Private Practice in the Age of Technology: EHRs and Telemental Health

Susan C. Litton, Ph.D.
Disclaimer

I am the creator of PSYBooks (psybooks.com) – which is an EHR for mental health professionals. It would be dishonest to tell you that I’m not biased toward it – because I am.

However, I can also tell you that I’m dedicated to people finding the right practice management tools for themselves – even if it’s just paper and pencil. With that in mind, although I do use PSYBooks to demonstrate various concepts in the presentation, please know that my primary goal is to teach and to pass along general information that I hope will be helpful.

Susan C. Litton, Ph.D.
Should technology even be used in mental health private practice? Is the view of our field changing?
How is technology being used in private practice?

1. Practice management tasks
2. Telemental health
3. Treatment-related technologies
1. Typical practice management tasks:
   - Scheduling
   - Billing (both client and insurance)
   - Accepting payments (client, insurance, ERA)
   - Documentation (both for the medical record and also for your personal notes)
   - Accounting and reports
2. Telemental health tasks

In addition to practice management, telemental health providers may also need:

- Video
- Online scheduling
- Online payment capability
- Online file storage
- Encrypted email
- Encrypted texting
3. Treatment-related technologies

• Apps (weight loss apps, fitness trackers, mood trackers, journaling apps, etc.)
• Sending clients to websites for specific information, online relaxation tapes, etc.
• Virtual reality treatments for phobias
• Other
Focus of This Presentation

This presentation will focus on the first two:

1. Practice management tasks
2. Telemental health
We Will Cover:

1. Practice Management Systems
2. Telemental Health
3. Putting it all Together
4. Demonstration
Definitions

Originally, the term EHR (Electronic Health Record) had a very specific meaning. However, at this point in time, the terms EHR, EMR (Electronic Medical Record) and practice management system are all used synonymously.

healthIT.gov offers this definition:

“EHRs are, at their simplest, digital (computerized) versions of patients' paper charts.”

Learn EHR Basics
However, they are so much more. Because EHRs are computerized, they offer features paper charts can’t, such as instantaneous data aggregation and analysis, and the ability to connect electronically with clearinghouses and insurance companies for things such as efiling and ERA processing. A good EHR will also keep track of changes in the industry so you don’t have to. This includes things such as new diagnostic codes (e.g., ICD-10), new CPT codes and new form requirements (e.g., CMS-1500 02/12).
Another big value of EHRs is that you’ll be able to keep ALL of your client data and information in one place. There’s one login to remember and no redundant data entry.

I like to think of EHRs as a set of tools for therapists. They need not be limited to tools for billing and notes. As we’ll see later, EHRs can also provide some or all of the tools you need to be to deliver HIPAA-compliant telemental health services to your clients.
Which EHR is Best?

A question I commonly hear is, “But there are so many EHRs, how do I know which one is best for me?”

In general, it depends on the needs of your practice, but the next several slides are designed to help inform you of some of the issues.
Types of EHRs

There are several factors to consider when choosing an EHR. Two important ones are:

• Scope
• Method of delivery
## Ways to Categorize EHRs

<table>
<thead>
<tr>
<th>Scope</th>
<th>Method of Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medical</td>
<td>Desktop</td>
</tr>
<tr>
<td>Behavioral Health</td>
<td>Web</td>
</tr>
</tbody>
</table>

© 2017 by PSYBooks, LLC
## Scope

<table>
<thead>
<tr>
<th>Scope</th>
<th>Method of Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td><strong>Medical</strong></td>
<td></td>
</tr>
<tr>
<td>(All are agency types)</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Health</strong></td>
<td></td>
</tr>
<tr>
<td>Agency</td>
<td></td>
</tr>
<tr>
<td>Private Practice</td>
<td></td>
</tr>
</tbody>
</table>
Types of EHRs: Scope

Scope is less about the number of people who will use the EHR and more about the number of roles those people have. For example, a hospital or clinic EHR might need different workflows for doctors, nurses, case workers, lab techs, front office staff, billing staff, etc.

In contrast, an EHR for an independent practitioner probably just needs a single workflow for themselves. Even if they have office staff, those individuals can be added as users and given the permissions that the therapist specifies. They don’t need separate workflows.
Large scale medical EHRs are typically more expensive and harder to learn. Some require a representative to come to your facility and set it up - train your staff, etc., all of which adds enormously to the price and complexity.

Maintenance can also be problematic since it’s a customized product. Prices are typically several hundred thousand dollars and monthly maintenance fees are equally hefty.
Behavioral health EHRs that are designed primarily for agency use tend to have some of the disadvantages of medical EHRs, i.e., being more expensive and harder to learn. Even though these fall within the specialty EHR category, which helps some, their breadth of scope is really more like a medical EHR.
Clinic/Agency Behavioral Health EHRs

Like the medical EHRs, these EHRs tend to have different workflows for each role at the agency. For example, admins might have one workflow, nurses another, psychiatrists another and therapists yet another.

They also use a “shared chart” model, meaning that each consumer at the agency has a single digital chart which can be accessed and added to by anyone at the agency. You do not have your own charts for your clients.
In contrast, there are quite a few good EHRs that are designed just for behavioral health practitioners in private practice. These have the advantages of being:

- MUCH less expensive
- Relatively easy to learn
- They do NOT have a shared chart model (i.e., you DO have your own charts for your clients.)

Additionally, many of these types of products are developed by mental health professionals, so there tends to be an awareness of what those of us in the behavioral health field might need.
Types of EHRs: Scope Summary

To summarize, the breadth of scope distinction is whether the EHR is designed for:

1. A large scale medical facility or
2. A subspecialty, like behavioral health

Within the behavioral health subspecialty, we can break it down farther:

a. Designed for agencies
b. Designed specifically for private practice

Now we’ll discuss the second way to categorize EHRs, i.e., by their method of delivery.
### Ways to Categorize EHRs

<table>
<thead>
<tr>
<th>Method of Delivery</th>
<th>Desktop</th>
<th>Web</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Scope</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical</td>
<td>(All are agency types)</td>
<td></td>
</tr>
<tr>
<td>Behavioral Health</td>
<td>Agency</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Private Practice</td>
<td></td>
</tr>
</tbody>
</table>
All EHRs are software. However, how that software is delivered to you can vary. The two main types are:

- **Desktop apps**: Software that’s actually installed on your computer – either downloaded from the Internet or installed with a CD. It’s often said that this software “lives” on your computer.

- **Web apps**: Software that does NOT get installed on your computer, but that you access with a Web browser such as Chrome, Firefox, Edge or Safari. This kind of software “lives” on the Internet.
Desktop Apps: Pros

• Pros to having your EHR software on your computer:
  – It’s a one-time purchase instead of a monthly subscription fee
    • However, some companies charge a monthly fee for support
    • Also, when you buy a new computer – or if the software becomes outdated, you’ll likely have to purchase a new version of the software
  – Some people feel it’s safer
Desktop Apps: Cons

• Cons to having your EHR software on your computer:
  – You have to install it and there may be compatibility issues
  – You can never access your EHR except on that one machine
  – If your computer dies, you may have to purchase a new version of the software. Also, unless the program had a way for you to backup your files ahead of time (and you had done it), you may lose all your data
  – Getting updates can be problematic so your software may stay out of date
  – You are responsible for downloading necessary patches for bug fixes
  – **Client PHI is stored ON your computer so if you lose it or your computer gets stolen, you have a HIPAA breach**
Web Apps: Pros

• Pros to using a web based EHR:
  – There will never be compatibility issues.
  – You can access your EHR from any computer that has access to the Internet.
  – Getting a new computer is never a problem because there are no files to transfer. You access your data with your browser.
  – New requirements for codes, forms, etc., are all taken care of for you.
  – Bug fixes and other updates happen automatically, behind the scenes.
  – Client PHI is stored on the Web, so if your computer or tablet is stolen or lost, your client data is safe and you do NOT have a HIPAA breach (assuming you haven’t saved your password in your browser)
Web Apps: Cons

• Cons to using a web based EHR:
  – Some people feel they’re too expensive.
  – Some people are uncomfortable with the idea of having their patient data on the Internet because they don’t think it’s safe.
So . . . Is it Safe?

There are two types of potential safety issues when using a web-based app:

• Data at rest (when the data is just sitting on the server)

• Data in motion (as it’s going from your computer to the server and back)
“In motion” protection is typically handled by SSL (Secure Sockets Layer).

• The URL will begin with https:// (note the "s") instead of just http://
• There will be a closed lock displayed somewhere on your browser
Public-key encryption requires two keys: the "public" key and the "private" key.
Public-key encryption requires two keys: the “public” key and the “private” key.
SSL Encryption

Public-key encryption requires two keys: the “public” key and the “private” key

John Doe
08/02/1968
SSL Encryption

Public-key encryption requires two keys: the "public" key and the "private" key.

John Doe
08/02/1968

"Ö{ö;iÊ
²7|È~)ŠX
'w'α‡ª„L
‡4«Â1ë"
SSL Encryption

Public-key encryption requires two keys: the “public” key and the “private” key.

John Doe
08/02/1968

'Ø{ö;i(578,641),(694,745)
27 | È~}ŠX
'w'α‡¢“L
‡4«Â1ë"
SSL Encryption

Public-key encryption requires two keys: the “public” key and the “private” key.

John Doe
08/02/1968

🔒

Ễ deliberately encrypted

Decrypt with the private key

🔓
SSL Encryption

Public-key encryption requires two keys: the “public” key and the “private” key

John Doe
08/02/1968

0{ö;iÊ
²7|Ê¬}šX
'w'α‡ª“L
‡4‹Álê"

John Doe
08/02/1968
Data in Motion Security is Covered by SSL

• Current SSL certificates require 2048-bit numbers. (That's $2^{2048}$)

• It is estimated, that standard desktop computing power would take a little over 6.4 quadrillion years to break a 2048-bit SSL certificate.

• This encryption level hasn't been cracked yet and some feel it is NOT crackable now and probably won't be for many years to come.

DigiCert
So What Causes All of the Safety Issues?

The problems tend to arise with data at rest. And you may be surprised to see who and what the major culprits are.
So What Causes All of the Safety Issues?

Hacking actually accounts for a very small percentage of reported healthcare data breaches. One author who has analyzed healthcare breach data notes that the media most often involved in breach incidents are laptops and paper records, i.e., they don’t involve the Internet at all.
## Breaches Affecting 500 or More Individuals

<table>
<thead>
<tr>
<th>Type of Breach</th>
<th>Number</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Theft</td>
<td>68</td>
<td>63%</td>
</tr>
<tr>
<td>Other</td>
<td>15</td>
<td>14%</td>
</tr>
<tr>
<td>Loss</td>
<td>10</td>
<td>9%</td>
</tr>
<tr>
<td>Unauthorized Access</td>
<td>7</td>
<td>7%</td>
</tr>
<tr>
<td>Improper Disposal</td>
<td>3</td>
<td>3%</td>
</tr>
<tr>
<td>Hacking/IT Incident</td>
<td>2</td>
<td>2%</td>
</tr>
<tr>
<td>Incorrect Mailing</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Misdirected Email</td>
<td>1</td>
<td>1%</td>
</tr>
<tr>
<td>Phishing Scam</td>
<td>1</td>
<td>1%</td>
</tr>
</tbody>
</table>

Theft and loss account for 72% of the reported breaches as of March, 2013. The thing that most people fear – hacking and/or IT incidents – only account for 2% of the breaches.

[HHS.gov](http://www.hhs.gov)
SSL Encryption

In other words, data breaches are happening in one of two places: your computer (tablet/cell phone) or the server:

Public-key encryption requires two keys: the “public” key and the “private” key.
Data at rest issues can happen on your computer and/or the computer (server) you’re accessing.

Web-based EHRs eliminate your computer as a source of concern for breaches or data loss because no data is actually stored there. This automatically makes them at least 50% safer than a desktop EHR.

With a desktop EHR, if your computer is lost, stolen, or dies, you’ve not only lost all your client data, you may also have a HIPAA breach.
Security: Data at Rest (the Server)

With web-based EHRs, unless you specifically download files to your computer, the only computer you have to worry about is the one you’re sending your data to – called the server.

Servers, unlike your personal computer, typically have top-notch security and back-up systems.
Amazon's S3 Servers: An excellent example

"AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff."

Amazon Web Servers
But what if something happens to the server? Don’t their computers go down, too?

Yes. But good companies protect against this in several ways. They take a lot of preventative steps to protect their machines, and if those fail, and they also have:

"redundant co-location facilities that are geographically dispersed".

Healthcare and the Cloud Revisited: It's Your Data, How Do You Protect It?
In plain English, that means that the company makes frequent backups of your data on additional servers that are not in the same location as the original one. If a disaster occurs where one of your servers is housed, you’ll be switched over to use another one – often in a totally different part of the U.S. or the world. Chances are, you won’t even know this has happened. Companies strive to make such transitions pretty seamless.

Healthcare and the Cloud Revisited: It's Your Data, How Do You Protect It?
Additionally, in some cases, an EHR will encrypt data at rest, too, making it ultra-safe. For example, PSYBooks’ email system, file uploads, and some other aspects of the program are done this way:

SAFE

SAFE
Security Issues: Summary

Although no solution for protecting client data can ever be 100% safe, using a web-based EHR is probably the safest method you can use.
## Summary Table of the Types of EHRs

<table>
<thead>
<tr>
<th>Scope</th>
<th>Method of Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Desktop</td>
</tr>
<tr>
<td><strong>Medical</strong></td>
<td></td>
</tr>
<tr>
<td>(All are agency types)</td>
<td></td>
</tr>
<tr>
<td><strong>Behavioral Health</strong></td>
<td></td>
</tr>
<tr>
<td>Agency</td>
<td></td>
</tr>
<tr>
<td>Private Practice</td>
<td>☑️</td>
</tr>
</tbody>
</table>
Second Objection: Too Expensive

The other concern about EHRs is that they’re too expensive.
• Most private practice EHRs are in the $40 - $80 per month range. Some offer discounts for larger practices.
• If they include telemental health technologies that you would be purchasing elsewhere, the net out-of-pocket is even less.
• There are a few free EHRs but there are some issues with them.
Free EHRs

• They’re all large scale medical EHRs.
• They tend to not be as user-friendly or as carefully designed as other apps.
• They’re unlikely to have telemental health components so you would have to purchase those elsewhere.

It takes a lot of money to create an EHR. Those that are offered for free have to be getting their money somewhere – and that’s where problems can arise.
Three Types of “Free” EHRs

• Companies who want to use your clients’ data. Specifically, they de-identify it and sell it to willing buyers.

• Billing companies who want you to sign up for their services (for a fee) and who offer to “give” you a free EHR to do so. Usually, the total amount you pay is more than a stand-alone EHR would be.

• Companies (called “clearinghouses”) who are paid per claim fees by insurance companies and are hoping to make money when you efile or possibly on other types of interactions you may engage in with insurance companies.
The “Hit By a Bus” Phenomenon

Ethics experts encourage us to make sure we have our practices taken care of us in case of our death. We tend to put this kind of thinking off, but there’s always the “hit by a bus” possibility.

EHRs make this a breeze, because ALL of your client records are in one place.
Telemental Health

Part Two: Telemental Health
At this point in time, there is no “one” definition of telemental health. Rather, the definition is contextual, i.e., depending on the particular laws, ethics boards, insurance companies, employers, etc., that govern your practice.

No two states have the same laws or definitions and, within a state, organizational requirements also differ. For example, LPCs have different rules & guidelines than do psychologists or social workers. Employees of the VA will have different definitions and rules than employees at state agencies, private hospitals, or those of us in private practice, and so on.
However, a broad general definition that will give us a starting point is that telemental health is:

“The use of some sort of technology which allows us to provide behavioral health services at a distance.”
Defining the Parameters

To go a little deeper, let’s look at the underlined terms:

“The use of some sort of **technology** which allows us to provide **behavioral health services** at a **distance**.”

The next slides will discuss each of the underlined items.
Technology Defined

“The use of some sort of technology which allows us to provide behavioral health services at a distance.”

A definition I like to describe telemental health technology is:

“If it has a plug or a battery, it’s probably telemental health.”
Behavioral Health Services Defined

“The use of some sort of technology which allows us to provide behavioral health services at a distance.”

The broadest version of behavioral health services would be any contact with a new, existing or former client – or any contact with another individual about such a client.
An example of what might and might not constitute behavioral health services is that Georgia’s Composite Board specified that phone calls made ONLY for scheduling do not constitute telemental health. However, if, during the call, the client also comments about how they’re feeling or what’s going on in their lives, the line has been crossed – which would mean that the therapist would be required to take ethics CEUs in telemental health.
This could create tricky situations if you’re trying to avoid triggering the telemental health label because you don’t want to take the CEU hours. For example, imagine this scenario . . . you THINK you’re returning a simple call for scheduling, when . . .
“Don’t Tell Me How You Are!”

“Wait! Wait! Don’t tell me how you are! I don’t want to have to take the ethics CEUs for telemental health!”
Distance Defined

“The use of some sort of technology which allows us to provide behavioral health services at a distance”.

Distance doesn’t always really mean distance. For example, if you’re sitting in the room with your client, but the two of you are using your phones, tablets, etc., to share information, that may still qualify as telemental health since you’re each on your own device.
Distance Defined

Distance is less about physical distance, but refers more to the fact that the information is transported by some type of network or Wi-Fi from the client’s device to your device.
It seems then, that in trying to define telemental health, what we’re really talking about is the use of technology – pretty much any kind of technology (even phones) – in communicating with and/or serving our clients.
In Other Words . . .

Most of us are already doing it.
The Wave of the Future

• Many believe that we are right on the brink of a telemental health explosion, where more and more of our services will be provided by technologies such as video chat, encrypted email, etc.
• For some therapists, this may just be an occasional video chat session, e.g., for a mother who’s child is sick and can’t make it to your office that week.
• Others are wanting to establish practices that consist entirely of distance counseling.
This means that, whether we like it or not, the use of technology with clients makes us responsible for a host of both legal and risk management issues, which can feel a bit overwhelming.
Risk management issues in telemental health include:

1. Have a thorough Informed Consent
   A. This needs to be specific to telemental health although it can be part of a larger document

2. Make sure both you and the client understand how to use the required technology

3. Have contingency plans for client emergencies

4. Verify client identity and location
Legal Issues Include:

1. Issues mandated by state and local laws and licensing boards.

2. All technologies used must be HIPAA compliant
   - Privacy must be maintained for both therapist and client
   - All transmissions must be encrypted or else be able to explain why not
   - You must have a Business Associate Agreement (BAA) with each vendor you use
Did You Know . . .

These commonly used technologies are NOT HIPAA-compliant:

– Skype
– FaceTime
– Google Calendar, Gmail, Drive (free versions)
– Dropbox (free version)
– iCloud
– Hushmail (free version)

There are many, many more.
Actually, most popular products for these sorts of technologies do NOT offer a BAA or some of the other things required by HIPAA, especially in their free versions.

Even with paid versions, you should read the documentation carefully. In most cases, vendors of individual products like these added HIPAA compliance as an afterthought so they don’t always cover all the bases.
What Do I Use Instead?

To better understand the dilemma and the options, let’s start with the basics:

Telemental health requires both **hardware** and **software**.
Telemental Health Hardware

Here are some hardware items you may need. None are essential – it all depends on how you setup and manage your practice:

• Computer and/or tablet
• Phone (cell)
• Phone (land line)
• Fax Machine
You may want/need some of these:

- Encrypted email
- Encrypted texting
- Online file storage/sharing
- Online scheduling/calendars
- Video conferencing
- Efiling and/or sending digital statements
- Retrieving ERAs
- Various types of payment processing (when PHI is involved)
- Efax
With This Much Hardware & Software

How do we satisfy our legal and risk issues?
Your hardware itself doesn’t pose much risk. The software that RUNS your hardware is more likely to be problematic (i.e., operating systems such as Win10, Mac OS X, the current iPhone or Android operating systems, etc.)

Also, browsers (Firefox, Chrome, Edge, Safari, etc.), and other software installed on your hardware can have security issues.
How to Protect Hardware

1. The safest thing is to not keep PHI on your hardware

2. If you do, common ways to protect hardware are:
   – Password protect computers, tablets, cell phone
   – Encrypt the same items – or at least any files containing PHI
   – Consider getting “wipe” software you can activate in case your device is stolen

3. In addition, to make sure your operating system for the hardware is safe, set it to always receive updates when they’re available.
How to Protect Hardware

If you follow the suggestions above, we can pretty much eliminate your actual hardware (computer, cell phone, etc.) as a potential problem area.
Telemental Health Software

However, that still leaves us with a pretty long list of software:

- Encrypted email
- Encrypted texting
- Online file storage
- Online file sharing
- Online scheduling/calendars
- Efiling
- Retrieving ERAs
- Various types of payment processing
- Video conferencing
- Efax
Legal Issues:

According to our scary judge photo earlier, in addition to adhering to state and local laws, for each of these tasks, we also need to make sure we:

– Maintain privacy for both therapist and client
– Make sure all transmissions are encrypted or else be able to explain why not
– Have a Business Associate Agreement with each vendor
So That Means . . .

We would need to find one vendor for our encrypted email, another for our encrypted texting application, another for online file storage, another for video chat software . . . and so on down the list.

We’d also need to make sure we can get a Business Associate Agreement with each vendor and that all products are HIPAA compliant.
That’s a Pain and Costs $$$

Not only is it a pain to read through the documentation of each company to make SURE all the i’s are dotted and the t’s crossed, but setting up your telemental health technology this way is costly. Even those companies that offer a free version of their product typically charge for the HIPAA-compliant version (e.g., Hushmail).

Even if you’re only paying the equivalent of $10 or $20 a month for a service, if you multiply that by several different services, it adds up.
More Data Entry

Last but not least, when you have separate software for each of your telemental health tasks, you have to duplicate your data entry. In other words, you have to enter your client data in your calendar/scheduler, your email software, your billing software, your efiling software, your video chat software, etc.

Also, if your client’s info changes (e.g., new phone, address, email), you have to change it in each application.

However, there’s a better solution:
Putting it All Together

Part Three:

Bundle Services: EHR++
Many EHRs offer – or will be offering – quite a few of the technologies needed by telemental health. With your EHR, everything already IS HIPAA-compliant and encrypted and you already have a Business Associate Agreement with that vendor.

Also, since EHRs had HIPAA in mind from the outset, they are more likely to follow the laws closely.
Furthermore, if the EHR is designed well, everything will be integrated. You’ll only have to enter client data once and that same data will automatically be used to populate your billing, scheduler, email, video, etc. If a client’s info changes, you only have to make the change one place.
And Best of All . . .
With All Client Records in One Place

You only have ONE URL and password to remember.
What’s Available Now?

EHRs vary widely in the number of telemental health features they offer.

In the next slide, telemental health features currently offered by **most** EHRs are in green; features offered by **some** EHRs are in yellow; and features that may **not** currently be offered by any EHRs but are still things that **CAN** be done are in orange:
Telemental Health Software

Green = most EHRs. Yellow = some EHRs. Orange = can be done:

- Encrypted email
- Encrypted texting
- Online file storage
- Online file sharing
- Online scheduling/calendars
- Efiling
- Retrieving ERAs
- Various types of payment processing
- Video conferencing
- Efax
In other words:

• Most good EHRs currently offer efiling and ERA retrieval.
• Some also offer encrypted email, online file storage, online scheduling/calendars, various types of payment processing and video conferencing.
• Although I’m not aware of any EHRs that currently offer encrypted texting or efax, the technology is available so it’s probably just a matter of time.
Conclusion

• What this means is that either now – or in the near future – you should be able to get most of your telemental health technology needs met with at least some EHRs.
To summarize what we’ve covered so far:
• Telemental health is the wave of the future.
• EHRs that also offer technologies for telemental health makes sense because:
  – You only have one BA agreement to sign. Everything is automatically HIPAA-compliant.
  – You have ONE login and only have to enter client data once.
  – Client data is all organized. You don’t have your clinical notes in one place, your client financial records in another, your schedule in another, and client contact and other demographic info someplace else.
Qualifications of Good Behavioral Health EHRs

A good behavioral health EHR should:

• Be safe
• Be relatively inexpensive
• Have the features that YOU want
• Be user-friendly enough that you can figure out most things on your own
• Have a good way to get help and support for those things that stump you
• Be well-maintained and kept up to date
Does My EHR Support Telemental Health?

Look for EHRs that are still developing and adding new features. A static EHR usually isn’t a good idea because it may mean that it’s been abandoned by its developers. This would mean that it would be unlikely to grow and change with the industry.
Beware of Long-Term Contracts

Similarly, EHRs that require long-term contracts could be problematic if they end up not keeping up with the field. Technology changes extremely rapidly and you don’t want to be stuck with an EHR that could seem ancient after awhile.
Beware of Long-Term Contracts

I heard one horror story recently of a business that had signed a 5-year contract with an EHR and it had not even kept up with changes in the field at ALL in those 5 years. It was almost useless because it had old CPT codes, old HCFA forms, old diagnostic codes, etc.
Look for Some or All of These Features:

EHRs that are aware of the telemental health field and that have plans of developing their products in that direction, should have some or all of the following in addition to their normal EHR features:

- Encrypted email
- Online file storage
- Online scheduling/calendars
- Various types of online payment processing
- Video conferencing
What Features Do YOU Want?

Look for the features that YOU want. For example, if you know you’re never going to do video sessions, you don’t need an EHR that offers that. On the other hand, if an EHR has all the features you want and also happens to have video chat, it won’t hurt any to have a feature you don’t use.
Some Possible Candidates

- PSYBooks  
  https://psybooks.com
- SimplePractice  
  https://www.simplepractice.com/
- Therapy Notes  
  https://www.therapynotes.com/
- TherapyAppointment  
  http://therapyappointment.com/
Caveats About the List

The previous list are web-based, behavioral health, private practice EHRs about which I’ve heard more positive than negative feedback. However, except for PSYBooks, I have NOT used any of them myself, nor do I know whether they have – or intend to have – features for telemental health.
We will be using PSYBooks for the demo but most of the better EHRs have similar features. This is to give you an idea of what EHRs can do.
What replaces what, #1

The Active Charts Tab:

THIS = THIS
The Archived Charts Tab:

**THIS** = **THIS**
What replaces what, #3

An Individual Client Chart:

**THIS**  =  **THIS**
ERAs

- ERA = Electronic Remittance Advice
- ERAs are sometimes called “electronic EOBs”.
- When you sign up for ERAs, the insurance company sends an electronic version of the EOB directly to PSYBooks.
- PSYBooks parses the information for you automatically so all you have to do is review and approve it.
Questions?
References


References


