

**Telehealth:
Competency for
LEPs and Other
Healthcare Providers**

Written and presented by Dr. Gina Beaman, Psy.D.

1

About the Presenter

Dr. Gina Beaman

- Psy.D. in Educational Psychology
- Credentialed School Psychologist (PPSC)
- Licensed Educational Psychologist (LEP # 3286)
- Licensed Marriage and Family Therapy (LMFT # 36139)
- Certified Learning Disability Specialist for the California Community Colleges (LD Specialist)
- CASP Ethics Specialist
- Co-Chair, APA Division 16 Ethics Committee

2

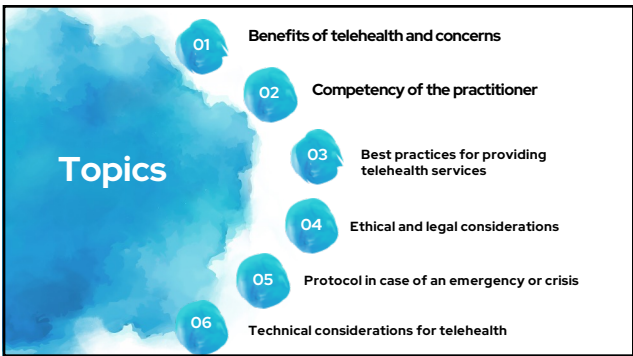
Disclaimer

- Any information provided in this presentation is not regarded as legal advice. This presentation is for informational purposes.
- I am not an attorney
- Always consult with legal counsel.
- In addition to these ethical standards, there is the ever-present necessity to differentiate legal mandates and ethical responsibility. The LEP is urged to become familiar with applicable legal requirements and standards and monitor all changes (CASP Code of Ethics for LEPs, 2015).

3

AB 1759 (Chapter 520, Statutes of 2022).
Under this new law, effective July 1, 2023, the BBS will begin requiring both applicants for licensure and licensees to have completed a minimum of three hours of training or coursework in the provision of mental health services via telehealth, which must include law and ethics related to telehealth.

4



5

What You Will Learn:

- How telehealth can help improve access to care, reduce barriers to treatment, and increase patient engagement.
- Best practices for providing telehealth services, such as using secure platforms, maintaining confidentiality, and ensuring proper documentation.
- Ethical and legal considerations of providing telehealth services, such as licensure, informed consent, and HIPAA and CMIA compliance.
- The steps that healthcare providers can take in the event of a crisis during a telehealth session.
- The technical considerations for telehealth, such as internet speed and bandwidth, and equipment requirements.

6

Telehealth... What is it?



"A mode of delivering health care services using information and communication technologies to facilitate the diagnosis, consultation, treatment, education, care management, and self-management of a patient's health care."

This is while the patient is at the originating site and the health care provider is at a distant site.

Business and Professions Code Section 2290.5(2),(4), & (6)

7

Types of Telehealth

Video synchronous interaction	Audio-only synchronous interaction	Asynchronous
Interactive video communications. The provider and client interactions occur in real-time and is most similar to face-to-face treatment. This is the most common type of telehealth.	Interactive audio only communications. The provider and client interactions occur in real-time via audio-only synchronous telehealth (i.e., over the phone).	Asynchronous communication is any communication that does not take place in real-time. This is often used in an intake or follow-up care. Asynchronous interactions include emails, text, faxes, apps, and online programs.

8

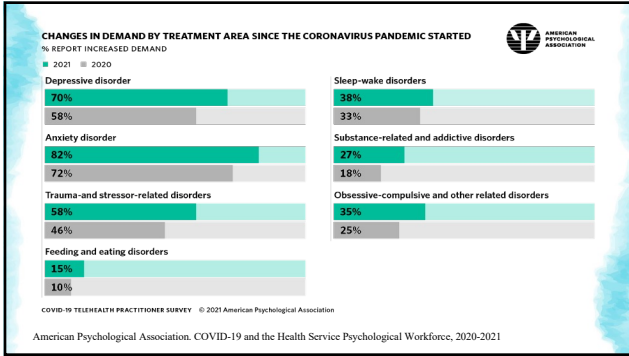
Adaptation is Key: The Importance of Telehealth to Mental Healthcare Providers

There are certain trends in society that are undeniably here to stay. Telehealth is but one that has become an integral part of our society.

In 2021, a survey conducted by the APA revealed that 96% of psychologists provided remote treatment to their patients. Only a few professionals reverted to in-person appointments entirely, while approximately 50% employed a hybrid approach to seeing clients.
(APA 2021 COVID-19 Practitioner Impact Survey).

According to that same survey, referrals for treatment went up 62% (APA 2021 COVID-19 Practitioner Impact Survey). The demand for mental treatment is rising, which requires mental healthcare providers to be available in multiple locations simultaneously. Telehealth enables providers to extend their services beyond the boundaries of an office setting.

9



10

"Achieving the promise and avoiding the pitfalls of electronically mediated care is not the responsibility of individual physicians alone. It requires coordinated effort across the profession, active engagement of specialty and professional organizations not only in medicine but also information technologies, and appropriate education and support for practicing clinicians"

(Chaet et al., 2017, p. 1139).

11


01

Benefits of Telehealth

Where there are benefits, there are also concerns

12

Benefits of Telehealth



Improved access to care:

- Allows us to provide services to clients who may not be able to travel to our office due to distance, transportation, or mobility issues.
- Can help increase access to care for underserved or rural populations.

Reduced barriers to treatment:

- Can help reduce the stigma associated with seeking mental health treatment or services as clients can receive care in the comfort and privacy of their own homes.
- Can be especially beneficial for children or adolescents who may feel more comfortable talking to a mental health care provider in a familiar environment.

13

Benefits Of Telehealth



Flexibility and convenience:

- Allows psychologists to provide services from anywhere with an internet connection.
- Can help reduce the need for in-person appointments, which can be time-consuming and costly for both the psychologist and client.

Enhanced collaboration:

- Telehealth can also help facilitate collaboration between LEPs and other healthcare providers, such as primary care physicians or school counselors.
- This can help ensure that clients receive coordinated and comprehensive care.

14

Benefits Of Telehealth

Increased client engagement and participation in treatment:

- By providing care in a more convenient and accessible format, patients may be more likely to attend appointments and follow through with treatment recommendations.

15

Concerns

NASP points out a number of concerns with the utilization of Telehealth/ Tele-Assessments:

- Privacy and confidentiality
- Inadequate training of the provider and support aides
- Reliability and validity of assessment results
- Test integrity
- Fit of service
- Storage and sharing of data

Adapted from NASP Guidance of Delivery of School Psychological Telehealth Services (2017)

16

Additional Concerns

- Technology barriers (aka: the great divide)
- Ethical considerations
- Establishing trust with client

17


02

Competency

Using Telehealth

18

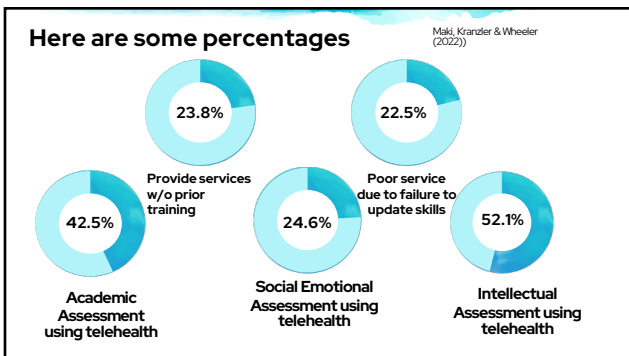
Confidence and Competence



- Differences between face to face and telehealth
- Methods for tailoring assessments and interventions
- Law and Ethics
- Safety

Perle, J. G., Perle, A. R., Scarisbrick, D. M., & Mahoney, J. J., 3rd (2022).

19



20

Competency in Telehealth

Psychologists have an ethical obligation to provide services only within the boundaries of their competence (Standard 2 Competence (2.01), APA, 2017); however, there is flexibility, especially in emergency situations to extend beyond those boundaries for a limited time (Standard 2 Competence (2.02), APA, 2017). That said, psychologists are encouraged to take reasonable steps and responsibility to ensure their competence in technology does not negatively impact clients and cause harm.

Chenneville, T., & Schwartz-Mette, R. (2020)

21

CASP and NASP

- > Under Professional Competency, CASP notes that psychologists offer services within their area of training and experience, accurately represent their competency levels to service recipients, and correct any misperceptions (CASP COE LEP (1) (A) (1) & (2), 2015).
- > According to NASP, virtual service delivery requires close adherence to ethical standards. School psychologists need to maintain and enhance their level of understanding of the concepts related to the delivery of services via telehealth technologies. The same ethical and professional standards should apply to telehealth services as to the in-person delivery of school psychological services. (Adapted from NASP Guidance of Delivery of School Psychological Telehealth Services (2017))

22

03

Best Practices for Telehealth

Guidelines for conducting telehealth sessions

23

Business and Professions Code (BPC) 1815.5. Standards of Practice for Telehealth.

- (a) If the client is located in California, the treating practitioner must have a California license
 - (a) Services offered via Telehealth are still subject to all the laws and regulations as face-to-face services.
 - (a) Actions a practitioner must complete upon initiating telehealth services:
 - (1) Obtain informed consent from the client and document it. This is consistent with BPC Section 2290.5. (same as face-to-face).
 - (2) Inform the client of the potential risks, limitations, and benefits of receiving treatment via telehealth.
 - (3) Ensure the client is provided with the practitioner's license or registration number and the type of license or registration.
 - (4) Ensure and document that the client has contact information of relevant resources, including emergency services and procedures nearest the client.
- <http://next.westlaw.com/> California code of regulation

24

Business and Professions Code (BPC) 1815.5. Standards of Practice for Telehealth continued

(d) Actions a practitioner must complete at the beginning of each and every telehealth session:

- (1) Verbally obtain from the client and document the client's full name and address of present location.
- (2) Assess whether the client is appropriate for telehealth.
- (3) Utilize industry best practices for telehealth to ensure client confidentiality and the security of the communication medium, i.e., video and/ or audio connection.

(e) A BBS licensee of California can provide telehealth services to client in another state only if the California licensee meets the requirements of the state the client is located and is allowed to practice via telehealth. This does not apply to LEPs as this license is not portable.

(f) Failure to comply with any provision of this regulation is considered unprofessional conduct.

<http://next.westlaw.com/> California code of regulation

25

Best Practices for Service Delivery of Telehealth

Guidelines for telehealth Considerations

3.04 Avoiding Harm
 (a) Psychologists take reasonable steps to avoid harming their client/patients, students, supervisees, research participants, organizational clients, and others, with whom they work, and to minimize harm where it is foreseeable and unavoidable (APA Code of Conduct, 2016a).

26

Best Practices for Delivery of Telehealth Services

Telehealth best practices through the lens of APA's (2016a) general principles C, D, & E:

As professionals, psychologists have a responsibility to uphold the dignity and value of every individual. Precautionary measures should always be taken to ensure that the services they provide are accurate, honest, and truthful, so as to not misrepresent the services they are providing. Psychologists must also acknowledge that fairness and justice are basic human rights that should be afforded to everyone, regardless of cultural, individual, or role differences. Additionally, psychologists should take into account factors such as disability, language, and socioeconomic status to avoid any unjust practices.

27

We Must Consider...

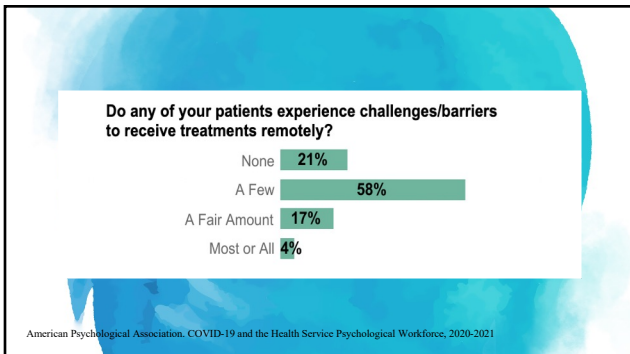
Client's preferred modality of service

- Is telehealth the clients preferred modality of service?
- If it is not, you must offer the same type of service through in-person visits

Transparency of potential risks and benefits

- Educate clients on telehealth services' potential risks and benefits.
- Educate clients on how to ensure their privacy and security during the telehealth session.
- Educate clients on how to use the telehealth platform effectively.

28



29

We Must Consider...

Diverse groups—multicultural, BIPOC, marginalized populations and special needs populations.

- Assess the clients' digital knowledge and fluency in the use and navigation of telehealth and technological communications.
- Assess the clients' access to appropriate equipment and adequate bandwidth, as many marginalized communities are structured to have limited access to appropriate technological communications as a result of structural inequities.

(Gergen Barnett, K., Mishuris, R.G., Williams, C.T. et al., 2022)

30



31

We Must Also Consider...

Fit of service

- Conduct an initial assessment to clarify if telehealth is an appropriate modality for the client.
- During every session, assess for mental status and stability.
- Look for engagement levels, any significant medical or mental health issues that may rise to the level of a crisis, and if so, are the interventions appropriate for a telehealth session?
- If conducting a psychoeducational assessment, is the client old enough and are they mentally able to participate in the testing without parent intervention?
- Do you need a trained paraprofessional to help the client?

32



33

Reciprocit

y The credentialing of school psychologists is regulated by individual states and official reciprocity between states does not exist. However, some states have alternate processes for credentialing incoming professionals with credentials from another state. Maintaining the NCSP credential often helps improve the ease of professional transition across states.

- > The National Association of School Psychologists (NASP) offers a Nationally Certified School Psychologist (NCSP). This is a non-practice credential, meaning that it does not, in itself, permit you to practice school psychology in any state. However, by carrying the NCSP you demonstrate that you meet the NASP standards for graduate preparation of school psychologists and for continuing education. Most states recognize the NCSP as part of their credentialing regulations and offer a more efficient path to state licensure or certification for those applicants that have their NCSP.

(<https://www.nasponline.org/standards-and-certification/school-psychology-credentialing-resources/state-credentialing-faqs>)

34

Portability

- > The BBS implemented Senate Bill 679 (SB 679) as of January 1, 2020. This bill focuses on the ability of licensed therapists and counselors to easily move or carry their license from California to another state. This bill is for LMFT, LCSW, and LPCC licenses ONLY. (BBS Memo, 10/13/2020)
- > SB 679 did not establish a license portability, or "licensure by credential" option for LEPs, because not many other states license them. The only other state found that issues an LEP license is Massachusetts. Therefore the LEP does not lend itself the portability as the other three licenses. (BBS Memo, 10/13/2020)

35

Contracting with Online Therapy Companies

The Board of Behavioral Sciences (BBS) recently surveyed clinicians' experiences working with online therapy companies in an Online Only Therapy Platform Survey, between April 10 and May 15, 2023 (BBS Memo, May 25, 2021).

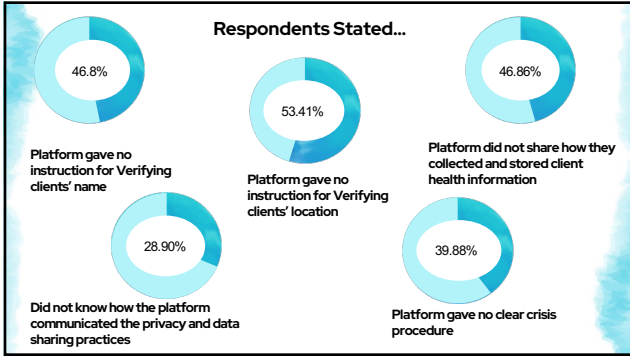
The results showed the following that have important legal and ethical implications:

- > The methods for matching the client with same-state clinicians, verifying clients' identity, location, and the collection, sharing, and storage of PHI were inconsistent or nonexistent.

&

- > Informed consent, privacy and data policies, custodianship of client records, and emergency procedures were not always clearly defined.

36



37

According to the NASP 2020 publication "Consideration for Contract Services in School Psychology," self-employed school psychologists (known as LEPs in California) bear the highest level of liability and responsibility. LEPs are primarily accountable for upholding ethical obligations, not the contracting company.

38

04 Ethical and Legal Considerations

39

Ethical and Legal

Guidelines for conducting telehealth sessions

Use Secure Platforms:

The security of telehealth platforms is essential to ensure the privacy and confidentiality of patient information.

Telehealth platforms should be HIPAA compliant and use secure encryption methods to protect patient data.

Healthcare providers should also use strong passwords and two-factor authentication to prevent unauthorized access to the platform.

40

Ethical and Legal

Guidelines for conducting telehealth sessions

During the COVID-19 shutdown in 2020, providers, many of whom had never before used video conferencing or telehealth, were thrust into the world of telehealth. At that time a COVID-19 Public Health Emergency (PHE) was enforced and the U.S. Department of Health and Human Services (HHS) relaxed their enforcement of the 1996 HIPAA laws and allowed providers to use popular communication apps such as Apple FaceTime, Facebook Messenger Video Chat, Google Hangouts, which is now Google Chat, Zoom, and Skype to name a few.

(Office for Civil Rights (OCR) <https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html>)

41

Fast Forward 3 years...

- On May 11, 2023 the PHE ended as well as many of the flexibilities. This means that HIPAA and HITECH laws are going to be enforced once again.
- The Office of Civil Rights (OCR) is providing a 90-calendar day transition period for covered health care providers to come into compliance with the HIPAA Rules with respect to their provision of telehealth.
- The transition period will be in effect beginning on May 12, 2023 and will expire on August 9, 2023.
- The OCR will continue to exercise its enforcement discretion and will not impose penalties on covered health care providers for noncompliance with the HIPAA Rules that occurs in connection with the good faith provision of telehealth during the 90-calendar day transition period.

<https://www.hhs.gov/about/news/2023/04/11/hhs-office-for-civil-rights-announces-expiration-covid-19-public-health-emergency-hipaa-office-enforcement-discretion.html>

42

Ethical and Legal

Guidelines for conducting telehealth sessions

Maintain Confidentiality:

Confidentiality is an essential aspect of healthcare services, and it becomes even more critical in telehealth services.

Healthcare providers should ensure that patients are in a private and secure location during the telehealth session to prevent unauthorized access to their personal information.

Providers should also avoid using public Wi-Fi or unsecured networks when providing telehealth services.

43

Confidentiality While Using Telehealth Services

Psychologists who provide telehealth services make reasonable efforts to educate, protect, and maintain the security and confidentiality of data and information and dispose of electronic information in ways that decrease the risk of loss of confidentiality through unintended access or disclosure and safe disposal of PHI (The APA Guidelines for the Practice of Telepsychology, 2013).

Be aware of the limitations regarding confidential transmission by Internet or electronic media and take care when transmitting or receiving such information via these mediums (CAMFT Code of Ethics, 6.4, 2019).

Take additional measures store, transfer, transmit, and/or dispose of client/patient records in ways that protect confidentiality (CAMFT Code of Ethics, 2.3, 2019).

44

Ethical and Legal

Guidelines for conducting telehealth sessions

Obtain Informed Consent:

Informed consent is essential in telehealth services like in-person healthcare services.

Obtain written consent from patients before providing telehealth services. Electronic signatures are allowed.

Healthcare providers must also ensure that patients understand the risks and benefits of telehealth services before providing care.

The consent form should provide information on the telehealth platform, potential risks and benefits, and patient rights and responsibilities.

45

Informed Consent for Telehealth...

- Outlines the standards for the client/ clinician relationship and is for their protection.
- Informs the client of the nature and purpose of the services, fees, and limits of confidentiality in clear and concise language (CASP Code of Ethics, LEPs (I) Professional Competency (C)(1).
- Addresses the particular concerns related to services provided via telehealth, such as added risk to confidentiality, security of data using telecommunications technology, and storage of information (The APA Guidelines for the Practice of Telepsychology, 2013)
- Informs the client in writing all possible rewards and risks despite age and ability to give informed consent (APA Ethics Code, Standard 3.10(a)(b))
- Consent must be appropriately documented whether it was verbal or written that telehealth is an acceptable mode of delivering health care services (APA Ethics Code, Standard 3.10(d)) (Business and Professions Code section 2290.5 (b)).

46

Ethical and Legal

Ensure Proper Documentation

Documentation is essential in healthcare services, and it becomes even more critical in telehealth services, especially when documenting electronically.

Healthcare providers should ensure that all telehealth sessions are documented accurately and thoroughly, including checking patient identity for the initial session, patient location every session (if in different location, document emergency services in that area), fit for telehealth modality, the date and time of the session, and the services provided.

The documentation should be stored securely and in compliance with HIPAA regulations.

Guidelines for conducting telehealth sessions

47

Ethical and Legal

Provide Patient Education:

Healthcare providers should provide patients with education on the telehealth platform and how to use it effectively.

Providers should also educate patients on the potential risks and benefits of telehealth services and how to ensure their privacy and security during the telehealth session.

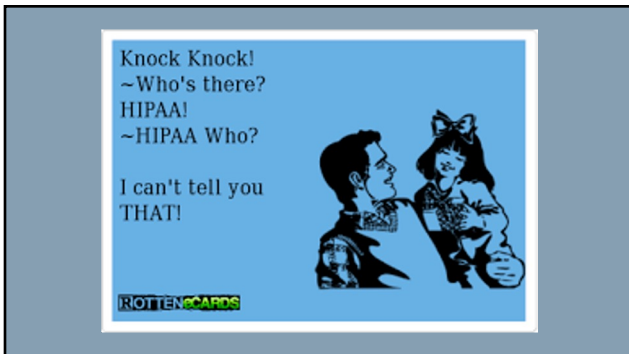
Educating the client on issues on the uniqueness of receiving telehealth services, only advances consumer protection, making for a more educated consumer who is in a better position to determine whether receipt of telehealth is the best fit for them (Board of psychology, Standards of practice for telehealth regulation advisory, accessed 5/25/23)

Guidelines for conducting telehealth sessions

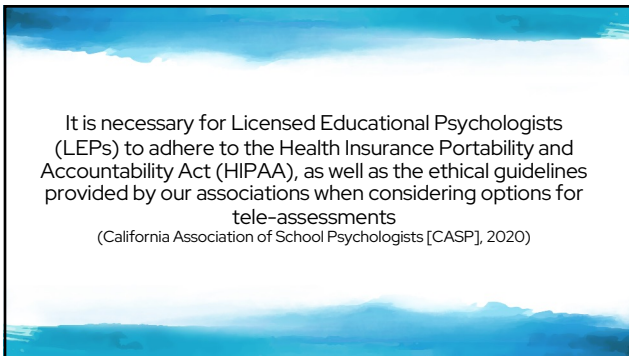
48



49



50



51

Let's Talk About...

PHI Patient Health Information


- HIPAA** Health Insurance Portability and Accountability Act (1996) A federal law
- HITECH** Health Information Technology for Economic and Clinical Health Act (2009) A federal law attached to HIPAA
- CMIA** California Confidentiality of Medical Information Act (2013) A state law

52

HIPAA

HIPAA's Administrative Simplification provisions are set national standards and requirements that actually include 2 components (AKA HIPAA).

Privacy Rule
Covers the protection of privacy and security of individually identifiable health information.




Security Rule
Covers all electronic healthcare transactions that are under the HIPAA rules.

53


HIPAA Privacy Rule:

- Establishes the circumstances under which PHI held by a covered entity can be accessed, used, or disclosed.
- Establishes the circumstances when PHI can and cannot be used or disclosed without patient authorization.
- Grants individuals certain rights to their own health information.



Rights and requirements: A guide to privacy and security of health information in California, 2013

54



➤ Established a national set of standards for the protection of PHI that is created, received, maintained, or transmitted in electronic media by a HIPAA covered entity or a business associate

➤ Protects electronic PHI (ePHI)

➤ Addresses three types of safeguards- administrative, technical, and physical that must be in place to secure an individual's ePHI

HIPAA Security Rule:

Rights and requirements: A guide to privacy and security of health information in California, 2013


55

HITECH	Business Associate
<ul style="list-style-type: none"> ➤ Extended HIPAA coverage to include "business associates" that, on behalf of the covered entity, perform functions or services that include handling of PHI. ➤ Extends to any covered entity that creates, receives, maintains, or transmits PHI on behalf of a covered entity or on behalf of a business associate 	<ul style="list-style-type: none"> ➤ A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information. ➤ A person that offers a personal health record to one or more individuals on behalf of a covered entity. ➤ A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

Rights and requirements: A guide to privacy and security of health information in California, 2013

56

CMIA



➤ The principle California state law addressing the privacy and security of medical information.

➤ Lists permitted uses and disclosures of medical information for entities covered by the law, as HIPAA does.

➤ Extends privacy protections only to identifiable health information, as with HIPAA.

➤ Grants individuals broad general access to their records.

Rights and requirements: A guide to privacy and security of health information in California, 2013

57

HIPAA vs. CMIA

- Are you covered under HIPAA or CMIA?
 - You will have to make that decision (refer to the CAMFT article [Are You a Covered Entity](#) in the resource section of this presentation).
 - Basically, if you transmit health information in electronic form (anything using the internet) in **connection** with covered transactions, you are a covered entity.
- If you are an LEP in private practice, which do you follow?
 - You could be under both
 - But if not under HIPAA, you are definitely under CMIA
 - CMIA is who you are -any health care provider
 - HIPAA is what you do-any health care provider that furnishes, bills, or is paid for health care in a normal course of business or simply saying you follow HIPAA

58

Are You HIPAA Compliant?


There are three main safeguards required to establish and maintain compliance with the HIPAA Security Rule:

Administrative Safeguards (risk prevention): Conduct a risk analysis of HIPAA breaches Establishing policies and procedures for creation, storage, and transfer of PHI	Technical Safeguards: Protect data loss/Unauthorized access Strong passwords Encryption Authentication	Physical Safeguards: Keeping devices secure Restricting who has access
---	---	---

<https://www.cphins.com/your-software-and-devices-are-not-hipaa-compliant/>

59

- **Risk Analysis/Assessments:** help establish policies and procedures so they can be used to evaluate the confidentiality, integrity, and availability of information systems in your practice. This is crucial in establishing other policies, procedures, and mitigation management.
- Action items include:
 - Assigned security responsibility
 - Workforce security
 - Information access management
 - Security awareness and training
 - Security incident procedures
 - Contingency planning



Administrative Safeguards

What's the Risk?

HIPAA Security Series #2 - Administrative Safeguards

60

Technical Safeguards

Technical safeguards generally refer to the security aspects of your information systems, policies and procedures used to protect ePHI and access to it.

- > **Access and Audit Controls:** ensures access is granted to only those who are authorized and provides users with the minimum level of access needed to perform the task at hand.
- > **Types of access controls include:**
 - o Unique user identifier
 - o Emergency access procedures
 - o Automatic logoff
 - o Encryption and decryption
- > **Integrity, Person Authentication, and Transmission Security :**
 - o Ensures protection for ePHI from being altered or destroyed.
 - o Ensures the person who wants access has permission (i.e. PIN, biometrics, smart card, token, or key).
 - o Ensures emails and communications via the internet are not improperly modified or disposed of by using encryption

HIPAA Security Series #4 - Technical Safeguards

61



62

Texts and Email

- > APA, CAMFT, NASP, & CASP all state therapists have the legal and ethical duty to keep and maintain confidentiality and take reasonable steps to ensure the confidentiality and security of PHI.
- > To date, HHS does not distinguish between emailing and texting, meaning the same technical safeguards that are used for your office computer and emailing should also be used for your smartphone and texting.
- > This translate into making a habit of using encrypted emails and texts when communicating any PHI with a potential or (past of present) client.

63

Texts and Email Continued

- > That said, legally, the client has the right to receive PHI in any mode they chose, including accepting the risk of unencrypted email and texts.
- > Clients may initiate communications with a provider using unencrypted email. Although it can be assumed that the client would be ok with this mode of communication and associated risks, you can also assume that they are not aware of the potential risks and need to be educated on those risks in order to make an informed decision (The Office for Civil Rights' guidance can be accessed on the U.S. Department of Health and Human Services, Created 12/15/08).

64

You must carefully study the standards in order to understand the responsibilities associated with your work.... Recognize that an action may be legal but unethical at the same time (Sattler, 2014).

65

Texting Through an Ethical Lens

- > Various codes of ethics are jeopardized with the use of electronic communications, in particular, Principles A & E of the APA Code of Ethics (Lustgarten, 2016).
- > APA Code of Ethics (2017), Principle (A) focuses on causing no harm and (E) focuses on respecting the rights and dignity of your clients, which is the foundation of privacy and confidentiality (Lustgarten, 2016).
- > The potential risks inherent in texting threaten privacy and confidentiality of PHI and may cause harm in certain situations, as intent, meaning, and interpretation can be misleading in texts.
- > Maintaining texting records and disposal of that information must be done in ways that protect privacy and confidentiality. Many of us have phones that automatically back-up data...your texts are also backed-up.

66

Physical Safeguards

These are the physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment from environmental hazards and unauthorized intrusions

Facility Access Controls

- Facility security plan
- Access control and validation measures
- Maintenance records

Workstation and Device Security

- Workstation use
- Workstation security
- Device (stationary and mobile) and Media controls

HIPAA Security Series #3- Physical Safeguards

67

Testing Practices and Test Security

Best practices for administering tests via telehealth & ensuring test security

68

Using Technology When Assessing

- The APA Task Force on Psychological Assessment and Evaluation Guidelines (2020) defined the term assessment as a complex activity, integrating knowledge, clinical judgment, reliable collateral information, and psychometric constructs with expertise in an area of professional practice or application.
- Psychologists are encouraged to consider the unique issues that may arise with test instruments and assessment approaches designed for in-person implementation, while maintaining the integrity of the tests' psychometric properties (APA Guidelines for the Practice of Telepsychology, 2013).
- Psychologists are encouraged to account for the unique impacts, suitability for diverse populations, and possible accommodations (APA guidelines 2013)


69

Psychologists Who Use Technology When Assessing Should...

- Strive to remain aware of the influence of technology on the assessment process
- Understand that reliability, validity, and fairness are still essential to the tests criteria
- Remember that the responsibilities continue to lie with the practitioner to be knowledgeable, understand the data used, and evaluate the validity and reliability of the tests used

70

All at once we all had questions



- Can I send student observation videos via Dropbox?
- Can I mail the blocks for the Block Design on the WISC-V to my client to use for tele-assessments?
- Can I email the DKEFS Trails subtests and color copies of the stimulus book to the client during the appointment and watch, via camera, the client, as they printed out the protocol and stimulus book to prevent practice effect and coaching?
- Can I leave protocols and stimulus books at the doorstep of the client and watch them retrieve the testing materials from a distance to make sure they were received to whom the materials were intended?
- Can I ask the client to rip up and shred copies of the stimulus pages I copied while they are on camera?
- Can the parent serve as the proctor during remote assessments?

71

Testing Practices

- There are multiple considerations to take into account when contemplating conducting an assessment utilizing a telehealth platform, such as materials, equipment requirements, environments, facilitators or no facilitators, and the person you are assessing.
- According to the NASP Principles for Professional Ethics (2020), Foundations of School Psychologists' Service Delivery includes Legal, Ethical, and Professional Practice, we must never forego these foundational structures for which our profession was built upon.
- We must continue to conduct our assessments in ethical ways that are consistent with well documented and valid empirical research for the assessments we are currently utilizing (NASP PPE, 2020).

72

Testing Practices

- Test publishers have provided information for psychologists to make informed decisions when conducting tele-assessment (CASP, 2020). However, many test publishers note on their websites that their testing instruments were **not** standardized for telehealth use, which should be noted when interpreting your results and in your reports.
- Although many testing publishers give guidelines and suggestions for conducting assessments (using certain tools) via telehealth, many still commit to the message of "it is not recommended".
- In regard to the WISC-V, Pearson clearly states using the WISC-V on any other platform other than Q-global, Q-interactive, or a Pearson-licensed telepractice provider/platform is not recommended (Pearson. (n.d)).

73

Testing Practices-NASP

NASP PPE (2020)

II. Professional Competence and Responsibility (Broad Theme)

II.3 the focus is on maintaining the highest standard for responsible professional practices in educational and psychological assessment (Guiding Principle).

"This guiding principle and its subsumed enforceable standards apply to school psychology assessment and intervention practices, including those that use technology such as computer-assisted and digital formats for assessment and interpretation, virtual reality assessment and intervention, distance assessment and telehealth intervention, or any other assessment or intervention modality."

The Standards that are under this principle include:

- II.3.2 Assessment Techniques
- II.3.5 Digital Administration and Scoring

74

Testing Practices-CASP

CASP COE (2021)

(4) Professional Practice- Technology and Social Media, it is recognized that technological opportunities can present ethical challenges and that it does not replace clinical and professional judgment.

(c) Online Platforms and Assessment, the focus is on ethical responsibility to ensure the tele-assessment follows all ethical codes.

- vii- integrity of the psychometric properties
- viii- appropriateness of the assessment using tele-assessment
- ix- use of a facilitator
- x- needed materials
- xi appropriateness of the environment

75

Test Security-NASP

The burden of test security lies with the Educational Psychologist, not parents, students, or adult clients.

NASP PPE (2020),
II. Professional Competence and Responsibility (Theme)
II.5 the focus is on intellectual property and protecting testing material from being used by unqualified persons. (guiding principle)

- II.5.1-Test Security
- II.5.2-Use of Restricted Materials
- II.5.3-Intellectual Property

76

Test Security-CASP

CASP COE (2021)
(4) Professional Practice- Technology and Social Media,
 School psychologists also consider security concerns regarding the storage and safety of electronic information, loss or compromised data, and informed consent for parents regarding its usage. School psychologists work to ensure the safety and security of electronic information.

(c) Online Platforms and Assessment

- (i)-school psychologists consider all components of online assessment, including internet safety and security.
- (iii)-maintain full responsibility for any technology used

77

Tele-Assessment and Confidentiality

In the spirit of gathering information and communicating with families, many have questioned whether they can:

- > Use regular, unencrypted, email to send observation videos, copies of the protocols and stimulus book pages, and receive completed intakes from parents/clients, and have parents/clients promise to shred the materials.
- > Use social media platforms or unprotected video methods to complete tele- assessments.

(CASP 2020)

78

Tele-Assessment and Confidentiality

- School psychologists/LEPs must continue to maintain client confidentiality even using telehealth. The platform you use must be specifically used for tele-assessment purposes, be HIPAA compliant, and should be able to provide you with a Business Associate Agreement (BAA). A BAA, part of the HIPAA Security Rule, is a written arrangement that specifies each party's responsibility when it comes to electronic Protected Health Information (ePHI) of the student/client.
- Best practices are to use encrypted emails for communication with clients when using PHI if you are using email.
- Dropbox will provide a BAA; however, you must obtain the BAA before any file containing PHI is uploaded to a Dropbox account.

(CASP, 2020)

79

Tele-Assessment and Confidentiality-NASP

NASP PPE (2020)

II. Professional Competence and Responsibility. (Broad Theme)

II.4, the focus is safeguarding and privacy of records. (Guiding Principle)

II.4.7 Electronic Record Keeping (Standard)

To the extent that school psychological records are under their control, school psychologists protect electronic files from unauthorized release or modification (e.g., by using passwords and encryption), and they take reasonable steps to ensure that school psychological records are not lost due to equipment failure.

80

Tele-Assessment and Confidentiality -CASP

CASP COE (2021)

(4) Professional Practice- Technology and Social Media (broad guideline)

(c) Online Platforms and Assessment

Tele-assessment is defined as a health or mental health assessment carried out remotely using audiovisual telecommunications between the school psychologist and the student.

(xx) and (xxi) focus on confidentiality within the environment, risk of access to data, risk using telecommunications (hardware, software, and other equipment), the use of HIPAA-compliant platforms, and only using platforms that the test publishers have granted.

81

05
Emergency Protocols

What is the right thing to do when there is a crisis and you are not in the same area as your client

82

What is protocol when there is a crisis during a telehealth session?

- > During a telehealth session, it is possible for a crisis situation to occur. A crisis situation may include a patient experiencing a medical emergency, a mental health crisis, or a safety concern.
- > It is important to maintain patient confidentiality during a crisis situation and minimize intrusion of privacy (APA Code of Ethics, 2017). Healthcare providers should only share patient information with other healthcare professionals as necessary to provide appropriate care and follow-up.
- > Crisis management during a telehealth session requires a calm and clear-headed approach. The protocol outlined on the following slides can help healthcare providers manage crisis situations effectively and ensure that their patients receive appropriate and timely care.
- > By establishing a crisis management protocol before providing telehealth services, healthcare providers can help ensure the safety and well-being of their patients.

83

The following protocol outlines the steps that healthcare providers can take in the event of a crisis during a telehealth session:

- > **Stay calm:** The healthcare provider should remain calm and composed during a crisis situation to help reassure the patient and to make clear and informed decisions.
- > **Assess the situation:** The healthcare provider should assess the situation and determine the level of urgency. If the patient is experiencing a medical emergency, you should call 911 immediately and contact their emergency contact person.
- > **Engage in crisis management:** If the patient is experiencing a mental health crisis, the healthcare provider should engage in crisis management strategies, such as providing emotional support and reassurance, offering coping strategies, and connecting the patient with appropriate resources, such as a crisis hotline or emergency services in their area.

84

Additional protocol outlines the steps that healthcare providers can take in the event of a crisis during a telehealth session:

- > **Ensure client safety:** If the patient is at risk of harm to themselves or others, the healthcare provider should take steps to ensure the patient's safety, such as contacting emergency services or notifying the patient's caregiver.
- > **Document the incident:** The healthcare provider should document the incident and the steps taken to manage the crisis situation, as well as any follow-up actions or referrals.
- > **Provide follow-up care:** The healthcare provider should provide appropriate follow-up care to the patient, such as scheduling a follow-up appointment or providing referrals to other healthcare professionals, as needed.

85

06
Technical Considerations & Challenges

You don't have to be tech savvy, but you do have to know what to do when something goes wrong

86

Technical Considerations

Internet Speed and Bandwidth:

- > Telehealth requires a stable and reliable internet connection with sufficient speed and bandwidth to support audio and video communication.
- > According to the Federal Communications Commission (FCC), video telemedicine requires a minimum download speed of 25 MB/s and a minimum upload speed of 3 MB/s. Depending on the number of devices simultaneously streaming content, latency, and other factors, higher download and upload speeds may be needed (O'Shea AMJ, Baum A, Haraldsson B, et al., 2022).
- > However, some platforms state that a minimum internet speed of 10 Mbps is needed for their telehealth sessions. Slower internet speeds can lead to poor quality audio and video, interruptions, and delays during the telehealth session.

87

Technical Considerations

Equipment Requirements:

- Telehealth requires the use of specific equipment, including a computer or mobile device with a camera and microphone, a reliable internet connection, and a secure telehealth platform.
- Healthcare providers may also require additional equipment, such as a high-quality camera or a headset with a microphone to provide the best quality service.

88

Technical Challenges

Technical difficulties can occur during telehealth sessions, which can negatively impact the quality and success of the session. Healthcare providers should be prepared to troubleshoot common technical issues, such as poor audio or video quality, internet connectivity problems, system outages, or platform malfunctions. Providers should have a backup plan in case of technical difficulties, such as switching to a phone call or rescheduling the session. These issues are all possible and can:

- Negatively impact the clinical rapport
- Negatively impact client success rate
- Decrease client satisfaction
- Increase client drop out rate
- Spoil tests

89

Common Technical Challenges and Recommendations

- **Device of connection issues experienced by clinician:**
Learn the platform extensively before providing any services.
- **Client may have incompatible devices and/or difficulty logging in:**
Begin assessing client's internet/device resources needs, skills, and resources. Provide client with a reference guide to the platform.
- **Client is unable to log into session due to poor internet/reception in their location:**
At initial session identify backup internet sources, such as alternative internet networks or personal hotspots.

(Adapted from: Wootton AR, McCuistian C, Legnitto Packard DA, Gruber VA, Saberi P., 2020)

90

Common Technical Challenges and Recommendations

- **Difficulty connecting and synching audio and video mid-session:**
Identify the issue. If difficulty with video, but there is audio: walk the steps to resolve the issue verbally. Additionally, use the platform chat feature to provide written instructions. If frozen or no video, try using ending the session and using audio only. Have a back up plan to call the client if this happens.
- **Unsteady or poorly framed video on part of the client:**
Inform the client of the difficulty to see them due to surroundings, lighting, or excessive movement. Educate the client on the importance of having the camera on a steady base, need for proper lighting, distance of camera, and environment.

(Adapted from: Wootton AR, McCustian C, Legnitto Packard DA, Gruber VA, Saberi P., 2020)

91

All This To Say...

92

It is important for healthcare providers to remember to...

- Tailor telehealth services to meet clients' needs.
- Be aware and address limitations and challenges for the population you are servicing.
- Understand there may be connectivity issues and a need for alternative methods of communication.

93

Telehealth services offer clients a more convenient and accessible way to receive healthcare services, but it is crucial for healthcare providers to:

- Comply with licensure requirements.
- Obtain informed consent before services begin.
- Ensure compliance with all aspects of HIPAA and CMIA.
- Maintain the same standard of care as you would for in-person healthcare services.

94

Licensed Educational Psychologists and other healthcare providers who provide telehealth services must prioritize:

- Client safety
- Client Privacy
- Quality of care by adhering to ethical and legal considerations and best practices.
- Crisis management protocols.

95

LEPs and other healthcare providers must also consider:

- Technical factors to ensure the success and quality of the service provided.
- Have reliable internet connection.
- Use equipment recommended by the HIPAA compliant platform you are using.
- Be prepared to troubleshoot technical issues while ensuring the security and privacy of patient information.

96

Secure Platforms and Online Companies

<p>Legal Considerations</p> <ul style="list-style-type: none"> > Licensure and Jurisdiction > Privacy and Data Protection <p>Ethical Considerations</p> <ul style="list-style-type: none"> > Competence and Training > Informed Consent and Boundaries > Confidentiality and Security > Cultural Competence and Diversity 	<p>Business Considerations</p> <ul style="list-style-type: none"> > Reimbursement and Insurance Coverage > Marketing and Advertising > Professional Liability Insurance <p>Logistic Considerations</p> <ul style="list-style-type: none"> > Technology Requirements and Infrastructure > Platform Selection and Security Measures > Scheduling and Time Zone Management
---	---

97

98

REFERENCES

American Psychological Association. (2013, July 31). *Guidelines for the practice of telepsychology*. <https://www.apa.org/practice/guidelines/telepsychology>.

American Psychological Association. (2017a). Ethical principles of psychologists and code of conduct (2002, amended effective June 1, 2010, and January 1, 2017). <http://www.apa.org/ethics/code/index.html>

American Psychological Association, APA Task Force on Psychological Assessment and Evaluation Guidelines. (2020). *APA Guidelines for Psychological Assessment and Evaluation*. Retrieved from <https://www.apa.org/about/policy/guidelines-psychological-assessment-evaluation.pdf>.

American Psychological Association. COVID-19 and the Health Service Psychological Workforce, 2020-2021. [Interactive Data Tool]. [<https://www.apa.org/pubs/reports/practitioner/covid-19-2021>]

99

REFERENCES

Board of Behavioral Sciences (Memo May, 25, 2023)

Barclays California Code of Regulations or Next Westlaw [https://govt.westlaw.com/calregs/Document/100E4B2134C821EC89E5000D3A7C4BC3?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=\(sc.Default\)#_co_anchor=19F4B26709F7911FD8A4BD4B8C4E59605](https://govt.westlaw.com/calregs/Document/100E4B2134C821EC89E5000D3A7C4BC3?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)#_co_anchor=19F4B26709F7911FD8A4BD4B8C4E59605)

California Association of School Psychologists. (2015). Licensed Educational Psychologist Code of Ethics. Retrieved from <https://casponline.org/pdfs/lep/LEP%20Code%20of%20Ethics%2010-15.pdf>

California Business and Professions Code Sec. 2290.5 (accessed April 2023) https://leginfo.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=2.&title=&part=&chapter=5.&article=12

100

REFERENCES

California Association of Marriage and Family Therapists. (2019). CAMFT Code of Ethics (amended effective December 2019, June 2011, January 2011, September 2009, July 2008, May 2002, April 1997, April 1992, October 1987, September 1978, March 1966). <https://www.camft.org/Membership/About-Us/Association-Documents/Code-of-Ethics>

Cheneyville, T., & Schwartz-Mette, R. (2020). Ethical considerations for psychologists in the time of COVID-19. *American Psychologist*, 75(5), 644-654. <https://doi.org/10.1037/amp0000661>

Gergen Barnett, K., Mishuris, R.G., Williams, C.T. et al. Telehealth's Double-Edged Sword: Bridging or Perpetuating Health Inequities?. *J GEN INTERN MED* 37, 2845-2848 (2022). <https://doi.org/10.1007/s11606-022-07481-w>

101

REFERENCES

HIPAA security series #4-Technical safeguards. Accessed May 18, 2023 <https://www.hhs.gov/sites/default/files/bcr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf> <https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html#:~:text=Physical%20Safeguards,Facility%20Access%20and%20text=A%20covered%20entity%20must%20limit%20authorized%20access%20is%20allowed.&text=Workstation%20and%20Device%20Security,to%20workstations%20and%20electronic%20media>

HHS for the Office of Civil Rights announces the expiration of COVID-19 public health emergency HIPAA notifications of enforcement discretion <https://www.hhs.gov/about/news/2023/04/11/hhs-office-for-civil-rights-announces-expiration-covid-19-public-health-emergency-hipaa-notifications-enforcement-discretion.html>. Accessed 5/29/2023.

Kathrin E. Maki, John H. Kranzler & Jessica M. Wheeler (2022): Ethical Dilemmas in School Psychology: Which Dilemmas Are Most Prevalent Today and How Well Prepared Are School Psychologists to Face Them?, *School Psychology Review*, DOI: 10.1080/2372966X.2022.2125338

102

REFERENCES

Lustgarten, S. D. (2016, January 1). New threats to client privacy. *Monitor on Psychology, 47*(1). <https://www.apa.org/monitor/2016/01/ce-corner>

National Association of School Psychologists. (2017). Guidance for delivery of school psychological telehealth [Brief]. Bethesda, MD: National Association of School Psychologists. <https://www.google.com/url?sa=t&ct=j&q=&esrc=s&source=web&cd=8&ved=2ahUKEwjQnrqfuuu8AHxgJlEhX4CkQFncECAGQAQ&url=https%3A%2F%2Fwww.nasponline.org%2F%39099.xml&usq=A0vVawlw9K8V5B8lCx8kkgcR0Gxq>

National Association of School Psychologists. (2020). Considerations for contract services in school psychology [Brief]. Bethesda, MD: National Association of School Psychologists.

O'Shea AMJ, Baum A, Haraldsson B, et al. Association of Adequacy of Broadband Internet Service With Access to Primary Care in the Veterans Health Administration Before and During the COVID-19 Pandemic. *JAMA Netw Open.* 2022;5(10):e2236524. doi:10.1001/jamanetworkopen.2022.36524

103

REFERENCES

Overcoming technological challenges: lessons learned from a telehealth counseling study https://escholarship.org/content/qt07n1m297/qt07n1m297_noSplash_e0bc3877137b6f4c3c9eaaea4b956238.pdf (accessed May 2023)

Perle, J. G., Perle, A. R., Scarisbrick, D. M., & Mahoney, J. J., 3rd (2022). Educating for the Future: a Preliminary Investigation of Doctoral-Level Clinical Psychology Training Program's Implementation of Telehealth Education. *Journal of technology in behavioral science, 7*(3), 351-357. 351-357. <https://doi.org/10.1007/s41347-022-00255-5>

Risk analysis report template. Quality insights of Delaware, regional extension center, privacy & security community of practice. January 7, 2011 v.1 [<https://hipaacow.org/wp-content/uploads/2012/09/HCR-Guide-for-the-HIPAA-COW-Risk-Toolkit-9-13-13.doc>]

104

REFERENCES

The Office for Civil Rights' guidance can be accessed on the U.S. Department of Health and Human Services, 12/15/08. [<https://www.hhs.gov/hipaa/for-professionals/faq/570/does-hipaa-permit-healthcare-providers-to-use-email-to-discuss-health-issues-with-patients/index.html>]. Retrieved 5/31/23.

Rights and requirements: A guide to privacy and security of health information in California, 2013. [<https://www.chcf.org/wp-content/uploads/2017/12/PDF-PrivacySecurityGuide.pdf>]

Standards of Practice for Telehealth Regulation Advisory. Department of Consumer Affairs, Board of Psychology. https://www.psychology.ca.gov/laws_regs/telehealth_standards.shtml. Accessed 5/25/23.

Website with new california healthcare laws that take effect January 2023 <https://www.idsupra.com/legalnews/new-california-health-care-laws-take-3842829/>

Wootton AR, McCuistian C, Legnitto Packard DA, Gruber VA, Saberi P. Overcoming Technological Challenges: Lessons Learned from a Telehealth Counseling Study. *Telemed J E Health.* 2020 Oct;26(10):1278-1283. doi: 10.1089/tmj.2019.0191. Epub 2019 Dec 3. PMID: 31800368.

105



106
