Thought?*)

Susan C. Litton
Decatur, Georgia, United States

Every health care professional must keep records. For those of us in private practice, the responsibility falls on us to make wise decisions about the optimal ways to do this. With the widespread integration of telehealth, not only must we choose our bookkeeping methods, but most of us currently use at least one—if not several—digital tools in our clinical work. This article examines the electronic health record (EHR) as a holistic solution for addressing various digital tasks clinicians encounter, including clinical needs, plus the management of medical records and associated bookkeeping responsibilities. Attention is devoted to convenience factors as well as legal and ethical considerations. Finally, readers will learn concepts to help them evaluate health care software, enabling them to make the wisest choices among products.

Clinical Impact Statement
The electronic health record (EHR) a mental health practitioner chooses can significantly impact clinical and nonclinical aspects of their work. A well-chosen EHR can improve access to records and provide secure communication, while a poor product can lead to data privacy issues which may not have been adequately explained nor agreed to by the client. This article explores positive and negative implications of behavioral health EHRs and offers suggestions to clinicians for how to make wise choices among products.

Keywords: electronic health records, mental health, patient privacy, practice management

Wild and Wooly? Come On!

I do not know about you, but if I saw an article on electronic health records (EHRs), I would expect boring. Maybe even exceedingly boring. However, historical and ongoing events in the field of EHRs have taken unexpected twists and turns, creating an atmosphere that does in fact feel a bit tumultuous. For this article to be thorough, we must first cover some basics. But trust me. We will get to the wild and wooly.

Evaluating Medical Software

Many papers of this type choose a handful of products and review them. While that approach is certainly appealing to most readers, it poses several challenges. First, software can be rated on many different dimensions, such as number and type of features, usability (how easy it is to learn and use), and look and feel. Although those things are relatively easy to rate, they are not always the most important. It is also crucial to determine whether the software allows you to practice legally and ethically. Not all health care software meets these standards, and many things that might seem reassuring are merely marketing ploys.

Additionally, software can have problematic technical issues in the code itself that a nontechnical reviewer may not realize are present so would not know to mention. Historical events related to

Jeffrey Zimmerman served as action editor.
Susan C. Litton https://orcid.org/0000-0002-7928-6413
Correspondence concerning this article should be addressed to Susan C. Litton, Decatur, GA 30033, United States. Email: susan@susanlitton.com

the software's development can also have an impact on its performance. Finally, a product can change radically and unexpectedly. Earlier this year, I observed two health care software products, which I would have previously rated as 5-star, undergo changes that were so severe that I felt I could no longer endorse them at all.

For these kinds of reasons, this article will take a different approach. Instead of reviewing a handful of EHRs, we will explore concepts and even a bit of EHR history, all aimed at teaching you how to evaluate your own medical software. Let us get started!

What Is an EHR and Why Would I Want One?

EHR stands for electronic health record, sometimes referred to as an electronic medical record (EMR) or a practice management system. Although these three terms were originally intended to mean different things, their distinctions have blurred over time, leading to more or less interchangeable use today. The most used term is EHR, and that is the term that will be used throughout this article. However, the discussions will generally apply to all similar systems.

For our purposes, EHRs can be broadly defined as a set of integrated tools aimed at digitizing some or all of a patient's medical record. A crucial component of this definition is the term "integrated." You do not just want a collection of tools. You want a collection of tools that integrate with one another in such a fashion as to make your life as a clinician easier, not harder.

What Tasks Do EHRs Do?

Personally, I want an EHR that does pretty much every task I need to do as a clinician or, at least, as many of them as possible. To give us a list to work with, I came up with the following set of 15 tasks for which I use my EHR in my own private practice:

1. A calendar with appointment reminders that includes repeating appointments for office, video, and phone sessions
2. A tool for creating custom forms for informed consents, Health Insurance Portability and Accountability Act (HIPAA) notices, and other digital intake items
3. A feature that allows clients to e-sign documents
4. A video program for telehealth appointments
5. A way to e-file insurance claims, retrieve ERAs (electronic remittance advice), and check claim status
6. A method to send or print digital statements and receipts for clients
7. An online payment system that updates client balances accordingly
8. A comprehensive notes system, including intake forms, treatment plans, process notes, and psychotherapy notes
9. A 100% end-to-end encrypted email tool (100% end-to-end encryption means it is virtually unhackable, even when files are at rest.)
10. A 100% end-to-end encrypted text messaging tool
11. A 100% end-to-end encrypted file storage area
12. A way to generate various reports, including medical records and financial reports
13. A secure, companion mobile app for use on the go
14. A client portal with tools for email, texting, file sharing, and appointments
15. Easy onboarding of new clients, including the ability for them to fill out and update their own demographics forms

This is just a basic list—nothing fancy. Your list might only have eight tasks—or it might have 30. But we all have routine tasks we do with our clients. In an ideal world, I want my EHR to do all of them.

There are many reasons why having these tools in a single EHR is a better solution than if I had 15 standalone tools that did the same tasks. Some of the reasons are convenience, but others have legal and data security implications. Before we go farther, we need to add a brief sidebar for those of you who prefer paper records—or at least paper notes.

A Sidenote on Notes

Many therapists prefer to maintain paper notes, even if they use EHRs for everything else. This is totally legal, and in fact, when we get to some of the "wooly" aspects of EHRs, some of you

who have switched to digital notes may begin wondering if you should rethink that. However, before we all start cutting down more trees, let us look at some of the issues with paper notes:

- The biggest concerns with paper records are natural or man-made disasters. Fires, floods, theft, and other unexpected catastrophic events can totally destroy and/or expose paper records. In extreme weather events such as tornados, floods, or hurricanes, paper records could end up scattered around the affected area. During Hurricane Katrina, many medical professionals lost all records they had been maintaining on their patients.
- Paper notes are not searchable. If you forget the name of your client's grandfather—which they may have mentioned in the very beginning of their therapy but not since, you can likely discover it fairly easily with digital notes. Not so with paper.
- If you see long-term clients—or if clients from the past want to resume therapy—archived paper records can be difficult to access. While I always kept current paper records in locked file cabinets behind two locked doors, risk assessments performed at various points in my career determined that storing older records in archive boxes in an attic space (off my attic office) and later a crawl space (off my new basement office) met HIPAA security requirements for long-term storage. However, despite being secure, both locations required a flashlight and involved me bending into unnatural positions and/or crawling on hands and knees to dig through boxes to find what I needed. I have known other therapists who rent long-term storage units for this purpose. While this is also a secure solution, it is equally inconvenient and adds a monthly expense. With EHRs, reactivating older records is usually as easy as clicking a button to move the client from inactive status to active, with all previous records still readily available.
- Paper records can create storage issues as illustrated by the above examples. In my own practice, I am now completely paperless. I shredded all older records as they have exceeded the required retention period. Since around 2010, I have been managing my practice entirely online, eliminating the creation of new paper records. This ensures that I no longer need to worry about paper patient records potentially falling into the wrong hands if I were to die or become disabled.

How EHRs Make Our Lives Easier

Here is a partial list of the convenience factors EHRs can provide:

- Getting bundled tools in an EHR is typically less expensive than procuring each tool separately. This one often surprises people. It is easy to see the fees to an EHR company as being high, but if you add up the costs you are paying for each of your standalone apps, you may be shocked.
- EHRs generally save time by reducing data entry through structured interfaces. They also remember and auto-suggest your previous entries, making repetitive tasks more efficient.
- Tools are synchronized, meaning if your patient moves or gets a new email address, you only need to enter it once and all tools update automatically. With standalone apps, you would have to manually check and update each one.
- Synchronized tools help reduce errors by eliminating the need for multiple manual updates required when using standalone apps, ensuring consistent and accurate information across all platforms.
- With an EHR, you only have one program to learn and one password to remember.
- Planning for your unexpected death or disability is greatly simplified. I have asked one person to oversee my practice should something happen to me. She has her own login information. If it becomes necessary for her to take over, all she has to do is sign in to my EHR—from anywhere—and she will be able to see my entire schedule along with contact information on each client so she can notify them. She can also create medical records for any clients who want them and/or send their records securely to their new therapists. She will be able to do all of this from her own home. No need to come to my office.
- Medical records are easy and fast to produce.

This one is worth elaborating. If you are a psychologist or other type of mental health professional and you have seen at least one client and recorded at least one piece of information about them, you have produced a medical record for that client. Those of us in the mental health fields are not always trained to know this. However, whether you prefer to call the individuals you see patients, clients, or some other term, everything pertaining to them is considered part of their medical record. This includes obvious things like treatment plans, progress notes, and assessments, but it also includes all correspondence with or about the client, which, in the current environment, is often done via email or texting. Some therapists prefer to keep original texts and emails as part of the medical record. However, others prefer to just document each text or email sent or received and keep the documentation in their chart. Whichever you decide, it is essential to document all communication, and it is also important to treat all patients the same. It may be tempting to keep more complete records on high-risk patients. However, this is legally unwise, as it could lead attorneys to allege favoritism or bias, potentially undermining any testimony you might need to provide for any future legal proceedings. Medical records also include an itemization of all encounters, whether by telehealth, phone, or in-person. They include insurance claims and any statements and/or receipts you have generated plus all payment records. And, of course, they also include all forms you have your clients fill out, such as intake forms and informed consents plus legal documents, such as your HIPAA Privacy Policy or documents you use for the Cures Act (i.e., OpenNotes).

With EHRs, it is often possible to store a client's entire medical record within a single app. Before I started using EHRs, I used to panic when I was required to produce a medical record. The task involved collecting documents from a variety of places, sorting and scanning it all to produce a single file or set of files that was logical and easy to follow, then figuring out the best way to safely deliver it to the person or agency requesting it. It was usually at least a 3- to 4-hr project, and that was if I did not have to rummage through the older, archived records stored in my aforementioned attic or basement storage spaces. Now that I use an EHR, completing this task takes 5 min or less. I enter the dates I want, check boxes to indicate the items I want to include, click Submit, and I have my document.

There is nothing that says a medical record has to be maintained in a single app—or kept in a single filing cabinet if you prefer paper records. However, when requested, we do have to be able to produce a complete medical record within a reasonable amount of time. When the entire medical record is maintained in a single app, it will make your life a lot easier.

- The final EHR convenience factor we will mention is that with an EHR, all tools are encrypted and HIPAA compliant, plus you have a single business associate agreement (BAA) for the whole thing. (BAAs are contracts between you, as a health care provider, and the business associate, i.e., the company providing the tool or service.)

You likely just skimmed that last bullet point, mentally marking it as "Of course." However, this is actually where the wild and wooly begins.

In the past, we could pretty much just sign BAAs. However, software companies now exhibit significant variability in how they are crafting their BAAs. Some companies continue to align with the original purpose of a BAA, which is to provide certain protections and transparency for both providers and clients. However, other health care software companies have begun diverging from this original intent rather severely (S. C. Litton, 2024) and have written BAAs that are specifically designed to benefit the company as opposed to its users. We have reached the end of an era where hastily approving BAAs without actually reading them, though never encouraged, likely would not have caused any disastrous or unexpected consequences. However, because of this new twist, finding one BAA you feel good about for a single product is a lot easier than having to carefully read all the fine print for each standalone product you are using.

How EHRs Help With Legal Essentials and Time-Savers

The list above comprises some of the "niceties" of having an EHR. Ways they make your life easier. However, complying with some parts of HIPAA becomes nearly impossible without an EHR. And by the way, if you have signed even one BAA, that action almost certainly pushed you

into the "must comply with HIPAA" category, even if you had been avoiding triggering HIPAA for years (S. C. Litton, 2024). There are some specific HIPAA standards that may be impossible to meet without an EHR. We will discuss two of the biggest ones.

HIPAA Security Rule: Audit Controls 45 CFR § 164.312

The Audit Controls Standard is required, not just addressable. That means we must implement it as specified. Failure to comply with required standards is considered nonnegotiable and may result in penalties or other consequences. The Audit Controls Standard specifies that you must have a way to monitor the system activity and usage with each of your software programs that interacts with protected health information (PHI). If you are using standalone tools, this could apply to accounting software as well as programs like Word or Excel, if any of them contain PHI. Most EHRs automatically log this information for you behind the scenes. You do not need to set it up; good EHRs are just programmed to do it. A few entries from an audit log in an EHR might look something like this (see Figure 1).

If you have standalone tools in addition to or instead of an EHR, you would need to make sure that each of them has the ability to produce logs similar to the one shown in Figure 1. The likelihood of many, if any, standalone tools offering this feature is remote at best. If you are a single practitioner with no office staff, you might be able to make a case for keeping manual logs for each of your software products if you are the only one who ever accesses them. However, trying to produce a log similar to the one above by hand would be tedious. Also, a manual log does not have the advantage of having digitized time/date stamps so it could be viewed as less reliable in legal contexts.

Another HIPAA standard to consider is the following.

HIPAA Security Rule: Integrity Controls 45 CFR § 164.312(c)

The objective of the Integrity Controls standard is to protect PHI from unauthorized modification or corruption. A medical record is to be complete, unaltered, and accurate throughout its life cycle. It is permissible to delete data from a medical record, but only if those data are retrievable. For example, if you make an error, you may want to remove it to keep the chart neater and easier to follow. However, there must be a way to retrieve it, that is, to see what was deleted, when the deletion occurred, who deleted it, and the reason for the deletion. (Providing reasons for deletions in medical records is an essential risk management strategy that all health professionals should follow.)

The last row in the EHR audit log we saw above is for a note that was deleted. However, the user can click the orange link (circled in Figure 2), and it will display the entire contents of the portion that was removed and the reason for deletion (assuming the person deleting it provided the reason; see Figure 2).

Most EHRs provide a way to do this but again, few, if any, standalone tools do. Without it, I am not sure there is a way to prove that nothing in the chart has been altered or deleted, should you need to. If you have kept your notes in Word, or a paper notebook, how can you convince a court that none of your notes have been deleted? Same question for any other standalone tool you might be using. As with the Audit Controls standard, it may not be

Figure 1
Sample Entries From an EHR Audit Log

Date/Time	Action	Action Taken By	Acted On	Description
07/23/2023 12:02 am EDT	Added note	Jane Therapist, Ph.D.	Manuel Client	Medical Record > Progress Notes 07/23/2023 (Signed)
07/23/2023 12:02 am EDT	Added session	Jane Therapist, Ph.D.	Manuel Client	07/22/2023 90791
07/23/2023 12:02 am EDT	Viewed notes	Jane Therapist, Ph.D.	Manuel Client	
07/23/2023 12:03 am EDT	Signed note	Jane Therapist, Ph.D.	Manuel Client Medical Record > Progress Notes 07/23/2023 (Unsigned)	Medical Record > Progress Notes 07/23/2023 (Signed)
07/23/2023 12:03 am EDT	Deleted note	Jane Therapist, Ph.D.	Manuel Client Medical Record: 07/23/2023	Deleted note: Medical Record: 07/23/2023

Note. EHR = electronic health record. See the online article for the color version of this figure.

Figure 2
Accessing Deleted Notes in an EHR Audit Log

Date/Time	Action	Action Taken By	Acted On	Description
07/23/2023 12:02 am EDT	Added note	Jane Therapist, Ph.D.	Manuel Client	Medical Record > Progress Notes 07/23/2023 (Signed)
07/23/2023 12:02 am EDT	Added session	Jane Therapist, Ph.D.	Manuel Client	07/22/2023 90791
07/23/2023 12:02 am EDT	Viewed notes	Jane Therapist, Ph.D.	Manuel Client	
07/23/2023 12:03 am EDT	Signed note	Jane Therapist, Ph.D.	Manuel Client Medical Record > Progress Notes 07/23/2023 (Unsigned)	Medical Record > Progress Notes 07/23/2023 (Signed)
07/23/2023 12:03 am EDT	Deleted note	Jane Therapist, Ph.D.	Manuel Client Medical Record: 07/23/2023	Deleted note: Medical Record: 07/23/2023

Note. EHR = electronic health record. See the online article for the color version of this figure.

possible to meet the Integrity Controls requirement when using those kinds of commercial products for your medical records.

Security Policies: Required for all Health Care Providers

We have looked at two examples of legal essentials but there are others. However, rather than trying to list them all (which *could* get boring), we will move on to discuss a legal time-saver: preparing and updating your HIPAA Security Policy. Most therapists—even new ones—are aware that HIPAA specifies that they need to have a privacy policy. However, many therapists—even ones who have been in practice for a long time—are unaware that they also need to have a security policy (Office for Civil Rights, 2013). Security policies are unique to each individual's practice. Before writing them, you must conduct a risk assessment. Risk assessments require that we catalogue every piece of equipment, hardware, and software utilized in our practice to pinpoint potential risks to the confidentiality, integrity, and availability of PHI. Returning to my hypothetical example, if I use 15 standalone tools in my practice, I would need to draft a separate policy and procedure for each tool as part of my security policy. Conversely, if I am using an EHR that incorporates those same 15 tools in a single app, I only have to write one software policy and procedure—for the EHR.

De-Identification and EHRs

HIPAA specifies two methods for de-identifying PHI (Office for Civil Rights, 2022). Assuming the de-identification is done correctly, the likelihood of an individual being recognized, though possible, is considered remote. For this reason, de-identified data are no longer considered PHI.

De-identification by itself is neither good nor bad. It is likely that the original authors of HIPAA assumed that companies might encounter situations—possibly for research and/or internal business operations—where they felt they should de-identify PHI as an additional security measure. For this reason, the drafters of HIPAA wrote specifications for how it should be done. The safe harbor method of de-identification is the most used and also generally the more secure of the two methods. Safe Harbor lists 18 identifiers, all of which must be removed from the PHI. These 18 identifiers apply not just to the client but to relatives, employers, or other household members living with the client.

It is relatively easy for de-identification software to remove a patient's identifiers from structured data (name, birth date, address, etc.) because such data are almost always labeled. However, the same type of data on client relatives, employers, and household members is not always clearly labeled and might be easy to miss. A bigger problem is that EHRs also have large areas of unstructured data, called "free text" where identifiers are not specifically labeled. Free text areas might be your clients' intake forms, treatment plans, or progress notes. It could also include results from any assessments, plus any other files or forms you (or they) may have uploaded into their chart. De-identification software could easily miss identifiers in free text areas, which, over time, would likely be the largest part of the medical record.

Even when done correctly, de-identification programs are not foolproof because of the issues

mentioned above (Office for Civil Rights, 2022). When de-identification is paired with artificial intelligence, the possibility of ensuring confidentiality deteriorates rapidly. Unfortunately, as discussed above, some popular EHRs have recently started crafting their BAAs in ways that may pose significant threats to de-identification.

When De-Identification Is Used Against Us and Our Clients

Recently, some health care software products, including a popular EHR, published new Terms of Service and Business Associate Agreements. In these updates, they state that by de-identifying all PHI entered into their applications, the data cease to be classified as PHI, which is true. Moreover, they assert that all such data belong to them and that they are free to do whatever they want with it. This means that, should these companies decide to feed these de-identified data into an AI engine, their new terms have staked out their legal right to do so. To make matters worse, they also state that they are not obligated to tell you they are doing it. If you sign something like this, you are legally endorsing and accepting the product and its business practices.

At first glance, this may look like a decent way for an EHR to legally generate more income. However, software companies engaging in these questionable de-identification practices are behaving legally only if they are correctly applying the rules for de-identification. There is some indication that that may not always be the case. Dalton (2023) pointed out that one such EHR mentioned using initials in their de-identified data. According to HIPAA, initials are considered PHI when they are maintained in a designated record set, as would be true with EHRs (U.S. Department of Health & Human Services, n.d.). This means software companies would be expected to remove initials during de-identification. It is unclear whether EHRs using initials are unaware of correct de-identification procedures or whether they are choosing to ignore them. Either way, if any one of these identifiers remains in the data after the de-identification process, it would not be considered fully de-identified under the safe harbor method, and therefore, companies doing this may not be behaving legally.

However, even when de-identification is done correctly, there are still very real concerns, as suggested just from the title of an article by Miller: "De-Identifying Medical Patient Data Doesn't Protect Our Privacy." Miller explains how easy it is to reidentify data which have been de-identified. Miller further notes that the primary (if not only) safeguard against reidentification depends on the company's commitment to their customers that they would not reidentify the data (Miller, 2021). However, in companies using the de-identification practices described above, this basic protection is absent. Worse, some EHR companies explicitly assert their right to withhold disclosure about their intentions regarding data input into their systems. This lack of disclosure creates potential opportunities for reidentification by entities to which they sell information—the exact situation Miller is cautioning against. There is nothing to prevent this. This could provide devastating consequences to both patients and therapists, even though, if the PHI is being correctly de-identified, the company is operating legally.

There is a historical example of a situation not unlike what we are seeing today (Federal Trade Commission, 2016). That case involved an EHR named Practice Fusion, a free EHR that launched in 2005. Because it was free, providers flocked to sign up. Like the current business practices described above, Practice Fusion also retained the right to sell/reuse de-identified data that had been entered into their system. Most subscribers accepted that business model and signed up. The product was free, and at that point in time, we had no reason to question a company's right to sell de-identified data. Practice Fusion sold its data to a subsidiary they established specifically for reviewing health care providers. In other words, they sold the data to themselves. In this case, the only information the subsidiary company needed to accomplish its goal of posting online reviews of providers was a list of the patients' names and phone numbers, along with the name of the provider and when they last saw them. This was very easy to extract from the original data. Employees of the subsidiary company then called the patients, claiming that their doctors had requested a postvisit satisfaction survey. The unsuspecting patients thought they were being contacted by the doctor's office as a routine follow-up. Because they trusted their health care providers, patients began telling the interviewer how they were doing, providing much more personal health information than they normally would because

they thought they were talking to their doctor's office. They did not know they were providing a review. Verbatim transcripts of what patients told interviewers began showing up online, revealing very personal individual health care information. Neither the providers nor their patients realized what was happening until people began recognizing friends and neighbors from the reviews. Understandably, patients were horrified and blamed their doctors for posting their personal information online. This set off a flurry of activity as everyone began probing for more information about how this possibly could have happened.

The case was egregious enough to eventually reach the U.S. Department of Justice. Further investigation revealed that Practice Fusion had also been embedding prompts within the EHR system that encouraged doctors to prescribe opioids in situations where it might not have been clinically appropriate, aligning themselves with the interests of pharmaceutical companies. In 2020, Practice Fusion agreed to pay a settlement of over $145 million to resolve criminal and civil investigations into these practices. The case raised concerns about patient privacy, the ethical use of health care data, and the potential influence of EHR systems on medical decision making (U.S. Department of Justice, 2020).

It is easy for us to say, "Oh well … even though my EHR is doing the same kind of thing with de-identified data, they would not do anything THAT bad. All my colleagues are using this EHR so it must be fine." I suspect the subscribers to Practice Fusion would have said similar things before the true intent of that company became apparent.

Dr. Keely Kolmes has written a blog post titled "It had to be you: When your favorite EHR makes you break up with them" (Kolmes, 2023). Dr. Kolmes highlights the real struggle that occurs when you learn that an EHR you love and have been using for years no longer allows you to practice ethically. To back up their points, they reference some of the general principles in the APA Ethics Code.

In addition to the concerns highlighted by Dr. Kolmes, ethics issues around confidentiality are also pertinent here. All health care professionals have ethics codes regarding confidentiality. For example, Section 4 of The American Psychological Association's Code of Ethics, Privacy and Confidentiality, includes two standards that are pertinent: 4.01 Maintaining Confidentiality and 4.02 Discussing the Limits of Confidentiality. These standards specify that psychologists "have a primary obligation and take reasonable precautions to protect confidential information obtained through or stored in any medium." Furthermore, psychologists are to discuss with their patients "(1) the relevant limits of confidentiality and (2) the foreseeable uses of the information generated through their psychological activities (American Psychological Association, 2017)." Other behavioral health professional groups have similar standards. All health care professionals also have requirements around Telehealth Informed Consents. Those documents would most certainly need to cover and explain the kinds of issues present with the sale of de-identified data to undisclosed recipients.

Hopefully it is becoming clear that, at least in the health care software domain, behaving "legally" does not always equate to behaving "ethically." Worse, using those products may not allow us to follow our profession's ethics codes. For example, how can we discuss with our clients "foreseeable uses of [their] information" if our EHR refuses to give us that information?

In such situations, it is up to each of us to determine our own comfort level with the degree of risk. One of the unfortunate things is that, unlike the enforceable ethics codes that health care professionals have, it is harder to find a centralized authority or agency specifically focused on the ethical oversight of health care software companies. There are companies who, at first glance, look like they may be fulfilling this role by providing certificates of HIPAA compliance. However, those are simply commercial companies hoping to sell their seal-of-approval badges to health care software companies to help boost public confidence in their products. They do not provide oversight. The Federal Trade Commission (FTC) plays a role in overseeing privacy and security aspects under HIPAA but is less likely to regulate overall ethical conduct in business practices unless they specifically relate to consumer protection or antitrust concerns such as happened in the Practice Fusion case. However, those kinds of wheels move slowly. The Practice Fusion situation took close to 15 years to resolve. A tremendous amount of damage to both clients and health care providers can happen in that amount of time.

The History of EHRs (Psst: Even the History of EHRs Is Wooly)

There were pioneering experiments as early as the 1960s and 1970s aimed at computerizing medical records (Atherton, 2011). President George W. Bush, in his State of the Union Address on January 20, 2004, proposed a "Health Information Technology Plan" setting the stage for computerized health care records and a national database. This was followed by his 2005 budget, which included $50 million to be put toward local and regional grants toward this goal. By April 2004, more than 600 applications had been filed (George W. Bush White House Archives, n.d.).

The next significant milestone in EHR history was the "Meaningful Use" program, part of the Health Information Technology for Economic and Clinical Health (HITECH) Act enacted in 2009 during the Obama administration. A primary goal of both initiatives was to achieve "interoperability," allowing for a national health care database where data could be easily exchanged and accessed to improve the quality of care, increase efficiency, and reduce errors. It is noteworthy that this original goal of interoperability has never been achieved. However, over the years, a variety of bills toward this end have been proposed, modified, nullified, and/or partially accepted, resulting in major changes to the EHR landscape.

Despite advocacy efforts by the American Psychological Association Practice Organization (APAPO), psychologists and most other nonphysician providers were not included as eligible providers (EPs) in the Meaningful Use program (American Psychological Association, 2010). This disappointed some but pleased others, who were concerned about increased privacy risks to mental health patients. It is interesting to speculate that mental health professionals may have stronger feelings about privacy than other types of health care professionals, possibly since we tend to get to know our patients more intimately. Around 2006, I interviewed several therapists to determine their feelings toward using online products for patient records. I remember the reaction of one woman who looked at me with alarm when I mentioned the concept. "You mean store all my client information on the Internet? Up in the CLOUD?" she said, gesturing upward, as if, "the cloud" was somewhere up in the sky with other types of clouds. "Yes," I replied. "Oh no!" she responded. "I always want to have my records right here with me!" Her gesture changed to one of hugging herself, reminiscent of how a mother might fiercely protect her child by hugging the child tightly to her breast. Other participants in the study were not as expressive as this particular woman, but I always felt her response represented the concerns of many.

However, the fact that behavioral health was not included in Meaningful Use has had some interesting consequences. One of the main features of Meaningful Use was that health care providers were incentivized for using the type of EHR Meaningful Use required, called an "ONC-Certified" EHR. In 2021, Litton concluded that this type of EHR was:

> Only slightly short of disastrous. Many of the EHRs that came out during this period were just plain bad. Healthcare professionals—who wanted to focus on treating their patients—resented all the busywork they were now required to do and the maddening computer interfaces with which they had to do it. (p.45)

Bresnick (2015) spoke for many when she said:

> EHR usability has been a hot-button topic since the very start of meaningful use. Cumbersome interfaces, time-sucking point-and-click features, confusing documentation fields, convoluted methods to access historical data, and a "walled garden" approach to health information exchange have put providers in the pressure cooker for more than half a decade.

I have personally witnessed the so-called "walled garden" issue during an in-office appointment with one of my own physicians. He wanted to see me for a brief, 5-min follow-up later that week. He looked at his schedule, found the time he wanted to squeeze me into, and asked me if it worked for me. It did. Then, expressing his frustration that his EHR did not allow him, as a physician, to schedule appointments, he got up out of his chair and walked down the hall to tell the scheduler what to do. A few moments after he got back, his phone rang. It was the scheduler. They did not know how to create an appointment like that since it was not one of the normal point-and-click ones suggested by the EHR. My doctor knew a way to do it and told them how. They were able to follow his instructions and I got the appointment. However, one could hardly call this a "superior" user experience, and the EHR he was using is probably the biggest name in the field of Certified EHRs.

Meanwhile, other software developers—many of whom were behavioral health professionals—listened to the complaints about the ONC products and set out to build EHRs that were tailored specifically for mental health. These products did not hold ONC certification. Instead, they prioritized usability and simplified their offerings by excluding sections relevant only to physicians. Additionally, these products integrated a wider range of practice management and bookkeeping tools, making them more versatile. They used a subscription-based software delivery model called Software as a Service (SaaS).

Over time, more and more developers jumped on this bandwagon, with the end result being a large—and overwhelming—array of similar products from which to choose. It is not surprising that many new therapists just decide to just use the EHR their colleagues are using without investigating further. It would be helpful to have reviews of EHRs. However, that is hard to find. Most companies that claim to do this are actually commercial sites where EHR companies pay for favorable reviews. On those types of sites, top ratings are based on which company pays the most, not on the quality of the product. Similarly, some national and state professional organizations provide paid sponsorship endorsements or even offer special deals for products that have paid for this privilege. This can be equally misleading, especially since we look to these same agencies for ethical guidance.

An exception to these advertisements-posing-as-reviews is "Tame Your Practice"—a site developed and maintained by Rob Reinhardt, LPC (Reinhardt, n.d.). Rob, an IT professional as well as a practicing LPC, schedules online meetings with EHR developers to personally review their products. Maintaining "Tame Your Practice" is quite a significant undertaking because many of the products Rob reviews are consistently adding new features. Also, new products are continually being developed. It is an impossible task to keep up with all products equally well, so some of the reviews you read may be outdated and/or incomplete. Also, although Rob is an IT professional, his reviews tend to primarily focus on available features, which, as was discussed above, limits their effectiveness. However, it may be useful to at least browse Rob's site to get ideas. Despite its drawbacks, Tame Your Practice nevertheless provides an overview of many EHRs available today. You could possibly use it as a starting point and then do your own research on the products that interest you to gather a deeper level of information and correct any inaccuracies Rob's site may have. Rob is also available for consultation for those who would like his take on some of the more involved issues we have discussed. Again, though, it is unlikely that Rob will have 100% up-to-date information on any one product. Your best source for that is the product itself.

The other new development in the EHR landscape is that there are now several open-source models that can be used to build EHRs. "Open source" refers to a type of software for which the original source code is made freely available and can be redistributed and modified by anyone. This greatly speeds up the process of building new EHRs and has encouraged the emergence of several new products, some of which may endure but others seem to already be fading away.

A potential pitfall of using open-source EHRs is that developers who can piece together open-source components may not have the skill set needed to modify the code when requirements change and/or users find things they do not like. As a software developer, it is much easier to work on a code you have written yourself. You do not have that advantage when you have built the product by piecing together various modules of code created by others.

Practical Considerations

The following things fall in the "last but definitely not least" category:

- *Customer Service:* Although it is hard to evaluate customer service ahead of time, pay attention to the types of customer service offered by a product you are considering. Do you prefer to contact a company via email? Phone? Chat? Video appointment? Look for a company that offers your preferred communication style(s), and that seems to have good customer service ratings. Pay attention to the representative's responses when you reach out to them with questions. Are responses timely? Courteous? If the person you talk to does not know an answer, do they offer to escalate your question?
- *Abandoned Products:* You want an EHR that is continually improving. Some developers launch a product, promote it for a

while, and then partially or completely abandon it. They ignore feedback from users, do not add new features or improvements, and may not even make necessary updates when things like new diagnoses come out. Avoid these products.

- *Conglomerate Products:* Some companies buy smaller EHRs and rebrand them under their own umbrella. A big name in the EHR conglomerate sector is Therapy Brands, which now owns several of the EHRs listed on the "Tame Your Practice" website. There are many such companies; Therapy Brands is just a big one. There are several potential concerns with the conglomerate business model, including lack of integration and standardization, sometimes having to log in to more than one product and enter duplicate client data to accomplish your tasks. Sometimes a product you have loved for years will be changed into something totally different which you do not love after it is bought and changed by a conglomerate. Although you have no way of knowing what might happen to any product in the future, it is probably best to not sign up for an EHR that is already owned by a conglomerate company. It is not always easy to tell, but you can ask their customer service representatives about the ownership history of their product. Phrases like "powered by" or "affiliate of" are clues.
- *Client Portals and Perceived Professionalism:* I live in a large city. All of my health care providers email me through their EHRs. I never actually see their email address. I am notified that they have written me through the EHR's portal and I sign in to read their email. It would seem unprofessional—and possibly even a bit creepy—if they used a commercial email account for our exchanges, even if it was something like Proton Mail or Hushmail that I know to be secure.

There is an anecdotal story worth sharing here: A few years back, I had a potential new client contact me for an appointment. She told me she was interviewing three therapists. I was the middle one. She explained that she intended to see all of us and then would make her selection. I sent her my intake documents through my EHR's portal. She filled them out and returned them before we met. Toward the end of our appointment, she said, "I think I'd like to work with you. I do have another appointment, but I can cancel it." I told her it also felt like a good fit to me and that I would be happy to work with her. As I began looking for times I could see her, she asked, "Do you want to know why I chose you?" I did and was a bit shocked by her answer, which was:

> It's because you have a portal. Neither of the other two therapists I scheduled appointments with do, and I feel like if they're not up to date with business practices, they may also not be up to date with the latest treatment options.

Of course, we all know that correlation does not imply causation, but the important point here is that in a consumer's mind, it did. For some, using an EHR with a portal will make you seem more professional.

- *Encrypted Email and Texting:* Previous research on reported breaches in health care suggests that health care providers are worse at protecting client emails than any other type of covered entity. (Covered entities, as defined by HIPAA, include health care providers, insurance companies, and clearinghouses.) More specifically, health care providers account for 90.7% of all email breaches (S. Litton, 2021). Details of the breach data show that in many cases, providers were sanctioned for using regular, nonencrypted or partially encrypted commercial email products such as Gmail, Google Workspace, Outlook, Yahoo, and AOL. Some of these commercial products offer no encryption. Even those that do, including some offering HIPAA Compliance and BAAs, only offer partial encryption. Many behavioral health providers, even those using EHRs that have encrypted email and texting, continue to use regular unsecured email or texting for contacting clients. This is something we, as providers, have control over. We can prevent these types of breaches. We are required to communicate securely with our patients. If a client asks us to communicate using nonsecure products, the HIPAA Privacy Policy says we must comply (U.S. Department of Health and Human Services, 2003). However, these should be exceptions, not our general rule,

and if we do have an exception, it needs to be documented. Your release should state that you offered to use secure products with this individual and explained the risks of not doing so, but the client refused and requested that you use a different, less secure method of communication.

- *Commercial Email/Texting Products:* Some therapists try to make a case for Google Workspace being an EHR. It is not. It is a group of standalone tools that are only secure 80%–85% of the time (Google Transparency Report Help Center, n.d.) and that likely will not allow you, as a provider, to meet your HIPAA obligations. Keep in mind that commercial products such as Workspace and Microsoft's Outlook were not originally intended to be health care products. Their primary audience has always been business. Somewhere along the way, they decided to add the minimum requirements to allow them to compete in the health care sector. However, their lack of 100% end-to-end encryption makes those types of products less than optimal choices for health care providers. Personally, I prefer to have my email and texting applications embedded in my EHR, assuming those features are encrypted 100% end-to-end. However, Hushmail and Proton Mail both have excellent security standards if you prefer to use standalone tools for email.
- *Grammarly and Speech-to-Text Services:* Products like Grammarly and also voice transcription or other speech-to-text services generally should not be utilized within your EHR. Products of this sort are classified as AI-driven technology because they learn and remodel themselves from user interactions and ping what you write or speak back and forth to their server. If you are using them within your EHR, you are providing an opening to all your client records, which could cause your entire record set to be compromised.
- *Progress Monitoring Tools:* One factor that some clinicians find important is the inclusion of progress monitoring tools in EHRs, to assist with insurance guidelines or to serve as a part of treatment. The only EHRs I have seen that have these kinds tools are not ones I would recommend for other reasons. However, it is likely that more EHRs will include these tools over time, so if you do not like what you see now and it is a feature you want, keep watching.
- *EHRs and Artificial Intelligence:* If an EHR enters into agreements with other companies to share, sell, or trade data sets with an AI engine, even if the data is de-identified, I would not personally feel comfortable using that EHR. My decision has to do with how AI works, how EHRs work, and in particular, the fact that AI models are programmed to learn. EHRs, by their nature, contain enough demographic information on each of the clients in your practice to allow them to be fully identified. An EHR that gives an AI tool access to its data is essentially handing the AI tool the medical records for your entire caseload: their demographic info, plus all notes, forms, assessments or other files you have added.
- *Evaluate a Handful of EHRs Before Making Your Decision:* Almost all EHRs offer a free trial. If they do not, that is a red flag, and it may be wise to avoid that product. Once you have narrowed your search to three or four products that seem to have the set of tools you want, sign up for free trials with all and enter a fake client or two to play around with. Test all the tools you are likely to use. Sign up for free demos of products you are considering. If you have explored the software on your own for a bit before the demo, you can ask specific questions during the demo. Requesting a tour of the product from support staff is also helpful, as they may be able to show you things you might really like but had not known to ask about.

Summary

Health care providers have different reactions when they are first exposed to some of the problems we have discussed that are inherent in EHRs. Some consider going back to keeping only paper records (or congratulate themselves for never switching). Others look for EHRs that are safer than the one they are currently using. Others understand the risks with their current product but decide they are worth taking. Others put their heads in the sand and go into denial: It is not true; my company would not do that, and so on. Still others think the things presented here probably are true, but they just plain do not want to think

about changing EHRs, a position I certainly understand and have some sympathies for.

For me, by far the most troublesome issue is the selling of de-identified data by EHRs. Once I realized how Terms of Service are being used against us and how catastrophic that can be, I began counting the Terms of Service I was asked to sign in a single week. I stopped counting after a few days because the sheer number was astounding. During 1 week, I had to sign new Terms from my ISP, my power company, some new features on my TV, Disney, Apple, H&R Block, Intuit, and several resulting from the purchase of a new HVAC system. The list goes on and on. I did not read any of them. Nor do I intend to start. I am not recommending rubber stamping Terms of Service. I am just saying that I do not have the emotional bandwidth to read everything I am asked to sign to keep my life running smoothly. The dilemma is real.

However, in my hyperawareness of the issue, I have also become aware that I am more willing to take risks with my own data than I am with that of my clients. I identify with the psychologist I interviewed who hugged herself to indicate how she felt about protecting her client records. It is my ethical duty to educate my clients about the risks inherent in any products I ask them to use and in the Terms of Service those products may ask them to sign. Given that I was willing to rubber stamp 10–15 Terms of Service from various companies, might our clients be even more likely to do the same with Terms we ask them to sign, due to transference and the halo effect? The halo effect certainly seemed to play a part in what happened with the Practice Fusion case discussed above.

Even if you are not reading Terms from any other companies, you may want to consider reading Terms and BAAs for any EHRs or other health care products you are using. By reading the Terms, you will have a better understanding of the product and can inform your clients. If you do not trust yourself to understand all the legalese, it might be worth it to ask an attorney for help. When you combine what you learn from reading a product's Terms with a solid understanding of various other concepts from this article, you should be able to assemble a secure, integrated set of tools tailored to fit the unique circumstances of your practice with an acceptable amount of "wooliness."

References

American Psychological Association. (2010, September 30). *Electronic health records: Psychology seeks profession's inclusion as "meaningful users"*. https://www.apaservices.org/practice/update/2010/09-30/health-records

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct* (2002, Amended June 1, 2010, and January 1, 2017). https://www.apa.org/ethics/code

Atherton, J. (2011). Development of the electronic health record. *Virtual Mentor*, *13*(3), 186–189. https://doi.org/10.1001/virtualmentor.2011.13.3.mhst1-1103

Bresnick, J. (2015). EHR usability: Key to unlocking physician satisfaction, quality improvements. *EHR Intelligence*. https://ehrintelligence.com

Dalton, L. (Host). (2023, August 10). *Simple practice's revamped T&Cs* [Audio podcast episode]. Person Centered Tech. https://personcenteredtech.com/tag/simple-practices-revamped-tcs/

Federal Trade Commission. (2016, August 16). *FTC approves final order in practice fusion privacy case*. https://www.ftc.gov/news-events/press-releases/2016/08/ftc-approves-final-order-practice-fusion-privacy-case

George W. Bush White House Archives. (n.d.). *In focus: Technology—Economic policy*. https://georgewbush-whitehouse.archives.gov/infocus/technology/economic_policy200404/chap3.html

Google Transparency Report Help Center. (n.d.). *Email encryption FAQs*. https://support.google.com/transparencyreport/answer/7381230?hl=en

Kolmes, K. K. (2023, September 22). *It had to be you: When your favorite EHR makes you break up with them* [Blog post]. Dr. Keely Kolmes. https://drkkolmes.com/2023/09/22/it-had-to-be-you-when-your-favorite-ehr-makes-you-break-up-with-them/

Litton, S. (2021). *Telehealth for the mental health professions: Constructive and evidence-based tips for practicing safely, efficiently, and legally*. Professional Resource Press.

Litton, S. C. (2024). *How de-identification has turned HIPAA on its ear (and other HIPAA tidbits pertinent to those of us in private practice)*. Independent Practitioner, Winter 2024. https://division42.org/independent-practitioner/

Miller, K. (2021, July 19). *De-identifying medical patient data doesn't protect our privacy*. Stanford Institute for Human-Centered Artificial Intelligence (HAI). https://hai.stanford.edu/news/de-identifying-medical-patient-data-doesnt-protect-our-privacy

Office for Civil Rights. (2013). *Summary of the HIPAA security rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

Office for Civil Rights. (2022, October 25). *Guidance regarding methods for de-identification of protected health information in accordance with the health insurance portability and accountability act (HIPAA) privacy rule*. U.S. Department of Health and Human Services. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#safeharborguidance

Reinhardt, R. (n.d.). *Cloud practice management system EHR/EMR—Reviews*. Tame Your Practice. https://www.tameyourpractice.com/blog/cloud-practice-management-system-reviews/

U.S. Department of Health and Human Services. (n.d.). *De-identification*. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#safeharborguidance

U.S. Department of Health and Human Services. (2003). *Summary of the HIPAA privacy rule*. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

U.S. Department of Justice. (2020, January 27). *Electronic health records vendor to pay $145 million to resolve criminal and civil investigations*. https://www.justice.gov/opa/pr/electronic-health-records-vendor-pay-145-million-resolve-criminal-and-civil-investigations-0

Received February 13, 2024
Revision received September 30, 2024
Accepted November 4, 2024 ■