Daybreak University
MA and Ph.D. Programs in Counseling
with a Specialization in Marriage and Family Therapy (MFT)

Student Teletherapy and Virtual Supervision Compliance Policy

Student therapists agree to comply with the following concerning providing telehealth services and virtual supervision. Please initial each box, sign at the bottom, and submit it to the MFT Program Director.

1. Abide by all Daybreak University and Program policies and procedures regarding use of technology.
2. Agree not to violate any university or program policy, state, nor federal law.
3. Abide by the HIPAA rules and regulations.
4. Abide by the CCPA rules and regulations.
5. Agree not to use public wi-fi or hotspot to conduct telehealth sessions nor virtual supervision.
6. Obtain and maintain in working order all necessary electronic equipment for conducting teletherapy and virtual supervision. This may include a computer with a camera, internet, phone, and/or tablet.
7. Ensure that the electronic equipment used for teletherapy, and virtual supervision has anti-virus and up-to-date operating system installed.
8. Ensure the electronic equipment is charged and is located close to an electrical outlet.
9. Read and understand the portions of the most current AAMFT Code of Ethics https://aamft.org/Legal_Ethics/Code_of_Ethics.aspx pertaining to
    - Knowledge of regulatory standards (3.2)
    - Standard VI Technology Assisted Professional Services
10. Conduct teletherapy and virtual supervision ONLY in a secure location that is quiet, private, and free from distractions.
11. Conduct teletherapy and virtual supervision using ONLY the HIPAA compliant platform.
12. Read and understand AAMFT Best Practices in Online Practice of Couple and Family Therapy, available online through AAMFT (American Associated Marriage and Family Therapy) https://networks.aamft.org/telehealth/resources2/new-item2
13. Comply with teletherapy and virtual supervision standards of care including obtaining all informed consent and appropriate documents from clients PRIOR to commencing teletherapy and regularly confirming client and student therapist's identity and location.

14. Discuss with client and student therapists risks and benefits of teletherapy and virtual supervision PRIOR to commencing teletherapy and virtual supervision.

15. Communicate to clients and student therapists that technical difficulties may arise during their session. If this occurs, the student therapist or clinical supervisor will call the client by phone to re-establish communication about the next session appointment.

16. Comply with emergency protocols which include but are not limited to obtaining emergency numbers for the client's location (such a police officer, fire rescue), having access to clinical supervisor's contact information during teletherapy and virtual supervision sessions, and obtaining and having access to client's address where they are located at the time of the session.

17. Ensure that both the teletherapy clients and student therapists are appropriate for teletherapy including but not limited to understanding technology, being able to utilize required technology, are able to be in a secure, private location, are not in danger of self-harm or harm to others and are not chemically compromised.

18. Continuously monitor client's symptoms to determine if a referral to an in-person therapy format is warranted.

19. Store and maintain all client and student therapist data in a confidential manner.

20. Abide by the local, state, and provincial requirements and regulations where the client, student therapist, and supervisor are located.

21. Conduct teletherapy and virtual supervision only in areas where qualified.

22. Abide by the specifications set forth by California (https://bbs.ca.gov/pdf/agen_notice/2021/20210122_telehealth_v.pdf)

23. Abide by the BBS California Statutes and Regulations Relating to the Practices of Professional Clinical Counseling for Marriage and Family Therapy

    (https://www.bbs.ca.gov/pdf/publications/lawsregs.pdf)

24. Fill out the form by the BBS California responsibility statement for supervisors of a Marriage and Family Therapist trainee or associate.

    (https://www.bbs.ca.gov/pdf/forms/mft/mfrespon.pdf)

Telehealth Technology Usage Policy

1. Technology Use: MFT providers will use secure and encrypted software for telehealth sessions and will ensure that all equipment used is up to date and functioning correctly.

2. Zoom Sessions: Providers will ensure that Zoom sessions are conducted in private areas and will not be recorded or shared without the client's informed consent.

3. When using Zoom as teletherapy, ensure to use Zoom Healthcare which is in compliance with HIPAA BAA.

4. Recording Sessions: If recording sessions are necessary, providers will obtain the client's informed consent, ensure that the recording is stored securely, and will not be shared with unauthorized individuals.

5. Saving in Google Drive or Emails: Providers will ensure that all emails and documents containing clients' personal and sensitive information are sent through encrypted channels and stored securely in Google Drive or other secure platforms. Any sharing of these documents with unauthorized individuals is prohibited.

6. Informed Consent: Providers will obtain informed consent from clients before initiating any telehealth session and inform them of the risks and benefits of telehealth services.

7. Confidentiality: Providers will adhere to all state and federal confidentiality laws and regulations, and all client information will be kept strictly confidential.

8. Technical Issues: Providers will have a backup plan in place for technical issues that may arise during telehealth sessions, such as network interruptions or equipment malfunctions.

9. Termination of Services: Providers reserve the right to terminate telehealth services if they determine that telehealth is not clinically appropriate or if there is a breach of this policy.

Beginning Requirements

1. Obtained a trainee position at the Daybreak University Couples and Family Therapy Center (CFTC).
2. Submit a signed Affiliation Agreement to the Clinical Director if a trainee practices outside of the Daybreak University CFTC.
3. Complete the BBS MFT Supervisor Responsibility Statement.
4. Join TheraNest and set up your account. TheraNest is a professional online service used to track and report clinical training hours. TheraNest meets BBS regulations to assist the Trainee/Intern in viewing status, as well as providing required BBS forms.
5. Join Zoom and set up your account as Zoom Healthcare which is in compliance with HIPAA BAA and send the signed Agreement to the Clinical Director.
6. Contact clients using Daybreak University Couples and Family Therapy Center (CFTC) emails, which is in compliance with the regulations.

Ongoing Requirements

1. Attend and participate in your Supervised Practicum course each week via Zoom.
2. Comply with the current BBS Statutes and Regulations.
3. Comply with the policies and procedures set by the MFT program.
4. Comply with the policies and procedures set by your clinical training site.
5. Comply with all ethical and legal obligations during your clinical training.
6. Have your supervisor sign the BBS Weekly Summary of Hours of Experience log form each week.
7. Immediately report all changes and/or concerns at your site to the Clinical Training Director. These changes may include a. Supervisor changes b. Site location changes c. Changes to the four-way clinical training agreement (i.e. early termination or an extension of the terms of agreement)
8. If a student's malpractice insurance or AAMFT membership has expired, then the student will need to renew their policy and/or membership and submit the renewal documentation to show that the coverage is up to date.
9. The student is responsible for notifying the program in a timely manner of any professional or personal difficulties, which may affect the performance of his or her professional duties and responsibilities.

Upon Initiation of Telehealth Services

The regulations require the therapist to engage in four specific one-time actions upon initiation of telehealth services to a client. The four actions are as follows:

1. **Obtain Consent:** The therapist providing telehealth services must obtain consent from the client as required by the "telehealth statute" (Business and Professions Code Section 2290.5).4 The statute requires the therapist to 1) inform the client about the use of telehealth; 2) obtain from the client verbal or written consent for the use of telehealth as an acceptable mode of delivering psychotherapy services; and 3) document the consent obtained by the client in the client's treatment record.
2. **Disclose Risks/Limitations:** The therapist must inform the client of the potential risks and limitations of receiving treatment via telehealth.5 This disclosure may be done verbally or in writing. Either way, documentation of the disclosure in the client's record is recommended. Potential risks and limitations of telehealth may include: technical failures; interruption by unauthorized persons; unauthorized access to transmitted and/or stored confidential information; and decreased availability of the therapist in the event of a crisis. C*AMFT Code of Ethics* Section 1.4.2 also requires the therapist who is rendering telehealth services to "inform patients of the potential risks, consequences, and benefits,

including but not limited to, issues of confidentiality, clinical limitations, transmission difficulties, and ability to respond to emergencies."

3. **Disclose License/Registration:** The therapist must also provide the client with his or her license or registration number and the type of license or registration. This disclosure can be done verbally or in writing. Most therapists have this information on their Disclosure Statements or Informed Consent Forms.
4. **Provide Contact Information of Relevant Resources:** The therapist must document reasonable efforts to ascertain the contact information of relevant resources, including emergency services in the client's geographic area.

For Each Telehealth Session

The regulations provide three actions the therapist must take each and every time he or she performs telehealth with a client. The three actions are as follows:

1. At the beginning of each telehealth session, the therapist must verbally obtain from the client the client's name and document such name and the address of the client's present location. According to the BBS, obtaining the client's full name and present location may lessen the possibility of impersonation of a client. Further, should an emergency situation arise, the therapist would be equipped with information regarding the client's location, which may change from session to session.
2. The therapist, during each telehealth session, must assess whether the client is appropriate for telehealth, including but not limited to, consideration of the client's psychosocial situation. The BBS is concerned the client's mental health could change from session to session, hence the therapist should assess whether the rendering of psychotherapy via telehealth continues to be appropriate for the client.
3. The necessary documentation of this issue may vary, depending on the client and his or her particular circumstances. For example, in circumstances where the client is in significant distress, or has a chronic history of serious behavioral health problems, a therapist may determine that it is appropriate to document in considerable detail, his or her effort to carefully assess the suitability and appropriateness of telehealth services for the particular patient at that time. In other circumstances, it may be adequate to document that the therapist believes, based upon his or her discussion with the client, that the use of telehealth is appropriate to the client's needs.
4. For each session, the therapist must utilize industry best practices for telehealth to ensure both client confidentiality and the security of the communication medium. A key inquiry is whether the voice, video, and file transfers through the platform are secured or encrypted. In addition, consider researching if any video or voice data is stored on the platform's server(s) and if yes, whether the files on the server(s) are encrypted. Documentation of the therapist's due diligence in researching and verifying the security of the communication medium is essential. Therapists who utilize a videoconferencing platform for telehealth should take care to protect their computers from viruses that can

not only damage the computer, but also collect private stored data by installing antivirus software and firewalls. The computer or mobile device used for videoconferencing should be regularly receiving the most recent security updates. It is recommended to choose strong and unique passwords for both the computer and the platform's account. Providers who are HIPAA "covered entities" should ensure the technology used for telehealth services is compatible with HIPAA requirements.

HIPPA Rules and Regulations

HIPAA (Health Insurance Portability and Accountability Act) is a U.S. federal law that establishes rules and regulations to protect the privacy and security of individuals' health information. If you are taking an online class related to HIPAA requirements, here are some key things you should know:

1. HIPAA applies to "covered entities" and "business associates." Covered entities are healthcare providers, health plans, and healthcare clearinghouses. Business associates are individuals or organizations that provide services to covered entities and have access to protected health information (PHI). Both covered entities and business associates must comply with HIPAA rules.
2. HIPAA has two main components: the Privacy Rule and the Security Rule. The Privacy Rule establishes national standards for protecting the privacy of PHI. The Security Rule establishes national standards for protecting electronic PHI (ePHI) that is created, received, maintained, or transmitted by covered entities and business associates.
3. HIPAA requires covered entities and business associates to implement administrative, physical, and technical safeguards to protect PHI and ePHI. These safeguards include things like implementing access controls, encrypting ePHI, conducting regular risk assessments, and training employees on HIPAA policies and procedures.
4. HIPAA also requires covered entities and business associates to notify individuals if there is a breach of their unsecured PHI or ePHI. Notifications must be made without unreasonable delay and no later than 60 days after the discovery of the breach.
5. HIPAA violations can result in significant penalties, including fines and legal action. Covered entities and business associates should take HIPAA compliance seriously and ensure that they have appropriate policies, procedures, and safeguards in place.

In summary, HIPAA is a federal law that establishes rules and regulations to protect the privacy and security of individuals' health information. Covered entities and business associates must comply with HIPAA rules, including implementing safeguards to protect PHI and ePHI, notifying individuals in the event of a breach, and taking HIPAA compliance seriously to avoid penalties.

Business Associate Agreement (BAA) Regulations

A BAA (Business Associate Agreement) is a legal agreement that outlines the responsibilities and obligations of a business associate (BA) when handling protected health information (PHI) on behalf of a covered entity (CE) under HIPAA (Health Insurance Portability and Accountability Act).

The BAA agreement rules are as follows:

1. Covered entities must enter into a BAA with their telehealth vendors or service providers that have access to PHI. This includes any third-party software or technology used to provide telehealth services.
2. The BAA must include specific provisions related to telehealth, such as how PHI will be transmitted and secured during telehealth sessions, the role of the vendor or service provider in protecting PHI, and how any breaches will be handled.
3. Business associates must comply with all HIPAA regulations related to telehealth, including the use of encryption to protect PHI during transmission, and ensuring that PHI is only accessed by authorized individuals.
4. Covered entities must conduct due diligence to ensure that their telehealth vendors or service providers are HIPAA-compliant and have appropriate safeguards in place to protect PHI.
5. Business associates must report any breaches of PHI to the covered entity immediately and take steps to mitigate the harm caused by the breach.

It is important to note that the rules and regulations related to telehealth and BAA agreements may vary depending on the specific state and local laws and regulations, as well as the specific type of telehealth service being provided. Therefore, it's always best to consult with a legal expert to ensure that your telehealth BAA agreement is in compliance with all applicable laws and regulations.

California Consumer Privacy Rights

The California Consumer Privacy Act (CCPA) is a comprehensive privacy law that grants California residents certain rights over their personal information and imposes obligations on businesses that collect, use, and disclose that information.

Under the CCPA, California residents have the right to:

1. Know what personal information is being collected about them.
2. Know whether their personal information is sold or disclosed and to whom.
3. Opt-out of the sale of their personal information.
4. Access their personal information.
5. Request the deletion of their personal information.
6. Not be discriminated against for exercising their CCPA rights.

Businesses subject to the CCPA must:

1. Provide certain disclosures to California residents regarding the collection, use, and disclosure of their personal information.
2. Implement reasonable security measures to protect personal information from unauthorized access, destruction, use, modification, or disclosure.
3. Comply with opt-out requests from California residents who do not want their personal information sold.
4. Provide access to personal information and delete it upon request.
5. Not discriminate against California residents who exercise their CCPA rights.

The CCPA is enforced by the California Attorney General's office, and individuals may also have a private right of action for certain data breaches.

Google Workspace Regulations

Using and storing client information on Google Drive and email for telehealth purposes requires compliance with HIPAA regulations to protect the privacy and security of the client's protected health information (PHI):

1. Sign a Business Associate Agreement (BAA) with Google: Before using Google Drive or email to store and share PHI, it's essential to sign a BAA with Google. This agreement outlines the responsibilities and obligations of both parties to ensure compliance with HIPAA regulations.
2. Enable two-factor authentication: It's essential to enable two-factor authentication for both Google Drive and email to add an extra layer of security to protect PHI from unauthorized access.
3. Encrypt data: Any PHI stored on Google Drive should be encrypted using a strong encryption method to ensure that even if someone unauthorized gets access to it, they cannot read it.

4. Use secure transmission methods: Emails containing PHI should be encrypted before sending and sent through secure transmission methods, such as a HIPAA-compliant email service or a secure file transfer protocol (SFTP).
5. Limit access: Access to PHI on Google Drive should be limited to only authorized individuals who have a need to know the information.
6. Monitor and track access: Keep track of who is accessing PHI on Google Drive and email and ensure that any unauthorized access is immediately reported and addressed.
7. Train staff: Ensure that all staff members who have access to PHI stored on Google Drive and email receive regular HIPAA training to ensure they understand the importance of protecting PHI and are aware of HIPAA compliance requirements.

By following these rules, you can help ensure that the client's PHI is protected while using and storing client information on Google Drive and email for telehealth purposes in a HIPAA compliant manner.

Google Regulations for HIPAA and BAA

1. Enabling Google Vault for email and chat retention and eDiscovery purposes
2. Enabling Mobile Device Management (MDM) to manage and secure mobile devices that access PHI
3. Enabling Data Loss Prevention (DLP) to prevent sensitive information from being shared
4. Enabling two-factor authentication (2FA) to add an additional layer of security to user accounts
5. Configuring security settings for Google Meet, Calendar, and other collaboration tools
6. It's important to note that while Google Workspace can be configured to be HIPAA-compliant, you as a customer are responsible for ensuring that you use the service in a compliant manner, and that you have policies and procedures in place to protect the privacy and security of PHI.

Collecting Client Information using Google Form Regulations

Collecting client information with Google Forms for telehealth purposes requires compliance with HIPAA regulations to protect the privacy and security of the client's protected health information (PHI). Here are some rules to follow:

1. Sign a Business Associate Agreement (BAA) with Google: Before using Google Forms to collect PHI, it's essential to sign a BAA with Google. This agreement outlines the responsibilities and obligations of both parties to ensure compliance with HIPAA regulations.
2. Train staff: Ensure that all staff members who have access to the PHI collected through Google Forms receive regular HIPAA training to ensure they understand the importance of protecting PHI and are aware of HIPAA compliance requirements.
3. Enable two-factor authentication: Enable two-factor authentication for the Google account to add an extra layer of security to protect PHI from unauthorized access.
4. Use a secure connection: Ensure that the Google Form is accessed through a secure and encrypted connection to protect PHI while in transit.
5. Collect the minimum necessary information: Collect only the minimum necessary PHI needed for telehealth purposes, and avoid collecting any unnecessary information.
6. Limit access: Access to the collected PHI on Google Forms should be limited to only authorized individuals who have a need to know the information.
7. Monitor and track access: Keep track of who is accessing the PHI collected through Google Forms and ensure that any unauthorized access is immediately reported and addressed.
8. Delete PHI after use: Once the PHI collected through Google Forms is no longer needed, it should be deleted from the Google account to ensure that it is not accidentally disclosed or accessed.

By following these rules, you can help ensure that the client's PHI is protected while collecting client information with Google Forms for telehealth purposes in a HIPAA compliant manner.

TheraNest

TheraNest is a practice management software designed for mental health providers, and it can be used by students who are studying to become mental health professionals to manage their clients' information and records. Students who are enrolled in counseling, psychology, or social work programs can use TheraNest to track their clients' progress, manage their appointments, and securely store their confidential health information.

TheraNest provides a range of features that can be helpful for students who are working with clients, including:

1. Scheduling and appointment management: Students can use TheraNest to schedule appointments with their clients, send appointment reminders, and manage their availability.

2. Client management: TheraNest allows students to create client profiles, store confidential health information, and track progress notes and treatment plans.
3. Billing and invoicing: TheraNest offers billing and invoicing features that can help students manage their finances and streamline their accounting processes.
4. Secure messaging: TheraNest includes a secure messaging system that enables students to communicate with their clients in a secure and HIPAA-compliant way.
5. Telehealth services: TheraNest also offers telehealth features that allow students to conduct remote counseling sessions with their clients.

TheraNest is a HIPAA compliant practice management software for mental health providers. TheraNest is designed to meet the privacy and security requirements of the Health Insurance Portability and Accountability Act (HIPAA) and is committed to maintaining the confidentiality and security of patient health information.

TheraNest includes various security features and safeguards to ensure the confidentiality and integrity of patient data, including:

- Data encryption both in transit and at rest
- Role-based access control to restrict access to sensitive information
- Automatic session timeouts to prevent unauthorized access
- User activity logging to monitor and track system usage
- Regular system backups to ensure data availability and integrity

Patient Rights & Consent

State law requires the health care provider initiating the use of telehealth to obtain written or verbal consent once before the initial delivery of telehealth services. Medi-Cal has developed Telehealth Patient Consent Language, which includes language outlining a beneficiary's right to in-person services, the voluntary nature of consent, the availability of transport to access in-person services if needed, and potential limitations/risks of receiving services via telehealth. Patient consent can be completed verbally or in writing. Patients who consent to synchronous video must separately consent to synchronous audio-only services.

Recording and Confidentiality

Students are required to present recordings of their clinical work as part of the clinical training requirements. Recordings must be treated in the same manner as any other confidential materials and the student must obtain written consent by the client prior to recording. Recordings are to be kept in a locked place at your clinical training site and while transporting the recording tape, all precautions must be taken

to guard confidentiality. To be HIPAA compliant, the acceptable session recording formats include CD/DVD and flash drives, or personal recording devices (camera, cell phone, laptop, or tablet) which must be password protected. For Zoom recordings, record to the Zoom Healthcare clouds and delete after supervision.

Clinical Training Student Requirements

Once a student begins their clinical training, they are required to join TheraNest. TheraNest is a web-based computer software program designed to assist students in tracking and reporting one's hours. Clinical training hours will be submitted utilizing this web-based computer software program. Students are responsible for all BBS paperwork and should keep their paperwork in a safe and secure place. Students can obtain the required clinical training paperwork by downloading it from Google Drive from CFTC.

Clinical Training Probation

1. Students must meet and comply with the BBS Statutes and Regulations, as well as the policies set by the MFT program. A student may be placed on Clinical Training Probation, which subjects the student to a period of review and additional requirements as deemed by the faculty committee due to a violation of BBS, MFT program, and/or clinical training site requirements.

2. Students may be placed on Clinical Training Probation for one or more of the following reasons, but is not limited to:
    - Incomplete/Missing Clinical Training Paperwork
    - Unprofessional Conduct
    - Deficient Clinical Skills
    - Lack of Sufficient Progress
    - Gross Negligence
    - Violation of BBS Statutes and Regulations
    - Violation of Clinical Training Site Policies
    - Violation of MFT Program Policies
3. Students placed on Clinical Training Probation will receive a formal letter indicating their period of probation and the additional requirements the student will need to meet in order to continue in their clinical training. Students must complete the additional requirements in order to remain in their clinical training site and continue accruing hours.
4. ours. The minimum requirements for clinical hours will be 1,750 hours comprising of direct counseling with individuals, groups, couples or families and a maximum 1,250 of

non-clinical experience which includes supervision, workshops, training, and conferences, administering psychological tests, writing clinical reports, writing progress or process notes, and client-centered advocacy. Client contact hours include therapy with individuals, couples, families, group therapy and/or teletherapy.

5. Client-centered advocacy is defined in the Business and Professions Code (BPC) 4980.34 (h) as including, but not limited to, “researching, identifying, and accessing resources, or other activities, related to obtaining or providing services and supports for clients or groups of clients receiving psychotherapy or counseling services.” Group therapy hours are counted by the number of hours, not the number of clients within the group.
6. Students may not count hours for the BBS or the MFT program for any week where supervision was not provided. If a supervisor is providing supervision on a volunteer basis, a letter of agreement is needed. On the Experience Verification form, there is a place for the supervisor to indicate if they are providing supervision on a volunteer basis, as opposed to self-employed or on a paid basis. If the supervisor is working on a volunteer basis, then attach the original written agreement between you and the applicant’s employer required by Title 16, California Code of Regulations Section 1833 (b) (4). This letter of agreement is needed any time your supervisor is not paid by your employer for the provision of supervision.

State Regulations and Rules

It is essential to follow each state's regulations when providing Marriage and Family Therapy (MFT) through telehealth services. Each state has its own guidelines and requirements for telehealth therapy, and it is crucial to understand and adhere to them to avoid any legal or ethical issues. Some states may require specific licenses, certifications, or training for MFT telehealth therapy. Additionally, there may be rules regarding informed consent, confidentiality, and technology requirements that must be followed. By following each state's regulations, MFT providers can ensure that they are providing safe and effective telehealth therapy to their clients while also maintaining compliance with state laws and regulations.

State/Provincial Telehealth Guidelines

This guideline contains information pertaining to teletherapy laws at the state-level, including any waivers to certain teletherapy requirements and policies regarding insurance reimbursement for teletherapy. Not all states have regulations; updates will be made to this page as new information is received. This information can change rapidly.

https://www.aamft.org/Events/State_Guide_for_Telehealth.aspx

California State Regulations on Telehealth

Marriage and Family Therapist Trainees and Telehealth Marriage and family therapist trainees are unlicensed and unregistered individuals who are currently enrolled in their master's or doctoral degree program designed to qualify them for licensure as a marriage and family therapist, and who have completed at least 12 semester units or 18 quarter units of their degree program. MFT trainees are permitted to provide services via telehealth. The school must approve and have an agreement with the site detailing, among other things, the methods by which supervision shall be provided. MFT trainees can count pre-degree hours toward licensure, so they need to make sure they follow the law regarding counting experience hours. If they are working in a governmental entity, school, college, university, or institution that is nonprofit and charitable, they may obtain supervision via videoconferencing. If they are working in a setting other than the types listed above, the law requires the supervisor to be in person.
https://bbs.ca.gov/pdf/agen_notice/2021/20210122_telehealth_v.pdf

Virginia State Regulations on Telehealth

Licensure Board COVID-19 Information : The licensure board has a webpage listing COVID-19 information for LMFTs and LMHCs.

https://www.dhp.virginia.gov/counseling/

The Virginia Board of Counseling regulates the practice of Marriage and Family Therapy in the state. The Board has specific regulations related to telehealth services, which apply to MFT supervisees who are providing such services under the supervision of a licensed MFT supervisor.

The relevant law and regulations for MFT supervisees in Virginia providing telehealth services are:

1. Virginia Code § 54.1-3500.1: This law outlines the requirements for the provision of telehealth services in the state. It requires that telehealth services be provided in a manner that is consistent with the standards of care for in-person services and that practitioners must ensure the security and privacy of electronic communications.
2. Virginia Board of Counseling Regulations (18 VAC 115-50-115): These regulations specifically address the provision of telehealth services by MFTs in Virginia. The regulations require that MFTs must be licensed in the state and that they must comply with all laws and regulations related to the provision of telehealth services.
3. Virginia Board of Counseling Guidance Document: The Board has also provided guidance for MFTs who are providing telehealth services in Virginia. The guidance

document outlines the specific requirements for informed consent, confidentiality, and security for telehealth services.

As an MFT supervisor in Virginia, it is important to be familiar with all relevant laws, regulations, and guidance related to the provision of telehealth services. It is also important to ensure that you are providing services under the supervision of a licensed MFT supervisor and that you are complying with all ethical and legal guidelines for the provision of mental health services.

New Jersey State Regulations on Telehealth

Out-of-State Healthcare Providers Can Offer Services to New Jersey Residents During COVID-19 Emergency (3/20/20): The State of New Jersey is allowing individuals who hold current licenses as an LMFT or other healthcare licenses in good standing in other states and have been practicing within the last five years, will be able to secure a license in New Jersey by completing a simple form. Additional information for out-of-state providers. These temporary licenses are valid for 180 days after completion.

Temporary waiver of telemedicine rules to allow healthcare practitioners to more easily provide care via telemedicine. The expiration of this order is congruent with Executive Order #103, which appears to be whenever the state of emergency ends, or when the Governor announces the end of Order #103.

https://www.njconsumeraffairs.gov/COVID19/Documents/FAQ-Telehealth.pdf#search=telehealth

Arizona State Regulations on Telehealth

With the efforts to reduce community spread of COVID-19, many practitioners are seeking guidance on telepractice. Continuity of care is vital to mental health clients, and in this new climate, we encourage our licensees to become competent in telehealth delivery to continue to serve those in need. There are many resources to assist behavioral health professionals in providing technology assisted therapy. The Board does not have restrictions on which license types (temporary licensees, associate level or independent level licensees) can provide telepractice, however there may be limitations if providers are working through third party reimbursement.

Out of state clinicians, please read: Board statutes and rules related to telepractice.

http://www.azbbhe.us/node/847

- Guidance on revisions to A.A.C. R4-6-1106

Governor Ducey's Executive Order 2020-15 - Expansion of Telemedicine

Federal and National Resources:

- Medicaid guidance on telemedicine
- Department of Health and Human Services COVID-19 telehealth update FAQ
- Association of Health Insurance Providers' members response to COVID-19
- AAMFT COVID-19 update including telehealth resources
- ACA telehealth information
- ASWB regulatory provisions
- CACREP response
- NAADAC COVID-19 update including telehealth resources
- NASW telehealth resource
- NBCC COVID-19 update including telehealth resources

Executive Order Expanding Telemedicine Coverage: Executive Order 20-15 requires insurance plans regulated by the state to cover telehealth and requires that reimbursement rates for providers be no lower than the rate for the same service performed in-person.

Student therapist: _____
Print Name

Signature: _____ Date: _____