Webinar Materials for “Using Text and Email with Clients – Guidance and Resources for Providers”

Guidance on Texting and Email With Clients for EASA-Affiliated Clinicians

Author: Roy Huggins, LPC NCC
Version: 1
Completed Date:

Preamble

Purpose of This Document

This guidance is intended to assist EASA clinicians and administrators in creating organizational policies regarding the use of text messaging for communications between clinicians and their clients, client guardians, and client caregivers.

Policies surrounding the use of texting in this context will require that administrators and clinicians make choices intended to balance the clinical needs of clients and families, as well as the typical behavior patterns of those persons, with the legal and ethical concerns that arise in the use of email and text messaging as part of clinical communications. These policy choices will need to address:

- Whether or not to allow email and/or texting at all in agency policies.
- Selection of communications services, software, hardware, and potentially other technological elements.
- Procedures for the secure use of email and texting services.
- Procedures to set up clients and clinicians for successful and safe use of email and texting in their relationships.
- Procedures for limiting the contents of emails and text messaging-based communications to subject matter appropriate for the medium and for the clinician-client dyad.

Intended Audience

This guidance is intended for use by administrators, legal counsel, information system security advisors, and mental/behavioral health clinicians in EASA-affiliated agencies throughout Oregon.

Scope of Legal-Ethical Guidance

This guidance will address security and privacy standards defined in the various federal rules that are collectively referred to as “HIPAA.” It will not address other regulatory or legal standards.

This guidance will also address the ethical standards of the following mental health professional associations:

- American Association of Marriage and Family Therapists
- American Counseling Association
- American Psychological Association
- National Association of Social Workers
- National Board for Certified Counselors

This guidance is not a replacement for legal advice nor for the advice of personnel in charge of information system security. Legal counsel and, where applicable, personnel in charge of information system security must always be consulted before acting on the advice in this document.

Abstract and Summary of Guidance

SMS texting and email are old technologies that were not designed for use in environments where security is necessary. In addition, the influence of mobile communications technology on professional ethics is only starting to be realized and managed by professional associations. However, a large variety of secure and compliance-supporting services have popped up to fill the security void for healthcare agencies.

A 3-Piece, Secure and Compliant Solution

It is relatively easy for mental/behavioral health agencies to manage the risks involved in texting and email by:

1. Using specialized email and texting services which support security and compliance needs.
2. Supporting clients and families to use these services when communicating with their providers.
3. Monitoring the use of mobile communications in therapeutic relationships to make sure they remain supportive of healthy therapeutic boundaries.

Unfortunately, in regards to texting in particular, the 3-piece solution described above requires clients to possess smartphones with sufficient data service, and it is not always viable for all client populations. Additionally, secure email and texting services may also present barriers to use that result in client noncompliance with the agency’s communication policies.

The Nonsecure -- but Still Compliant -- Alternative

There remains, then, the possibility to employ appropriately provisioned SMS texting and conventional email services with clients who desire to accept the privacy risks. This solution -- which is described below in more detail -- carries greater risk, but may be compliant and acceptable for some agencies.

Important Concepts

The following are definitions of terms and concepts vital to this guidance.

Note that the definitions provided below are designed to ensure that this guidance is the most useful it can be to its intended audience, rather than being designed to ensure that this guidance uses the same terminology that is used in the telecommunications industry.

Policy-Related Terms

Service

This refers to 3rd-party vendors that supply communications or other services.

For example, SMS texting services would usually be provided by a phone company such as AT&T, Cricket, T-Mobile, and the like. It is also possible to get SMS *sending* (but not receiving) services through cloud services like Twilio.

For another example, messaging apps are generally part of a service. E.g. Apple’s iMessage is a service provided by Apple for its customers.

Nonsecure Service

A service which does not employ technical and administrative security measures sufficient, by themselves, to meet the regulatory and ethical needs of mental health clinicians for keeping information secure.

For example, SMS texting is nonsecure. It may still be usable as part of a compliant solution, however.

Most messaging apps are also nonsecure under this definition, even though they may employ encryption as part of their functionality.

Secure Service

A service that employs technical and administrative security measures sufficient, within themselves, to meet the regulatory and ethical needs of mental health clinicians for keeping information secure.

Some messaging apps are secure under this definition, because they will execute HIPAA Business Associate Agreements and also employ such important measures as strong encryption and authentication. However, they would still need to be combined with other factors to create a compliant solution.

Solution

A combination of devices, services, and policies meant to achieve a particular result.

For example, SMS texting is a “service.” Using SMS texting in conjunction with a defined set of assessments and procedures would be a “solution.”

Compliant Solution

A solution that ensures that its desired result is achieved in a manner that is compliant with the regulatory and ethical standards covered in this guidance.

For example, a compliant solution could consist of the use of a secure messaging app along with policies and procedures for onboarding clients to using the app and supporting healthy boundaries throughout the therapeutic relationship. **This solution is compliant because of the combination of risk management policies and secure technology choices. The secure technology choices do not, by themselves, make compliance. Only the whole solution is compliant.**

For another example, a compliant solution could consist of performing a collaborative analysis of a client’s technical capabilities and risks surrounding text messaging, getting a signed request from the client or guardian to use nonsecure SMS texting, discussing with the client what is appropriate to text about and what is not, and then proceeding to use that SMS texting service with the client. **This solution can be compliant because of the manner in which it uses risk management policies -- even though the (SMS-based) service is not secure.** More on policies based in nonsecure services will be covered below.

Types of Email and Their Strengths and Weaknesses

Email 1) Conventional Email

Email as we typically know it travels from one service provider to another over the Internet. If a clinician sends an email to a client, for example, the email message travels from the clinician’s email service provider to the client’s email service provider. The client then retrieves the email from their “Inbox” and reads it.

Email that functions like this will be referred to as “conventional email.”

Important characteristics of conventional email:

1. Conventional emails can be exchanged between any two parties who possess email service. Many free email services exist, making email accessible to anyone with a device that can access the Internet.
2. By default, conventional email is a “nonsecure” service (see definition below.) Sometimes it can use technical security, however.

3. **As described in item 2 above, conventional email may not provide technical security. It can be part of some compliant solutions, however.**
4. **As described in item 1 above, conventional email has excellent interoperability. This makes it more practical for use with clients who do not possess smartphones or who do not wish to use specialized apps.**

Email 2) Escrow Secure Email

Many readers of this document will have used escrow email at work or when visiting their medical provider. Escrow email refers to a system where the sender (often a clinician) designates an outgoing email as “secure.” Rather than sending the message itself, the clinician’s email service sends the recipient a notification that instructs the recipient to click a link and log in to a web page portal where they can read the sender’s secure message.

Escrow secure emails do not deliver their message contents to the recipient’s Inbox. The message itself remains solely inside the sender’s email system.

Examples of services that provide escrow secure email include Hushmail, LuxSci, Protonmail, most patient portals, GSuite Gmail’s confidential mode, and many, many others.

Important characteristics of escrow secure email:

1. Escrow secure emails can be sent to anyone who possesses an email service. Not all escrow secure email services will facilitate a reply, however. Escrow secure email is, for the most part, well-suited to sending a single important message securely and less well-suited to facilitating conversations.
2. Escrow secure email is one of the more technically secure methods of electronic transmission available short of using a specialized messaging app.
3. **As described in item 2 above, escrow secure email provides both security *and* can be a key piece of a compliant solution for email.**
4. **As described in item 1 above, escrow secure email has excellent interoperability. However, it is not conducive to conversations with a high volume of messages being exchanged. It is less likely to be successful with clients who do not wish to use a messaging portal.**

Types of Texting and Their Strengths and Weaknesses

What is “Texting”?

Huggins (2016) defines texting as “...messaging in the form of short, often informally written, messages using a mobile device.” Text messages may also be read or written on laptop or desktop computers as a convenience. Their focus, however, is for use on mobile telephones including classic cellular phones and smartphones. The terms “Texting” and “text messages”, as used in this guidance, may refer to any of the specific media defined here.

Importantly: In this guidance, the word “texting” does *not* refer solely to SMS.

Texting 1) SMS / MMS

SMS is the medium behind classic text messaging as seen on cellular phones for as long as texting has existed.

MMS is a slight variation on SMS that allows the transmission of media such as pictures and videos. In this guidance, “SMS” will be a stand-in term for both SMS and MMS messages, and should be construed as always referring to both media.

Android smartphones and classic cellular phones generally use SMS for all their built-in texting.

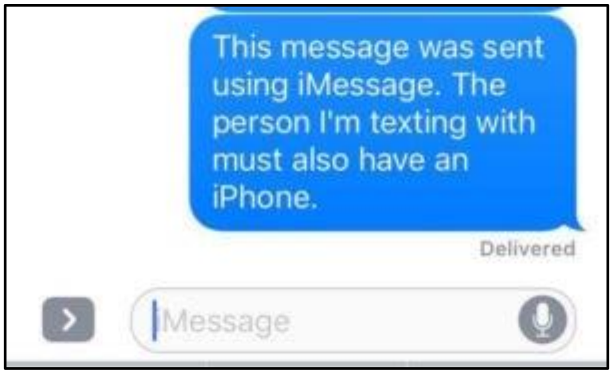
Important characteristics of SMS:

5. SMS messages can be exchanged between nearly any two cellular devices regardless of what services they subscribe to, including classic cellular phones and smartphones. E.g. an iPhone serviced by AT&T can freely exchange SMS messages with a 15-year-old Nokia cellular phone serviced by Cricket.
6. Due to the nature of the SMS medium, SMS is *always* a “nonsecure” service (see definition below.) It is not possible for SMS messages to use technical security measures that meet the definition of “secure” for this guidance. However, SMS may be part of a “compliant solution” (see definition below.)
7. **As described in item 2 above, SMS texting cannot provide technical security. It can be part of some compliant solutions, however.**
8. **As described in item 1 above, SMS texting has excellent interoperability. This makes it more practical for use with clients who do not possess smartphones or who do not wish to use specialized apps.**

Texting 2) Messaging Apps

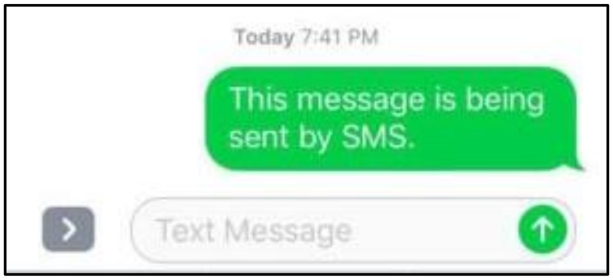
Many applications of texting are performed by proprietary apps, utilizing their own protocols and methods of exchanging information, that allow individuals to exchange text messages with each other. In this guidance, we will call these “messaging apps.”

A very common example of a messaging app is iMessage, which is the app used when iPhones text with other iPhones. In such cases, the user’s iPhone does not use SMS at all to exchange messages. Instead, it uses Apple’s proprietary iMessage network to exchange messages between the two iPhones. Such messages will appear with a blue background on each user’s iPhone. iPhones will use SMS when communicating with other devices which are not Apple devices. When an iPhone uses SMS to exchange messages, the background of the message appears green.



This message was sent using iMessage. The person I'm texting with must also have an iPhone.

Fig. 1: Screenshot of an iMessage message on an iPhone



This message is being sent by SMS.

Fig. 2: Screenshot of an SMS message on an iPhone

Other popular examples of messaging apps include WhatsApp, Viber, Snapchat, Signal, TigerConnect, OhMD, Spruce Health, and many, many more.

Important characteristics of messaging apps:

1. Messaging apps may or may not be technically secure, and they may or may not be compatible with compliant texting solutions (see definition below.) Security and compliance compatibility depend entirely on the particular service and how it interfaces with regulatory and ethical needs. However, there is great potential among messaging apps for both security and compatibility with compliance needs.
2. Nearly all messaging apps can only exchange messages with themselves. I.e. all parties involved in the texting exchange have to be using the same app/messaging service. E.g. Apple's iMessage only works for talking to other people using Apple's iMessage.
3. Generally, messaging apps *cannot* be used on classic cellular phones -- they require smartphones or computers to function.
4. **As described in item 1 above, the right messaging app can provide both security *and* be a key piece of a compliant solution for texting.**
5. **As described in items 2 and 3 above, messaging apps have poor interoperability. This makes them impossible to use with clients who do not possess smartphones and more difficult to use with clients who do not wish to use specialized apps.**

The Devices We Use and How They Fit In

Personal Devices

In this guidance, “personal device” refers to devices that are owned by the individual using them. Personal devices are differentiated from devices supplied by the agency.

Device 1) Classic Cellular Phone

This refers to a handheld device used to communicate via the cellular phone network. Classic cellular phones are typically in the form of “candy bar” phones, “flip phones,” and the like. In this guidance, the term “classic cellular phone” also encompasses the form of mobile device called “feature phones.”

We’re using this term to differentiate “dumb” or “feature” phones from smartphones.

Clinicians and administrators should maintain awareness that many lower-SES people in the United States possess classic cellular phones rather than smartphones. They may have limited cellular service plans, as well. This opens up the opportunity for texting-based communication with lower-SES clients, but limits that communication to SMS texting only.

Generally speaking, classic cellular phones can use SMS texting, but they cannot use any messaging apps. Communications solutions that depend on secure messaging apps will not work if anyone involved (clinician, client, family, etc.) has a classic cellular phone.

Device 2) Smartphone

This refers to a mobile device that acts as a miniature computer and is able to connect to both the telephone network and the Internet. Smartphones can use their cellular connection or available WiFi services to do this.

The term smartphone generally means Apple iPhones, Android phones, and Windows phones. However, wherever this guidance mentions smartphones, one may get equivalent functionality and/or equivalent security risks from a tablet (e.g. iPads or Android tablets) or a computer.

Generally speaking, smartphones can use both SMS texting and a large variety of messaging apps. When all parties (clinician, client, family, etc.) involved in a relationship possess smartphones with consistent phone service, solutions focused on secure messaging apps and/or any kind of email can function well.

Device 3) Computers and Tablets

This refers to a tablet computer, laptop computer, or desktop computer. iPads and Android tablets are “tablet computers.”

Computers are generally Windows-, Macintosh-, and possibly Linux-based computers.

Messaging apps are often usable on computers and tablets. Some tablets support cellular connectivity, however, and so may also be able to do SMS texting.

Outside of tablets which support cellular connectivity, computers and tablets generally require an Internet connection (e.g. WiFi) in order to perform any form of email or texting.

Generally speaking, computers and tablets can use messaging apps and all forms of email, but typically cannot be used with SMS messaging. Computers and tablets, when paired with readily available Internet service, may be part of a communication solution that involves any form of email and/or secure messaging apps.

Permissibility of Using Email or Texting in Clinical Contexts

Do HIPAA and professional ethics allow clinicians to use email or texting in any form? There is not a specific “okay” or “not okay” designation for either form of communication. Rather, there are standards that need to be applied against the particular texting-based or email-based solution that the agency wishes to use.

Here we break down the two standards that are most immediately relevant to email and all forms of texting: Transmission Security, maintenance of records, and the use of third party service providers to handle sensitive client information.

Transmission Security

Texts and emails travel over the Internet (and sometimes telephone networks.) So just like there is a need for US Postal Service truck drivers to protect their cargo from intrusion on the road, there is a need to secure the privacy and integrity of texts and emails as they travel to their destinations.

Professional Ethics on Transmission Security

Ethics codes which directly address transmission security are consistent in requiring that **technical security measures** be used to keep transmissions secure, and that **clients are informed of risks** in electronic transmissions. There is generally an implication that clients need to be allowed to opt out of the use of such transmissions if they don’t see the risks as acceptable.

Ethics codes and guidance documents vary on how they describe “technical security measures.” However, they frequently cite the essentiality of **encrypting** the information that is being transmitted.

HIPAA on Transmission Security

HIPAA’s Security Rule has a standard called, “Transmission Security.” It requires that sensitive information being transmitted over “electronic networks” must be protected with “**technical security measures**.” HIPAA defines “technical security measures” elsewhere in its rules, and so we know that the Transmission Security standard implies the necessity of **encrypting** messages, as well as using strong methods to **authenticate** the sender and receiver of messages.

Maintenance of Records

Professional Ethics and Maintenance of Records

Ethics codes call on clinicians to maintain records, although it is generally the licensing boards which define how long they must be kept.

Many ethics codes make a point of mentioning that emails and texts related to a client are **part of that client’s record**, and so must be kept along with the client’s other records. This also means there may be a need to specifically **inform clients** that emails and texts will be kept along with their other records.

HIPAA and Maintenance of Records

One of the HIPAA Security Rule’s essential requirements is that the **availability** of client information be maintained. In other words, HIPAA requires that client information is not lost and that it remains available to the agency for so long as records need to be kept.

While HIPAA empowers clients to make their own choices regarding privacy (see below), the responsibility to maintain the availability of client information is inherent and cannot be waived by clients.

What Records to Maintain

Ideally, the agency should retain each and every email or text message exchanged regarding a client’s care. Departure from this ideal should be done with caution, since all these communications are protected health information (PHI) under HIPAA and their **availability** must be maintained. HIPAA’s requirement that covered entities maintain the availability of PHI is relatively inflexible and is not impacted by client waivers.

For this reason, this author strongly recommends that services used for email or texting, whether secure or nonsecure, be chosen partly for their ability to indefinitely maintain all messages exchanged. This is one reason why **clinicians and other staff should never use personal services** for texting or email.

Third-Party Services

Unless the agency maintains email servers within its own facilities, all email and texting services are provided by a **third party**. As such, there is a need to ensure that the agency employs third party services in a manner that complies with ethical and legal standards.

Professional Ethics and Third-Party Services

Many ethics codes and guidance documents state that **clients need to be informed** of any third parties that have access to their information.

Beyond that, ethics codes tend not to be explicit about how clinicians are expected to vet third party service providers. However, the codes are clear that the clinician is responsible for the confidentiality of sensitive information and the safety of clients even if a breach of confidentiality or safety is the direct fault of a service provider and not the clinician's direct fault.

As such, it is certainly an ethical necessity to take care in employing third party services to handle client sensitive information. There is little-to-no concrete guidance in ethics codes on how to accomplish this, however.

HIPAA and Third-Party Services

When a third party is employed to "create, receive, maintain, or transmit" sensitive client information, HIPAA requires the agency to execute a HIPAA-compliant **Business Associate Agreement** with the third-party provider. This rule is relatively inflexible, and cannot be waived by clients.

As such, any service that is part of a compliant texting or email solution must execute a HIPAA Business Associate Agreement with the agency. It is the author's opinion that there is no reasonable risk management solution which avoids this requirement.

Business Associate Agreements are contracts. Many large vendors, such as Google, will only execute their own Business Associate contracts.

Using Nonsecure Services to Communicate With Clients

Professional Ethics and Nonsecure Communications

While ethics codes generally call on clinicians to use technical security measures, most especially encryption of messages, they also allow for clients to make autonomous decisions about their own privacy.

For example, it is ethically acceptable for a client to request that their records be released to any entity they would like. It is also acceptable for the client to accept the privacy risks inherent in receiving services while walking around a park or even sitting in a coffee shop.

Unlike HIPAA, however, many mental/behavioral health ethics codes state that clinicians have a **significant responsibility to ensure that clients actually understand the risks** involved in these activities. It is the author's opinion that they *may* also have a responsibility to assess if the client's acceptance of such risks is within the realm of reasonable safety.

HIPAA and Nonsecure Communications

The HIPAA Omnibus Rule clarified, and guidance from the Office of Civil Rights on individuals' right of access to their information further confirmed, that clients possess the autonomy to make decisions about the privacy of electronic transmissions containing their sensitive information.

The clinician or agency has a simple requirement to **inform clients** that third parties may be able to view their information as it passes through the transmission. This threshold of responsibility for informing clients of risks seems to be much lower than that required by professional ethics.

HIPAA does not require any specific form of documentation of the client's acceptance of the risks involved in nonsecure communications. The author strongly advises, however, that agencies obtain written and signed documentation that the client has been informed of risks and still wants their information transmitted via the nonsecure email or texting method they've agreed to use with their clinician.

Conclusions Regarding the Permissibility of Using Email or Texting in Clinical Contexts

It is the author's opinion that agency policy regarding email and texting should, in a contextual vacuum, center around using only a secure messaging app and, when necessary, secure escrow email. The messaging app and the secure escrow email service muse execute HIPAA-compliant Business Associate Agreements with the agency. The agency should also have office policies informing clients about the use of these services and how to use them to reach their clinician. The policy should also define the boundaries described below.

From there, agencies should decide how much they wish to support the use of conventional email or SMS texting when it is requested or appears to be necessary. Support for nonsecure communications services should increase with the need or demand of the client or family member, but should be mediated by an assessment of the risks involved in using nonsecure communications with that particular client.

Consideration as Telehealth Practice

The use of texting and email to communicate with clients and families could, depending on a variety of difficult-to-pin-down factors, be regarded as telehealth practice.

It is difficult to identify any particular authority which helps us to draw a line between which communications are part of healthcare and which are simply the management of administrative and other logistical matters.

It is also not specifically clear what must be done if a clinician's activity around email and texting does constitute telehealth services. There is certainly the question of the clinician's competence in using the email and/or texting medium for this purpose. There is also the question of whether or not the clinician and the agency are meeting standards of care surrounding telehealth. Discussion of those standards is outside the scope of this document, however.

This section does not offer any solutions to this potential problem. It is simply included to ensure that readers do not overlook this potential issue.

Vendor Selection: Telecommunications Services

Any email, SMS, or messaging app service would be a "telecommunications service" as we are talking about them here.

When choosing services, whether it is conventional email, secure escrow email, SMS texting, or a messaging app, the service must include at least these things:

- The vendor must execute a HIPAA-compliant Business Associate Agreement with the agency.
- The service must retain each and every message exchanged through it and make those messages available to authorized agency staff members.

Some examples of services who can do **both** conventional email and secure escrow email, who will execute BAAs, and who can be configured to retain any and all messages exchanged through them include:

- Google GSuite Gmail
- Hushmail
- LuxSci
- Microsoft 365 Outlook
- Many patient portals
- Many, many others. Person Centered Tech has a list of reviews here: https://personcenteredtech.com/pct_vendorreview_tag/secure-email/

Some examples of services which can provide SMS texting, who will execute BAAs, and who can be configured to retain any and all messages exchanged through them include:

- All Call Technologies
- Google Gsuite Google Voice (caution: the Google Voice included with free Gmail accounts is a different service)
- iPlum
- RingRx
- Spruce Health
- Many, many others. Person Centered Tech has a list of reviews here: https://personcenteredtech.com/pct_vendorreview_tag/voip/

Some examples of secure messaging app services who will execute BAAs and who can be configured to retain any and all messages exchanged through them include:

- Spruce Health
- OhMD
- TigerText's TigerConnect
- Some patient portal apps
- Many, many others. Person Centered Tech has a list of reviews here: https://personcenteredtech.com/pct_vendorreview_tag/secure-texting/

Setting Up For Success With Clients

Setting and Maintaining Effective Boundaries

Quick communication using mobile devices is great, but it can have clinical downsides. It is important that the agency develop internal policies to address how best to approach at least the following issues that arise when using email and texting with clients and their families.

Depending on the clinical modality being used, frequent clinical exchanges between clinician and client or family may be regarded as enabling of poor boundaries, it may be regarded as necessary for the client's ongoing treatment, or it may be something in-between.

There is also ostensibly a difference between messages regarding administrative/logistical issues and messages of a therapeutic or psychoeducational nature. Logistical messages may be closer to neutral in terms of impact on therapeutic boundaries, but that is not always true.

The agency's desire for email or texting may be limited to just administrative/logistical issues. Or it may be limited to a desire to facilitate crisis communication between clients and their clinicians.

The agency should analyze these points with regards to its population and make decisions about what kinds of messages and frequency are likely to support the clinical mission and what might interfere with it. Developing written guidelines and policies for clinical staff around this issue is important. They should address at least these questions:

- What is the purpose of using email with clients or families?

- What is the purpose of using texting with clients or families?
- How does the purpose of each medium indicate how frequently the agency wishes to use it with clients or families?
- How does the purpose of each medium indicate what forms of communications it should be used for? Appointment changes only? Low-intensity check-ins? Doing clinical homework? Crisis management?
- How does the purpose of each medium impact the turnaround time that clinicians or agency staff should promise for responding to messages from clients or families?

Communications Policies for Clients

Office policies for clients can help set them up early to know what the best ways to use email and texting are, and to give them guidance on how to use them appropriately. It is recommended that these policies address at least the following:

- An explanation of what services will be used and, if applicable, how to ask about alternative (usually nonsecure) services.
- How the client can acquire any necessary apps and/or connect with their therapist.
    - E.g. include email addresses to send emails to, phone numbers to text, instructions for registering with an app, etc.
- The official turnaround time for when messages will be returned.
    - Remember that clinicians and staff should probably not guarantee the same turnaround time that they would give to their own friends and family. E.g. even for text messages, the agency should consider listing an official turnaround time of at least 1 business day -- unless the agency's mission dictates otherwise.
- What kinds of content to use each service for.
    - For some agencies, it may be useful to list if one medium is intended only for administrative issues like appointment changes. Clinicians should probably speak to clients and families directly about guidance regarding email and texting for clinical purposes.

Fostering Client Collaboration

It is probably apparent at this point that with email and texting, there is a balance to be struck between security and convenience. Secure messaging apps may strike the most convenient balance, but only if clients and families are on board with using them.

Clients often want to use conventional email because they want to have a record of messages that stays within their favorite, trusted email service. They may want to use SMS (or iMessage) for the same reason. While there are compliant solutions for accommodating these desires, it is not recommended that you do so unless there is no other option.

Here are some techniques that sometimes work for encouraging clients who possess smartphones to engage in the use of secure services instead of their favored nonsecure ones:

- Present the agency's preferred, secure solution as "the way we do it." Rather than present it as *an* option, present it as *the* option.
- Prepare all staff at the agency to present a positive attitude towards the secure solution. The next point can help with this one.
- Make sure clinicians are confidently competent at using the secure solution. This helps ensure that the clinicians themselves do not present barriers to the client's adoption of the desired solution. It may be necessary to spend some significant time practicing with new tools.
- Don't hesitate to help clients and families get set up with the secure solution. If it is a messaging app, clinicians or staff may help the client download and install it.

Some Compliant Solution Recipes

Here are some concrete examples for applying the guidance provided above. The whole set of possible compliant solutions are not limited to these recipes, however!

1) An agency that works with very low SES populations who need frequent connection and who are supplied with free classic cellular phones and basic phone service.

Tech Choices:

- Clinicians' personal smartphones which have been registered with IT services.
- RingRx phone service, used through an app on the clinician's smartphone, with the SMS texting activated. RingRx executes a BAA with the agency and retains all messages exchanged.

The most relevant policies:

- A case worker or clinician interviews the client to determine if there are any particular risks in their life that might contraindicate the use of texting for clinical work. If the risks appear unacceptable, texting is not used with this client.
- The case worker or clinician makes sure the client understands how using texting may create confidentiality risks, and gets a signed document indicating that the risks are understood and that the client accepts them. If the client does not wish to accept the risks, texting is not used with this client.
- The client is supplied with the office policy on using text messaging to keep up contact as needed. As they work together, the case worker or clinician reminds them of the policy as needed.

2) An agency that works with adolescents from a variety of SES backgrounds and who need frequent connection with a clinician

Tech Choices:

- Clinicians' personal smartphones which have been registered with IT services.

- Google GSuite Gmail for email. GSuite provides a BAA and retains all messages.
- Google GSuite's managed version of Google Voice for phone and SMS. GSuite provides a BAA and retains all SMS messages as well as a log of calls.
- OhMD for secure texting. OhMD provides a BAA and retains all messages exchanged.

The most relevant policies:

- A staff member or clinician provides the office policy on communications and offers to help the client and any interested family members setup OhMD on a smartphone. It is pointed out that communications should all be done via telephone or OhMD.
- If there is a desire to use email (most likely from guardians), risks are explained to the interested party and they sign a document indicating that the risks are understood and that the client and/or guardian accepts them. They are supplied with information about what email address(es) to use and how to appropriately use email with the staff and/or clinician.
- If the client (or, in some cases, a family member) does not own a smartphone, but does own a classic cellular phone:
    - The staff member or clinician interviews the client to determine if there are any particular risks in their life that might contraindicate the use of texting for clinical work. If the risks appear unacceptable, texting is not used with this client.
    - The staff member or clinician makes sure the client and their authorized guardian understand how using texting may create confidentiality risks, and gets a signed document from both of them indicating that the risks are understood and that the client and the guardian accept them. If the client or guardian do not wish to accept the risks, texting is not used with this client.
    - The client is supplied with the office policy on using text messaging to keep up contact as needed. As they work together, the clinician reminds them of the policy as needed.

References

- American Association of Marriage and Family Therapists. (2015). Code of Ethics . Alexandria, VA: Author.
- American Counseling Association. (2014). Code of Ethics . Alexandria, VA: Author.
- American Psychological Association. (2010). American Psychological Association Ethical Principles of Psychologists and Code of Conduct . Washington, DC: Author.
- HHS Health Information Privacy Division. (n.d.). Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524. Retrieved June 1, 2019, from http://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/
- National Association of Social Workers. (2008). Code of Ethics . Washington, DC: Author.
- National Board for Certified Counselors. (2016). Code of Ethics . Greensboro, NC: Author.

- US Dept. of Health and Human Services. (2006). HIPAA Administrative Simplification. Washington, DC: Author.
- US Department of Health and Human Services. (2013). HIPAA Omnibus Final Rule. US Federal Register.

Resources

Sample Communications Policy (attached)

Sample Request for Nonsecure Communications Form (attached)

Email and Texting Risk Questionnaire (attached)

Disclaimer, Terms of Use, and Copyrights

The following document is developed by Person Centered Tech Incorporated and is offered for educational purposes. It is not offered with any intent or implied warranty of fitness for a particular purpose nor is there any warranty, guarantee, or general claim that this will in any way provide any particular level of legal protection.

This document is not a substitute for legal advice or consultation, nor is it a substitute for clinical or ethical consultation or advice. State laws and licensing board rules vary, as do the needs of individual clients. You must modify this document – or rule out its use – as necessary according to your local laws and rules as well as the needs of your clients and your practice.

Unless otherwise prohibited by law, Person Centered Tech Incorporated will not be liable to you or to any other third party for: (a) any direct, indirect, incidental, special, punitive, or consequential losses or damages, including, but not limited to, loss of profits, loss of earnings, loss of business opportunities, or personal injuries resulting directly or indirectly from use of this document; or (b) any losses, claims, damages, expenses, liabilities, or costs (including legal fees) resulting directly or indirectly from use of this document. The conditions in this paragraph apply to any acts, omissions, and negligence of Person Centered Tech Incorporated that would give rise to a course of legal action. You agree to indemnify and hold harmless Person Centered Tech Incorporated against all claims and expenses (including attorney fees) arising from the use of this document.

This document is provided "as is." Person Centered Tech Incorporated grants you right to use this document in your own health care practice. Your right to use this document is non-exclusive and may not be transferred to others. You may copy or modify this document according to your individual business needs, but you may not distribute copies of this document nor may you distribute documents derived from this one. You are also prohibited from using this document for educational purposes without prior written consent.

Your use of this document is also covered by Person Centered Tech's Terms of Service.

Email/Portal Messaging Solution Worksheet

Effective Date:

Authorized By:
Date Authorized:

Technology Choices

Service Provider(s):	● Conventional Email (if any): ○ BAA/Other Effective Date(s): ● Escrow/Forced TLS Email (if any): ○ BAA/Other Effective Date(s):
Clinician Device(s): *Choose all that apply*	● Smartphones: ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:) ● Tablets ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:) ● Computers: ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:)

Communications Policies

How We Use Email

- Clients should use the following method to email the agency staff and/or their clinician(s): ____________
- Clients are informed of how the emails exchanged with agency staff may be viewed by 3rd parties.

Email Contents

Depending on your choices, you may need to consider how the communications policy is impacted by telehealth laws and standards in your region.

- What we talk about. (Choose and Adapt One):
    - Email is strictly limited to scheduling and other administrative matters.
    - Email is mostly limited to scheduling and other administrative matters, but may also be used for treatment logistics like sending treatment plans, medication information, and similar communications.
    - Email may be used for a broad range of purposes including clinical check-ins, journaling, or other matters. Clients and clinicians will communicate regularly about how the use of email to talk about these matters is working for the relationship.

Email Timing

- Clinicians will respond to emails during these times: ____________________
- Clinicians will respond to emails from clients within the following timeframe: ___________ *(suggestion: list your turnaround time in business days.)*
    - It can be useful to note the following in the actual policy document: “Your clinician may sometimes respond more quickly than this, but please remember that this does not mean your clinician will always respond that quickly.”

Emergencies

- Clients are directed to use the following contact method during emergencies: __________

Record-Keeping

- Clients are informed that all emails exchanged regarding their care are part of their medical record.

Security & Privacy Policies

Technology Choices

- What services are permitted for email. (Choose and Adapt One):
    - Only the above-described escrow or forced TLS (“secure”) email services, which meet technical security standards, may be used by agency staff to communicate with clients and collaterals.
    - Secure email methods are preferred, but clients may request nonsecure email and a collaborative risk analysis will be performed to determine if privacy risks are acceptable to the client and if it can be safe for them. Agency staff may only use the email services described above to communicate with clients and collaterals.
    - Secure email methods are not available. Clients are offered nonsecure email and a collaborative risk analysis will be performed to determine if privacy risks are acceptable to the client and if it can be safe for them. Agency staff may only use the email services described above to communicate with clients and collaterals.

- Clinicians must only use approved devices when using agency email.
- Clinicians must follow other agency security policies, such as password policies.

Record Retention and Access

- The agency's email services retain emails in this way and for this long: _________________
- Appropriate agency administrators are able to access all emails ever exchanged by doing this: ________________
- When staff members leave the agency, this is how the agency ensures their emails remain in the agency's possession and are accessible by administrators: ____________

Texting Solution Worksheet

Effective Date:

Authorized By:
Date Authorized:

Technology Choices

Service Provider(s):	● SMS (if used): ○ BAA/Other Effective Date(s): ○ Classic Phone Company. Foregoing BAA. ● Secure Messaging App (if used): ○ BAA/Other Effective Date(s):
Clinician Device(s): *Choose all that apply*	● Smartphones: ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:) ● Tablets ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:) ● Computers: ○ Not Permitted ○ Agency-Supplied (describe:) ○ Personal ○ Hardening procedure (describe:) ○ Secure handling and use policies (describe:)

Communications Policies

How We Use Texting

- Clients should use the following method to text the agency staff and/or their clinician(s): ______________
- Clients are informed of how the texts exchanged with agency staff may be viewed by 3rd parties.

Texting Contents

Depending on your choices, you may need to consider how the communications policy is impacted by telehealth laws and standards in your region.

- What we talk about. (Choose and Adapt One):
    - Texting is strictly limited to scheduling and other administrative matters.
    - Texting is mostly limited to scheduling and other administrative matters, but may also be used for treatment logistics like sending treatment plans, medication information, and similar communications.
    - Texting may be used for a broad range of purposes including clinical check-ins, journaling, or other matters. Clients and clinicians will communicate regularly about how the use of texting to talk about these matters is working for the relationship.
- Sending files/documents. (Choose and Adapt One):
    - Texting should not used to send files or documents.
    - Texting may be used to send these kinds of files or documents: ___________
    - Texting may be used to send any kind of file or document wished.

Email Timing

- Clinicians will respond to texts during these times: _____________________
- Clinicians will respond to texts from clients within the following timeframe: ___________ *(suggestion: list your turnaround time in business days.)*
    - It can be useful to note the following in the actual policy document: “Your clinician may sometimes respond more quickly than this, but please remember that this does not mean your clinician will always respond that quickly.”

Emergencies

- Clients are directed to use the following contact method during emergencies: __________

Record-Keeping

- Clients are informed that all texts exchanged regarding their care are part of their medical record.

Security & Privacy Policies

Technology Choices

- What services are permitted for texting. (Choose and Adapt One):
    - Only the above-described secure messaging apps, which meet technical security standards, may be used by agency staff to communicate with clients and collaterals.
    - Secure messaging apps are preferred, but clients may request SMS texting and a collaborative risk analysis will be performed to determine if privacy risks are acceptable to the client and if it can be safe for them. Agency staff may only use the SMS service(s) described above to communicate with clients and collaterals.

    - Secure texting is not available. Clients are offered SMS texting and a collaborative risk analysis will be performed to determine if privacy risks are acceptable to the client and if it can be safe for them. Agency staff may only use the SMS service(s) described above to communicate with clients and collaterals.
- Clinicians must only use approved devices when texting with clients.
- Clinicians must follow other agency security policies, such as password policies.

Record Retention and Access

- The agency's texting services retain texts in this way and for this long: ________________
- Appropriate agency administrators are able to access all texts ever exchanged by doing this: ________________
- When staff members leave the agency, this is how the agency ensures their texts remain in the agency's possession and are accessible by administrators: ____________

REQUEST FOR TRANSMISSION OF PROTECTED HEALTH INFORMATION BY NON-SECURE MEANS

I, ___________________________________ AUTHORIZE: ______________________________
(name of client) (name of clinician)

____
(street address)

____

TO TRANSMIT TO ME BY NON-SECURE MEDIA THE FOLLOWING TYPES OF PROTECTED HEALTH INFORMATION RELATED TO MY HEALTH RECORDS AND HEALTH CARE TREATMENT:

- Information related to the scheduling of meetings or other appointments
- Information related to billing and payment (but not to include any financial or claims-related identifiers including, but not limited to, credit card numbers, insurance plan numbers, diagnosis codes, or procedure codes.)
- *If you judge it to be appropriate, add more items here*

<u>TERMINATION</u>

○ This authorization will terminate _____ days after the date listed below.

OR

○ This authorization will terminate when the following event occurs: ______________________________.

I have been informed of the risks, including but not limited to my confidentiality in treatment, of transmitting my protected health information by unsecured means. I understand that I am not required to sign this agreement in order to receive treatment. I also understand that I may terminate this authorization at any time.

OPTIONAL, BUT STRONGLY RECOMMENDED:
I understand that *[THERAPIST'S NAME]* makes available to me the following means of communication that are designed to be secure and to maintain confidentiality, and I still choose to request and authorize the above-named non-secure means:

- *Method 1 (e.g. encrypted email)*
- *Method 2 (e.g. secure texting apps for smartphones)*
- *Etc.*

___________________________________ __________________
(Signature of client) Date

Contacting Me

When you need to contact *[Therapist Name]* for any reason, these are the most effective ways to get in touch in a reasonable amount of time:
The following are examples. Choose, remove and add items appropriate for your practice

- By phone (555-867-5309.) You may leave messages on the voicemail, which is confidential.
- By secure text message (see below for details.)
- By secure email (see below for details.)
- By the secure contact page on the website (www.example.com/contact).
- If you wish to communicate with me by normal email or normal text message, please inquire about the potential confidentiality risks of doing so.
  OR
- If you wish to communicate with me by normal email or normal text message, please read and complete the Consent For Non-Secure Communications form included with these office policies.

If you have secure communications tools available, include this optional paragraph.
I subscribe to the following service(s) that can allow us to communicate more privately through the use of encryption and other privacy technologies. None of them will cost you money, but each requires some setup before they can be used. Please ask if you would like to use any of these services:
The following are examples. Choose, remove and add items depending on what you have available.

- Encrypted email.
- Secure text messaging. This service can be used on a computer or smartphone.
- A secure contact page on my website. You can type and send encrypted messages through this page. (www.example.com/contact)
- A secure "client portal," where we can exchange private messages via a secured website.
- Secure online video chat software.

If you need to send a file such as a PDF or other digital document, *[describe how the client should send digital files. E.g. "please send using the secure email service," "please send via the secure contact form on the website", "please print and FAX it to 555-867-5309," etc.]*

Please refrain from making contact with me using social media messaging systems such as Facebook Messenger or Twitter. These methods have very poor security and I am not prepared to watch them closely for important messages from clients.

It is important that we be able to communicate and also keep the confidential space that is vital to therapy. Please speak with me about any concerns you have regarding my preferred communication methods.

Response Time

I may not be able to respond to your messages and calls immediately. For voicemails and other messages, you can expect a response within *[list your response time for messages]* (weekends are excepted from this timeframe.) I may occasionally reply more quickly than that or on weekends, but please be aware that this will not always be possible.

Be aware that there may be times when I am unable to receive or respond to messages, such as when out of cellular range or out of town.

Emergency Contact

If you are ever experiencing an emergency, including a mental health crisis, please call *[name and contact information for crisis services.]*

If you need to contact me about an emergency, the best method is:
The following are examples. Choose, remove and add items appropriate for your practice

- By phone (555-867-5309.)
- If you cannot reach me by phone, please leave a voicemail and then follow up with a secure text message.

Your Records

Please know that all of our communications, including text messages and emails, are part of your medical record.

Disclosure Regarding Third-Party Access to Communications

Please know that if we use electronic communications methods, such as email, texting, online video, and possibly others, there are various technicians and administrators who maintain these services and may have access to the content of those communications. In some cases, these accesses are more likely than in others.

Of special consideration are work email addresses. If you use your work email to communicate with me, your employer may access our email communications. There may be similar issues involved in school email or other email accounts associated with organizations that you are affiliated with. Additionally, people with access to your computer, mobile phone, and/or other devices may also have access to your email and/or text messages. Please take a moment to contemplate the risks involved if any of these persons were to access the messages we exchange with each other.

Using This Document

This questionnaire is written as if it is something for the client to read on his/her own. However, remember that the purpose of it is to supply a jumping off point for you, the therapist, to meet the threshold set by the 2014 ACA Code of Ethics for informing clients of risks involved in the use of digital and networked communications technology. So you can use this questionnaire to help you structure a discussion with clients, you can give it to clients to help them think about the risks involved before they discuss them with you, or for whatever purposes you judge it helpful for you to meet your requirements

The final purpose of such a discussion would be to:

a) Help clients determine if the risks involved in email and/or texting are acceptable to them **and/or**

b) Help clients and you find what needs to be done to reduce the risks to reasonable levels. E.g. the client may limit what kinds of communications are acceptable, may choose to use a different email address, etc.

Do keep in mind that this document alone will not be sufficient to meet your needs. You also need to consider state laws, licensing board rules, and other sources of regulation or guidance regarding the use of email, texting, and electronic transmissions in general with clients.

Email and Texting Risk Questionnaire

Regarding Email

1. Technical experts often describe email as being like a postcard, in that it can be viewed by all hands it passes through. Are you familiar with the risks of emails being viewed by various engineers, administrators, and bad actors as it passes through the Internet?
2. Think about where you read and write emails, and what devices you do that on. Think about who can see you reading and writing emails in these places, and who can access the devices you use to read and write emails. Would there be any negative consequences to any of those people reading or glancing at emails exchanged with your therapist? Are there certain kinds of email contents that you would feel safe letting these people see and other kinds of contents you would not feel safe letting them see? Let your therapist know the answers to these questions if you wish to use email with him or her.
3. Think about which email address(es) you might use with your therapist. Who has access to each address? If you use a work email address, know that your employer may legally view all the emails your send receive with that address. Be aware that engineers and administrators at your email service provider may be able to view your emails.
4. How quickly do you normally receive replies from others via email? Do you expect replies more quickly than your therapist's stated response time? Can you see any negative consequences occurring if your therapist does not or cannot reply to an email as quickly as others in your life typically do?

Your therapist's email service is through this company: *[Name of Email Service.] Note that if you have a complex email setup, such as if you have email forwarding services from your website hosting provider, it would be wise to describe all the companies/groups involved in that setup.*

Regarding Texting

1. Text messages are often sent using the Internet, even though they are usually a part of one's phone service. Are you familiar with the risks of texts being viewed by various engineers, administrators, and bad actors as it passes through the Internet?
2. Are you aware that text messages wait on phone company computers until they are retrieved, and may remain there indefinitely? Can you imagine any negative consequences if engineers, administrators, or law enforcement personnel viewed these stored texts from or to your therapist?
3. Think about where you read and write text messages, and what devices you do that on. Think about who can see you reading and writing texts in these places, and who can access the devices you use to read and write texts. Would there be any negative consequences to any of those people reading or glancing at texts exchanged with your therapist? Are there certain kinds of text contents that you would feel safe letting these people see and other kinds of contents you would not feel safe letting

them see? Let your therapist know the answers to these questions if you wish to use texting with him or her.

4. How quickly do you normally receive replies from others via text? Do you expect replies more quickly than your therapist's stated response time? Can you see any negative consequences occurring if your therapist does not or cannot reply to a text as quickly as others in your life typically do?

Your therapist uses the following device(s) and phone service(s) to send and receive text messages: *Describe the phone and/or other devices you use for texting, and who your phone carrier is.*

Note that there are some interesting effects depending on what devices you and clients use. For example, if your client and you both use iPhones, then your text messages may not be typical SMS text messages. Instead, your messages may be iMessage chat messages. On iPhones, iMessage chats are colored blue, while classic SMS text messages are colored green.