Telemedicine

Telebehavioral Health

Telemental Health

Telehealth

Teletherapy

Distance Counseling

Telecare

TELEHEALTH (CEH 9)

The purpose of this course is to expand the knowledge and skills of mental health practitioners, by examining clinical, technical, and administrative principles in telehealth; and relevant ethical, legal and regulatory standards.

This course defines and underscores ethical, legal and regulatory standards for the delivery of mental health related services via telecommunication technologies as referenced by the following:

- American Academy of Child and Adolescent Psychiatry
- American Counseling Association: Distance Counseling, Technology, and Social Media
- American Mental Health Counseling Association (AMHCA)
- American Psychiatric Association Best Practices in Videoconferencing-Based Telemental Health,
- American Psychological Association
- American Telemedicine Association
- NAADAC: The Association for Addiction Professionals
- National Institutes of Health: Guidelines for Establishing a Telemental Health Program to Provide Evidence-Based Therapy for Trauma-Exposed Children and Families,
- NBCC Training Requirements.
- Telebehavioral Health Institute
- Rules and Regulations set forth by Alabama, Florida, Georgia, Louisiana, and Mississippi

INTERRELATED TERMS

Telemedicine - the use of telecommunications technologies to support the delivery of various medical, diagnostic and treatment-related services usually by doctors.

Telehealth - includes a wider variety of *remote healthcare services beyond the doctor-patient relationship*.

Telecare – the use of technology that allows consumers to stay safe and independent in their own homes.

e-health: health services and information delivered or enhanced through the Internet and related technologies.

mHealth: health and medical prevention and treatment supported by technologies (wireless gateways and connectivity, biosensors and wearable personal technology, precision medicine, patient engagement and empowerment).

Distance Counseling: the provision of counseling services by means other than face-to-face meetings, usually with the aid of technology (American Counseling Association).

Telebehavioral health: the delivery of behavioral health services using interactive technologies (use of audio, video or other electronic communications) between a practitioner and a client/patient who are not in the same physical location (Telebehavioral Health Institute).

Telemental health: the provision of mental health and substance abuse services from a distance, (American Telemedicine Association).

Teletherapy: a method of delivering counseling and marriage and family therapy/psychotherapy services using interactive technology-assisted media for the rendering of professional marriage and family therapy and psychotherapy services, limited to prevention, assessment, diagnosis, and treatment of mental, emotional, behavioral, relational, and addiction disorders to individuals, couples, and families, singularly or in groups that enables a licensee and a client separated by distance to interact via synchronous video and audio transmissions (LA LPC Board of Examiners).

Telepsychology or telemental health: The provision of behavioral and/or mental health care services using technological modalities in lieu of, or in addition to, traditional face-to-face methods (e.g., provision of therapy using the phone, diagnostic interviewing via videoteleconferencing, use of applications to track mood states, consultations via email, (American Psychological Association).

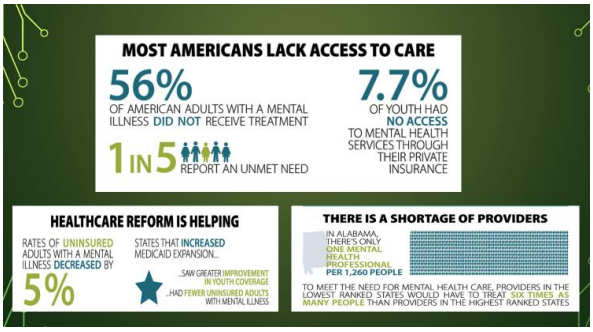
Telepsychiatry: a subset of telemedicine, involving direct interaction between a psychiatrist providing a range of services including evaluations, therapy (individual therapy, group therapy, family therapy), patient education and medication management, (American Psychiatric Association).

MODES OF TELETHERAPY

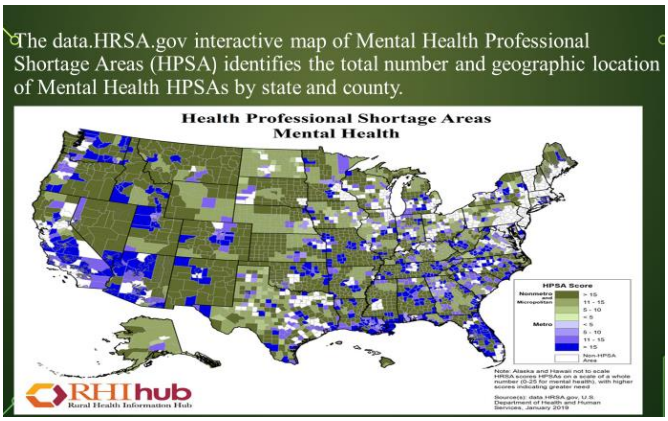
Avatar	Video	Textbase
		
Client and Therapist are represented by Animated characte Conducted in a Virtual Office	**Computer / Tablet/ Smartphone** **Face-to-Face Connection** **Asynchronous Communication**	**Computer/Smartphone Keyboard** **Chat / Email / Messaging / Texting** **Asynchronous Communication**

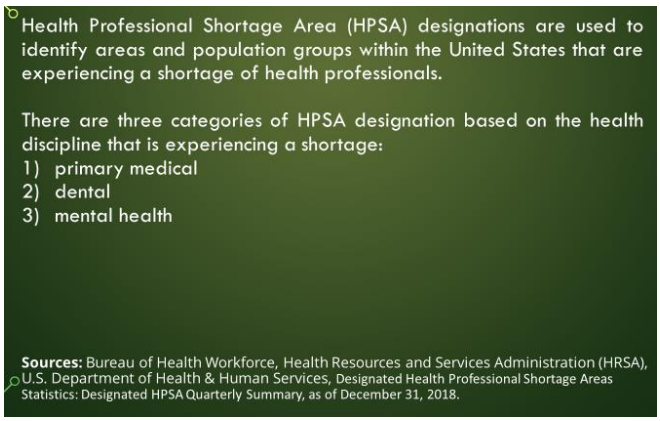
- Each has advantages and disadvantages; and ethical, legal , and reimbursement requirements
- Each can be secure (encrypted and private), or unsecure method

THE NEED FOR TELEMENTAL HEALTH



According to the Results from the 2017 National Survey on Drug Use and Health: Detailed Tables, 19.1% of residents aged 18 or older of nonmetropolitan counties had any mental illness (AMI) in 2017, approximately 6.8 million people.
In addition, 4.9%, or nearly 1.7 million, of residents of nonmetropolitan counties experienced serious thoughts of suicide during the year. While the prevalence of mental illness is similar between rural and urban residents, the services available are very different. Source: Rural Health Information Hub https://www.ruralhealthinfo.org/topics/mental-health





As of September 4, 2018, HRSA had designated 2,672 Mental Health Professional Shortage Areas in rural areas. It is estimated that it would take 1,851 practitioners to remove the designations.
Review Bureau of Health Workforce Health Resources and Services Administration (HRSA) U.S. Department of Health & Human Services As of June 2, 2019

BENEFITs of TELETHERAPY: Accessibly / Flexibility / Reduces Costs

- Access to extensive nationwide network of highly qualified, specialized, culturally and linguistically diverse licensed therapists.
- Greater access for clients and providers with disabilities.
- Greater options, allowing for more targeted and effectual outcomes.
- Flexibility in scheduling appointments.
- Reduction in traveling time and expenses.
- Except for the cost incurred by equipment, software, and technology, teletherapy has exceptional value and is affordable.

Mental Health services are generally the same whether the therapy is delivered onsite or via teletherapy.

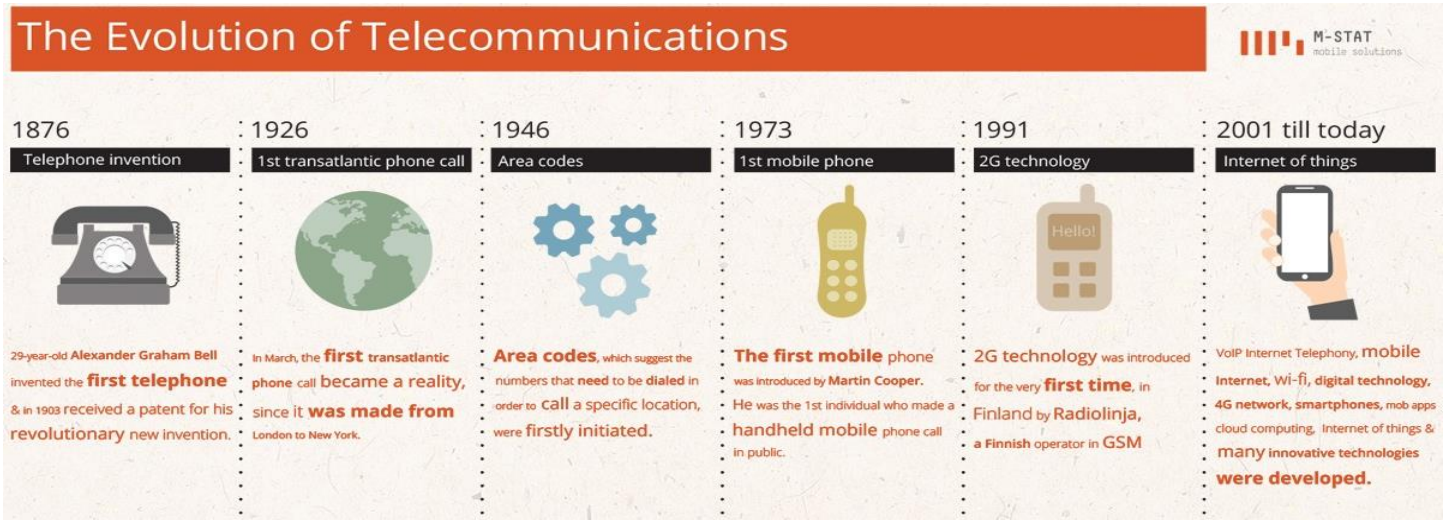
CHALLENGES & GROWTH

Telemental health touches federal laws and regulations (e.g., HIPAA), but most of the significant issues involve state law. Each state has a different licensing and regulatory requirements for mental health providers. This disparity among state laws creates significant legal and regulatory issues, including privacy, security, follow-up care, emergency care, treatment of minors and reimbursement.

Common Telemental Health Challenges

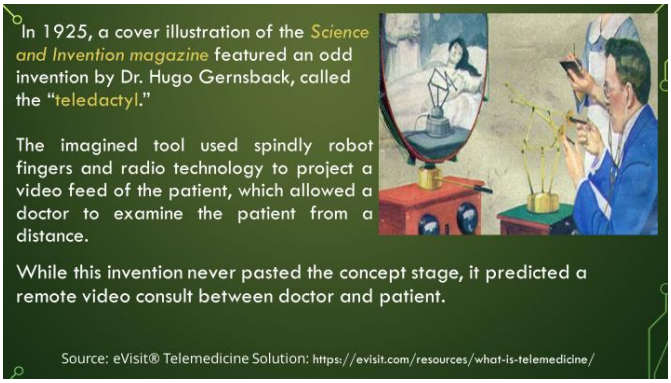
- Insurance may or may not cover telemental health — coverage depends on the policy and the state of residence.
  More than 40 states reimburse for telehealth under Medicaid plans,
  < 25 states require insurance companies to provide some form of reimbursement.
- Online platforms may make it difficult for providers to establish good rapport with their clients.
  It is more difficult to detect nonverbal cues using.
- Not all clients have, or understand, the technology needed for telemental health services.

THE HISTORY AND EVOLUTION OF TELEHEALTH HISTORICALLY



The idea of using telecommunications in the healthcare industry was first postulated in the early 1900s.

- Radio Telecardiology was first attempted in the 1910s
- Telephone-mediated Telestethoscopy in the 1920s
- Radiology image transfer and videophone experimentation in the early 1950s.



<u>In recent years, several factors have facilitated increased Telemedicine use:</u>

- Lower cost and more widely available communications systems;
- Lower cost, higher performance computers;
- Greater public confidence in the use of computer technology;
- Greater acceptance of the technology by medical professionals; and
- Emerging global standards in communications, video conferencing, and medical disciplines.

FEDERAL ROLE IN TELEHEALTH

<u>The Federal role in Telehealth includes:</u>

- funding of demonstration projects and evaluation,
- direct services provision,
- Medicare payment for Telehealth services, and
- regulation of remote devices and services.

<u>Some of the Federal Departments that play primary roles in Telehealth are the:</u>

- Department of Veterans Affairs (VA),
- Federal Communications Commission (FCC),
- Department of Defense (DoD), and
- Department of Health and Human Services (HHS).
    - Office of the National Coordinator for Health Information Technology (ONC),

- Centers for Medicare and Medicaid Services (CMS),
- Health Resources and Services Administration (HRSA),
- Indian Health Service (IHS),
- Food and Drug Administration (FDA), and
- Agency for Healthcare Research and Quality (AHRQ)

TELEHEALTH FOR PUBLIC HEALTH EMERGENCIES & DISASTER MEDICAL RESPONSES

Rationale for the use of Telehealth during response and recovery efforts includes:

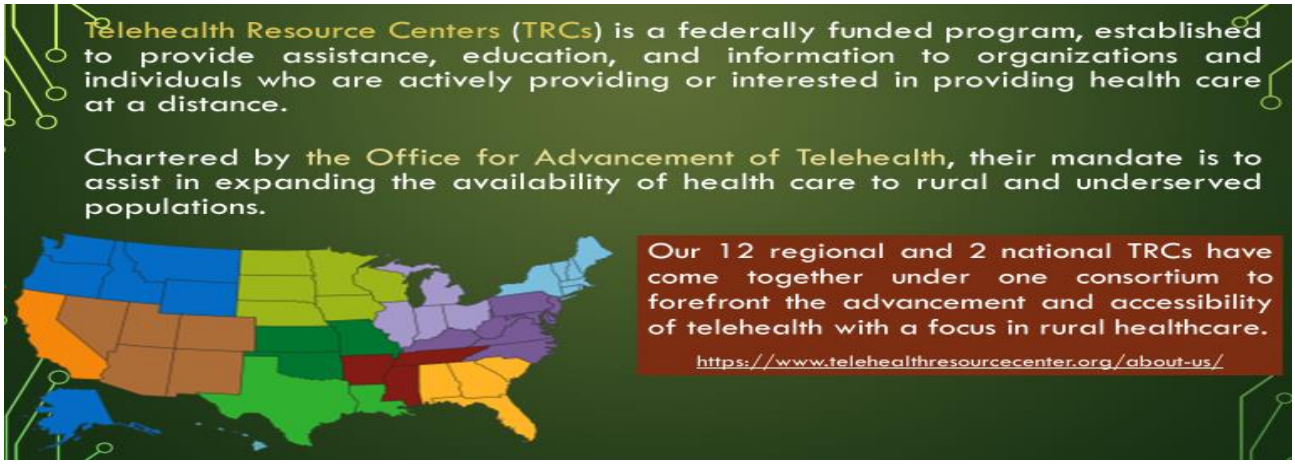
- Providing a more flexible response;
- Advancing consultation and medical expertise to proficiently impacted critically areas;
- Protecting responders from unnecessary exposure to danger;
- Refining public health emergencies and medical disasters management, responders, and support;
- Improving situational awareness;
- Reducing critical points of failure;
- Enhancing the interoperability and use of data and compensation mechanisms for providers;
- Offering specialist decision-making for triage and determination of appropriate investigation, treatment, or management;
- Providing increased accessibility to medical care for persons with disabilities and rural populations; and,
- Enhancing and strengthening patient and material accountability during patient rescue, transfer, and disposition.

REDUCING LEGAL BARRIERS

Large-scale public health emergencies and medical disasters that overwhelm local and State resources often require a response from healthcare professionals from other states or countries - directly or through telehealth. Because of the highly regulated nature of healthcare professions, in some cases there are significant perceived or actual legal barriers that might deter non-resident healthcare workers from providing Telehealth services during a public health emergency and disaster medical response.

THE EMERGENCY MANAGEMENT ASSISTANCE COMPACT (EMAC)

… a mutual aid agreement among States, allows States activate their own emergency response powers. When EMAC is triggered by a governor's declaration, it provides procedures and mechanisms for assistance, requests and response and provisions for liability, licensing, and reimbursement of certain healthcare professionals. EMAC states that a licensed person from a responding state is deemed licensed in the receiving state. EMAC is Congressionally-approved and enacted by legislatures in all states in substantially identical form.



REIMBURSEMENT

Teleherapy/Telemental health is reimburse in most states to include Medicaid and Medicare, but not for all disciplines.

- More than 40 states cover teletherapy under Medicaid and Medicare
- More than 20 states mandate that 3rd party insurers cover Telemental health equivalent to face-to-face.

WHAT IS HIPAA: PL 104-191

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. HIPAA required the Secretary of HHS to develop regulations protecting the privacy and security of certain health information. To fulfill this requirement, HHS published the HIPAA Privacy Rule and the HIPAA Security Rule.

Health and Human Services (**HHS**): Office for Civil Rights (OCR) has responsibility for enforcing the **Privacy and Security Rules** with voluntary compliance activities and civil money penalties.

HIPAA INSURANCE REFORM

HIPPA Insurance Reform (1997) changed the practice of health plans/insurers regarding portability and the continuity of health coverage by:

- Providing limitation on existing condition exclusions
- Prohibiting discrimination against individuals based on health status
- Helping individuals keep Health Insurance when they change jobs

- Preventing insurers from imposing pre-existing condition exclusions on new members when they have prior creditable coverage
- Guaranteeing that once employers or individuals purchase Health Insurance, those policies will be renewed

HIPPA TITLE II: ADMINISTRATIVE SIMPLIFICATION

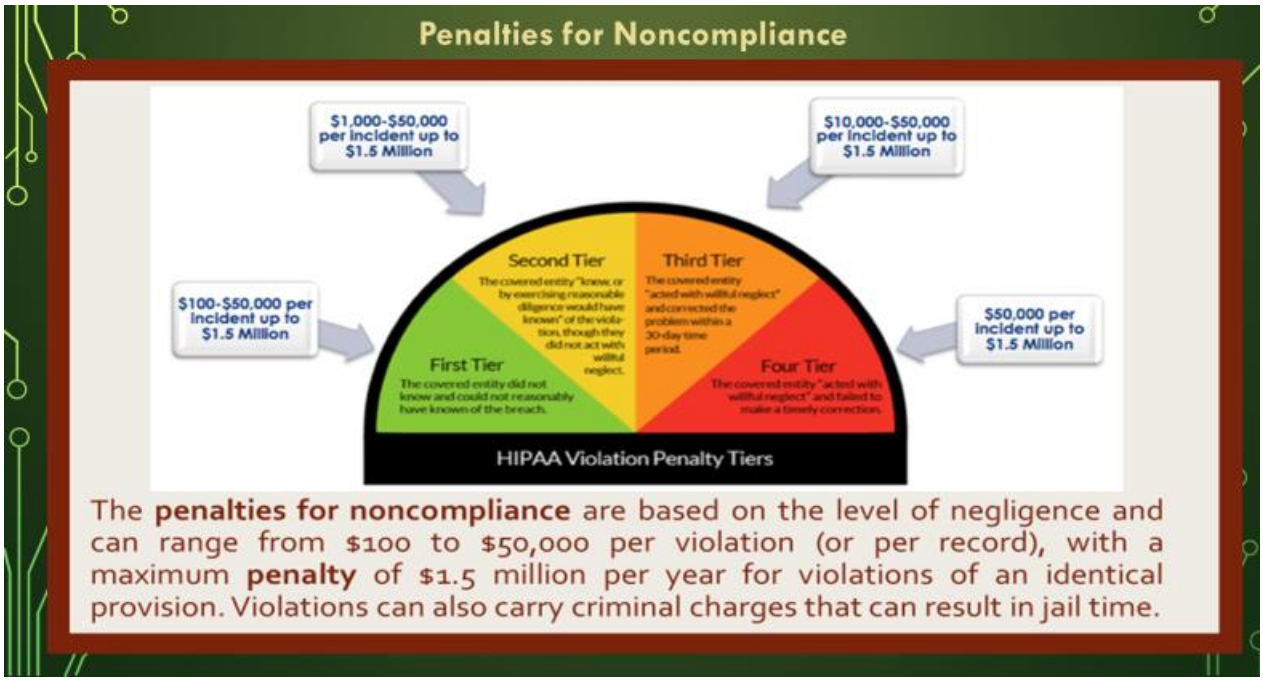
- **National Provider Identifier Standard.** Each healthcare entity, (individuals, employers, health plans and healthcare providers), must have a unique 10-digit *national provider identifier (*NPI) number.
- **Transactions and Code Sets Standard.** Healthcare organizations must follow a standardized mechanism for ***electronic data interchange*** (**EDI**) in order to submit and process insurance claims.
- **HIPAA Privacy Rule.** (Standards for Privacy of Individually Identifiable Health Information), establishes national standards to protect patient health information.
- **HIPAA Security Rule.** The Security Standards for the Protection of *Electronic Protected Health Information* sets standards for patient data security.
- **HIPAA Enforcement Rule.** This rule establishes guidelines for investigations into HIPAA compliance violations.

HIPAA, has two main purposes:

- to provide continuous health insurance coverage for workers who lose or change their job, and
- to reduce the administrative burdens and cost of healthcare by standardizing the electronic transmission of administrative and financial transactions.

Other goals include combating abuse, fraud and waste in health insurance and healthcare delivery and improving access to long-term care services and health insurance.

The **HIPAA Breach Notification Rule** within the Omnibus Rules requires covered entities and affected business associates to notify patients following a data breach.



In 2010, the **Federal Trade Commission** extended the breach notification rule and its enforcement to healthcare organizations not covered by HIPAA, including vendors of **electronic health records** (EHRs) and EHR-related systems. Covered entities must comply with **HIPAA security and privacy** regulations, and the **Federal Trade Commission Act**.

OCR further strengthened the HIPAA Security Rule in 2016 by bridging aspects of the ***National Institute of Standards and Technology's*** (**NIST**) Cybersecurity Framework to identify cybersecurity gaps and align HIPAA with national cybersecurity standards. **NIST** is a unit of the U.S. Commerce Department (National Bureau of Standards) that promotes and maintains measurement standards; and encourages and assist industry and science in the development and use these standards.

WHO IS AFFECTED BY HIPAA?

- **Covered Entities:** health entity who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
    - ***Health Care Providers***
    - ***Health Plans***
    - ***HealthCare Clearinghouses***
- **Business Associates:** a person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
- ***Third Party Vendors and Business Partners***

WHAT INFORMATION IS PROTECTED?

The HIPAA Privacy Rule protects all individually identifiable health information that is held or transmitted by a covered entity or a business associate. This information can be held in any form, including digital, paper or oral. This individually identifiable health information is also known as PHI.

List of 18 Personal Health Identifiers	
1. Names;	11. Certificate/license numbers;
2. Address, city, county, precinct, zip code;	12. Vehicle identifiers and serial numbers, license plate numbers;
3. Dates related to an individual (birth, admission, discharge, death, and age;	13. Device identifiers and serial numbers;
4. Phone numbers;	14. Web Universal Resource Locators (URLs);
5. Fax numbers;	15. Internet Protocol (IP) address numbers;
6. Electronic mail addresses;	16. Biometric identifiers, including finger and voice prints;
7. Social Security numbers;	17. Full face photographic images and any comparable images; and
8. Medical record numbers;	18. Any other unique identifying number, characteristic, or code
9. Health plan beneficiary numbers;	
10. Account numbers;	

Administrative Requirements of Privacy

Privacy Officer - must be appointed who is responsible for developing and implementing policies and procedures at a covered entity

- **Ongoing training** – all employees, volunteers and trainees must be trained on policies and procedures
- **Complaint process and sanctions –** method for individuals to make complaints concerning policies and procedures.
- **Policies, Procedures and Systems -** appropriate administrative, technical and physical safeguards in place to protect **PHI** and individual's.
- **Forms and documents** - to support individual participant rights and safeguard confidentiality of PHI
- **Records Retention Policy** (6 years)
- **Contracts with business associates** (written contract assuring information will be safeguarded)

WHAT IS THE SECURITY RULE

The **Security Ruled** defines the standards for safeguarding of PHI specifically in electronic form (ePHI) from unauthorized disclosure, destruction, or lost. *Privacy depends in part on security measures to ensure confidentiality.* The **Security Rule** requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

WHO IS COVERED BY THE SECURITY RULE

The Security Rule applies to **covered entities** as well as **business associates (**health plans, health care clearinghouses, and to any health care provider) who transmits health information in electronic form.
Any person organization that stores or transmits individually identifiable health information electronically.

WHAT IS PROTECTED BY THE SECURITY RULE

Electronic Protected Health information (ePHI) is individually identifiable health information relating to the past, present or future health condition of the individual in electronic form when it is stored, maintain, or transmitted.

ePHI include:

- Electronic Medical records (EMR)
- Electronic claims
- Computer databases with treatment history
- Digital Xray ease
- E-mail

Paper printouts of electronic information

THE SECURITY RULES REQUIREMENTS ORGANIZED INTO 3 GROUPS:

- **Administrative safeguards** - policies and procedures designed to show how the entity can comply with the Security Rules
- **Physical safeguards** -the controlling physical access to protect against inappropriate access to protect the data.
- **Technical safeguards** - the controlling of access to Computer Systems and the protection of communications containing PHI transmitted electronically over open networks.

ADMINISTRATIVE SAFEGUARDS

- **Security Management Process**. A covered entity must identify and analyze potential risks to **e-PHI**, and must implement reasonable and appropriate security measures that reduce risks and vulnerabilities.
- **Security Personnel.** A covered entity must designate a security official who is responsible for developing and implementing its security policies/procedures.
- **Information Access Management.** Consistent with the **Privacy Rule** standard limiting uses and disclosures of PHI, requires a covered entity to implement policies and procedures for authorizing access to **e-PHI** only when appropriate, based on the user / recipient's role (role-based access).
- **Workforce Training and Management.** A covered entity must train, and provide appropriate authorization and supervision of all workforce members who work with **e-PHI** regarding its security policies and procedures; and must have and apply appropriate sanctions against members who violate its policies and procedures.
- **Evaluation**. A covered entity must perform a periodic assessment of how well its security policies and procedures meet the requirements of the Security Rule.

PHYSICALS SAFEGUARDS

1. **Facility Access Control.** limit physical access to **ePHI**.
   - ***Contingency Operations****:* physical security and access in disaster or emergency.
   - ***Facility Security Plan:*** safeguards to protect facility and **ePHI** from unauthorized physical actions.
   - ***Access Control and Validation Procedures:*** controlling and validating access based role or function
   - ***Maintenance Records:*** record physical changes to security (repairs and removals)
2. **Workstation Use:** ensure employees' workstations are physically and virtually safe.
3. **Workstation Security.** physical protect of workstation from unauthorized users.
4. **Device and Media Controls.** all items storing electronic information must be properly handled, documented, saved, disposed and accounted for.
   - **Disposal:** procedures on how to properly dispose or destroy devices bearing ePHI.
   - **Media Re-Use:** ensuring that **ePHI** is completely removed from devices before using discarding or reuse for another purpose.
   - **Accountability:** document hardware's whereabouts and identify of responsible party.
   - **Maintain Data Backup and Storage:** ensure updated and accurate **ePHI** is accessible on demand.

TECHNICAL SAFEGUARDS

. . . technology policies and procedures for the use of **ePHI** and access control.

1. **Access Control:** system permissions are granted on a need-to-use basis.
   - **A *Unique User Identification*** to track and limit employee activity.
   - ***Automatic Logoff*** after a set amount of inactivity, to secure employee access .
   - ***Emergency Access Procedure*** for obtaining necessary **ePHI**.
   - ***Encryption and Decryption*** for **ePHI** while in transit, at rest and in use.
2. **Audit Controls:** system oversight to review and record all **ePHI** activity.
3. **Integrity:** protection of **ePHI** against unauthorized alterations or deletion with electronic mechanisms to prove it.
4. **Person or Entity Authentication:** verification of individual access to **ePHI**. (PINs, passwords, keycards, biometrics, etc.)
5. **Transmission Security:** guarding **ePHI** from unauthorized access while in transit - sending information over secure networks and platforms.

HITECH Act
Health Information Technology for Economic and Clinical Health

HITECH Act of 2009 provides HHS with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange.

MAJOR PURPOSES OF HITECH ACT:

- expanded the use of **Electronic Health Records** (**EHRs**)
- strengthened the **HIPAA Privacy and Security Rules** with respect to electronic health and medical records
- improve efficiencies and reduce costs in the Healthcare System
- stimulate the economy
- Provide guidance to **covered entities and business associates** in the implementation of technical safeguards to ensure the confidentiality, integrity, and availability of **PHI**.

WHO OR WHAT IS AFFECTED BY HITECH?

Covered Entities and Business Associations to include:

- Plans and health care clearinghouses
- business associates subcontractors/vendors
- federal healthcare contractors and federal agencies that use healthcare IT systems to exchange health data.

All of the above are now subject to numerous security requirements, including technical, physical and policy-related rules.

LAWS / REGULATIONS / STANDARDS/ GUIDELINES

Laws: products of written statutes, passed by either the U.S. Congress or state legislatures.
Regulations: standards and rules adopted by administrative agencies that govern how laws will be enforced. Although they are not laws, regulations have the force of law, because they are adopted under authority granted by statutes, and often include penalties for violations.

Standards: reflect relevant legal requirements which are enforceable under the respective state and federal regulation. **Professional Standards:** reflects the minimum criterion, specification, benchmark, requirements, guidelines, etc. of professional behavior and ethical conduct relative to prevention, assessment, diagnosis, and treatment of mental, emotional, behavioral, and addiction disorders.

Procedures: authorized, endorsed, or permissible way of doing something, that involves a course of action intended to achieve specific results in the delivery of healthcare.

Guidelines: suggest or recommend specific activities, behaviors, or conduct. Guidelines are intended to:

- educate and to inform;
- facilitate the continued systematic development of the profession
- ensure a high level of professional practice
- stimulate debate and research

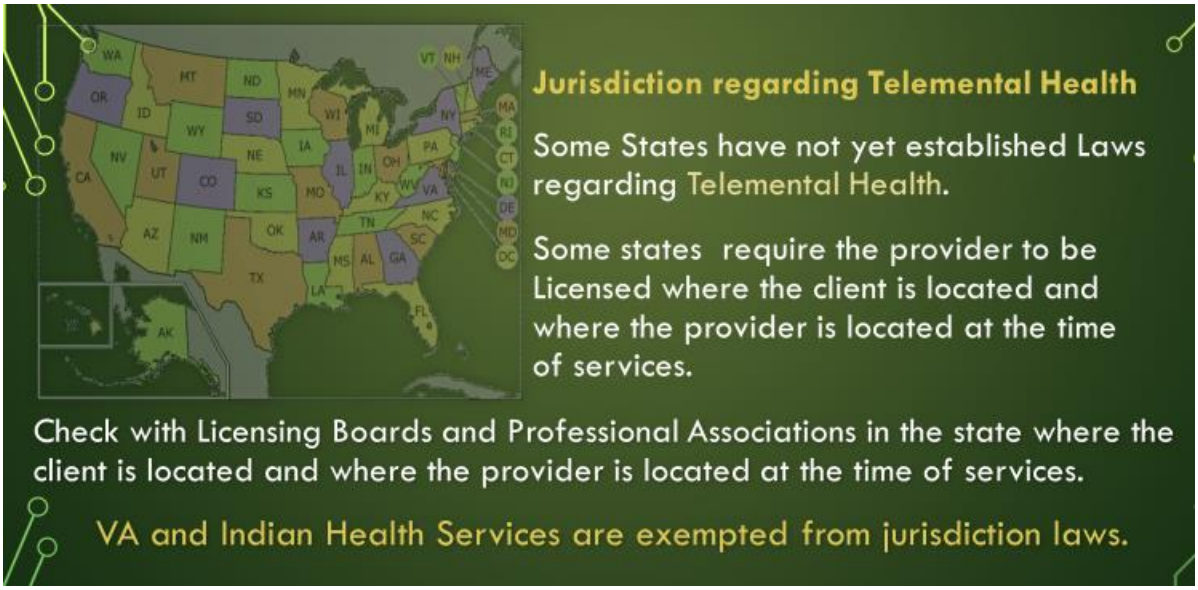
Guidelines are not intended to be mandatory or exhaustive; and may not be applicable to every professional or clinical situation.

Professional Guidelines intended to apply current standards of professional practice when utilizing telecommunication technologies as a means of delivering professional mental health services.
Professional Guidelines are not:

- to be promulgated as a means of establishing the identity of a particular group or specialty area; or with the purpose of excluding any professional from practicing in a particular area.
- intended to change any scope of practice or define the practice of any group of psychologists.
- definitive or intended to take precedence over professional judgment.

Adapted from the American Psychological Association: Guidelines for the Practice of Telepsychology (2019)

The delivery of behavioral/mental health services via technology must meet the same ethical and professional standards of care as face-to-face services.



STATE TELETHERAPY REGULATIONS

Alabama Requirements for TeleMental Health
CODE OF ETHICS AND STANDARDS OF PRACTICE http://abec.alabama.gov/PDFs/Code_Ethics_Nov-09.pdf
A.12. TECHNOLOGY APPLICATIONS

a. Use of Technology. When technology applications are used in counseling services, licensed professional counselors must ensure that: (1) the client is intellectually, emotionally, and physically capable of using the technology application; (2) the technology application is appropriate for the needs of the client; (3) the client understands the purpose and operation of the technology applications; and (4) a follow-up of client use of a technology application is provided to correct possible misconceptions, discover inappropriate use, and assess subsequent needs.
b. Explanation of Limitations. Licensed professional counselors ensure that clients are provided information as a part of the counseling relationship that adequately explains the limitations of technology applications.
c. Access to Technology Applications. Licensed professional counselors provide for equal access to technology applications in counseling services. (See A.2.a.).
d. Distance Technology Counseling Services. Licensed professional counselors who employ distance technology for counseling services must observe and demonstrate all aspects of client rights and welfare, client confidentiality, professional responsibility (including relationships with other professionals), procedures for assessment, and resolution of ethical issues reflected in the Code of Ethics and Standards of Practice adopted by the Alabama Board of Examiners in Counseling. **Addressing and resolving any disparities between ethical or legally-mandated practices required in face-to-face counseling services versus distance technology counseling services is the ethical duty of the licensed professional counselor.** Ethical standards for a licensed professional counselor who employs distance technology counseling services shall apply to client care and public protection regardless of the destination point of such counseling services, unless otherwise prohibited by law. (See A.3.a.).

FLORIDA REQUIREMENTS FOR TELEMENTAL HEALTH

Telehealth Provider: an individual who provides a health care service using telehealth, which includes, but is not limited to, a licensed physician, podiatrist, optometrist, nurse, nurse practitioner, pharmacist, dentist, chiropractor, acupuncturist, midwife, speech language pathologist, audiologist, occupational therapist, radiological personnel, respiratory therapist, dietician, athletic trainer, orthotist, pedorthist, prosthetist, electrologist, massage therapist, medical physicist, optician, hearing aid specialist, physical therapist, psychologist, clinical social worker, **mental health counselor, psychotherapist, marriage and family therapist**, behavior analyst, basic or advanced life support service, or air ambulance service.
Telehealth provider: an individual licensed under a multi-state health care licensure compact of which Florida is a member state or an individual who obtains an out-of-state telehealth registration.

Telehealth: the use of synchronous or asynchronous telecommunications technology by a telehealth provider to provide health care services, including, but not limited to, assessment, diagnosis, consultation, treatment, and monitoring of a patient; transfer of medical data; patient and professional health-related education; public health services; and health administration.

Telehealth does not include audio-only telephone calls, e-mail messages, or fax transmissions.

Florida Out of State Registration and Licensure Exceptions

Out-of-state health care professionals, without a Florida license, may use telehealth to deliver health care services to Florida patients if they register with the Department of Health or the applicable board, meet certain eligibility requirements, and pay a fee. To obtain an out-of-state registration the health care professional must:

- Complete an application;
- Maintain an active, unencumbered license issued by another state that is substantially similar to the corresponding Florida license;
- Not have been the subject of disciplinary action relating to his or her license for the previous 5 years;
- Designate a registered agent for service of process in Florida;
- Maintain professional liability coverage, that includes coverage for telehealth services to patients in Florida, in amounts equal to or greater than what are required for a Florida-licensed practitioner;
- Not open an office in Florida or provide in-person health care services to patients located in Florida.
- Only use a Florida-licensed pharmacy or a registered nonresident pharmacy or outsourcing facility to dispense medicinal drugs to patients located in Florida. (Pharmacists only)
-

Florida Licensure Exception.

A health care professional who is not licensed to provide health care services in Florida, but who holds an active license to provide health care services in another state, may provide health care services using telehealth to a patient located in Florida without a Florida license and without an out-of-state registration, if the services are provided:

(1) in response to an emergency medical condition; or

(2) in consultation with a Florida-licensed health care professional who has ultimate authority over the diagnosis and care of the patient.

GEORGIA REQUIREMENTS FOR TELEMENTAL HEALTH

- Prior to the delivery of clinical TeleMental Health, the licensee shall have obtained a minimum of six (6) continuing education hours.
- Prior to the delivery of supervision via Telemental health, the supervisor shall have obtained a minimum of nine (9) hours of continuing education.
    - The continuing education hours may include the same eight (8) categories identified under "Training for Licensee", plus three (3) hours in the category of: Supervising TeleMental Health Therapy.

I. Internet use dependency and psychological problems
II. Research in Telemental Health
III. Intake and Assessment
IV. Delivery Methods
V. Theory Integration
VI. Termination
VII. Risk Management
VIII. Business of Telemental Health

Mississippi - Rule 7.5: Practice of Distance Professional Services

Any person that provides counseling or supervision services through the means of Distance Professional Services must hold a license in good standing in both the location where services are provided by the professional as well as in the location of the recipient of the services and must also hold the Board Certified-TeleMental Health (BC-TMH) credential or its equivalent as recognized by the Center for Credentialing and Education, Inc. (CCE) or the National Board of Certified Counselors.

Distance Professional Services must be performed in accordance with these Rules and Regulations, the current American Counseling Association’s Code of Ethics, the current National Board for Certified Counselors Policy Regarding the Provision of Distance Professional Services, and Mississippi and Federal law.

Title 46: **PROFESSIONAL AND OCCUPATIONAL STANDARDS REVISED**

505. Teletherapy Guidelines for Licensees

A. This chapter defines and establishes minimum standards for the delivery of the practice of counseling, marriage and family therapy services and psychotherapeutic services using technology-assisted media. Teletherapy references the provision of counseling and psychotherapy services from a distance and is consistent with the same standards of practice as those in in-person settings.

B. Teletherapy is defined as a method of delivering counseling and marriage and family therapy/psychotherapy services as prescribed by R.S. 37:1116 using interactive technology-assisted media for the rendering of professional marriage and family therapy and psychotherapy services, limited to prevention, assessment, diagnosis, and treatment of mental, emotional, behavioral, relational, and addiction disorders to individuals, couples, and families, singularly or in groups that enables a licensee and a client separated by distance to interact via synchronous video and audio transmissions.

C. The board recognizes that safe and effective practices in teletherapy require specific training, skills, and techniques and has set forth the following regulatory standards to ensure competence and safety. This rule shall not be construed to alter the scope of practice of any licensee or authorize the delivery of services in a setting, or in a manner, not otherwise authorized by law.

Nothing in this section shall preclude a client from receiving in-person counseling or marriage and family therapy/psychotherapy services after agreeing to receive services via telehealth. Teletherapy shall be delivered in real-time (synchronous) using technology-assisted media such as videoconferencing and telephone through computers and mobile devices. The use of asynchronous modalities (e-mail, chatting, texting, and fax) is not appropriate and shall not be used for teletherapy, except in a crisis to ensure the client's safety and stability.

D. Licensees shall provide services consistent with the jurisdictional licensing laws and rules in the jurisdiction in which he/she is located. Licensees providing teletherapy services to clients outside of Louisiana must comply with the regulations in the state in which the client is located at the time of service. The licensee shall contact the licensing board in the state where the client is located and document all relevant regulations regarding teletherapy.

A nonresident of Louisiana who wishes to provide telemental health services in Louisiana must be licensed by the Board. Treatment, consultation, and supervision utilizing technology-assisted services will be held to the same standards of practice as those in traditional (in-person) settings.

E. Teletherapy is a specialty area and requires board approval. Licensees who may provide teletherapy must meet the following requirements:
   1. The licensee must be licensed in Louisiana.
   2. The licensee must be licensed in the state where the client is located.
   3. The licensee must have been practicing for at least 1 year
   4. The Licensee must complete either option below.
      a. Graduate-Level Academic Training. At least 1 graduate-level academic course (equivalent to a 3-credit hour semester/45 clock hours) in telemental health counseling.
      b. Professional Training. A minimum of 9 synchronous clock hours. The presenter shall meet continuing education standards established by the board. Teletherapy education/training shall include but is not limited to:
         I. Appropriateness of Teletherapy
         II. Teletherapy Theory and Practice
         III. Theory Integration
         IV. Modes of Delivery
         V. Risk Management
         VI. Managing Emergencies
         VII. Legal/Ethical Issues

   5. Licensees privileged in teletherapy must accrue 3 clock hours of continuing education during each renewal period.

F. At the onset of teletherapy, the licensee shall obtain verbal and/or written informed consent from the client and shall document such consent in the client's record.
   1. Electronic signature(s) and date may be used in the documentation of informed consent.
   2. Provisions of informed consent for teletherapy services shall include:

a. Mode and parameter of technology-assisted media(s), and technical failure
b. Scheduling and structure of teletherapy
c. Risks of teletherapy
d. Privacy and limits of confidentiality
e. Contact between sessions
f. Emergency Plan
g. Consultation and coordination of care with other professionals
h. Referrals and termination of Services
i. Information and record keeping
j. Billing and third-party payors
k. Ethical and legal rights, responsibilities, and limitations within and across state lines and/or international boundaries.

G. The licensee shall provide each client with his/her declaration or statement of practice on file with the Board office.

H. At the onset of each session the licensee shall verify and document the following:
1. The identity and location of the licensee and the client. If the client is a minor, the licensee must also verify the identity of the parent or guardian consenting to the minor's treatment. In cases were conservatorship, guardianship, or parental rights of the minor client have been modified by the court, the licensee shall obtain and review a copy of the custody agreement or court order before the onset of treatment.
2. The location and contact information of the emergency room and first responders nearest to the client's location

I. The licensee shall determine if the client may be properly diagnosed and/or treated via teletherapy services and shall affirm that technology-assisted media are appropriate for clients with sensory deficits. The licensee shall affirm the client's knowledge and use of selected technology-assisted media(s) (i.e., software and devices). Clients who cannot be diagnosed or treated properly via teletherapy services shall be dismissed and treated in-person, and/or properly terminated with appropriate referrals.

The licensee shall use technology assisted media(s) that is in compliance with HIPPA and HiTECH standards. The licensee shall not use social media platforms or functions (tweets, blogs, networking sites, etc.) in the delivery of teletherapy, and shall not reference clients generally or specifically on such formats.

J. Policies and procedures for the documentation, maintenance, access, transmission and destruction of record and information using technology assisted media shall be consistent with the standards for in-person services. Services must be accurately documented in teletherapy services, denoting the distance between the licensee and the client. Documentation shall include verification of the licensee's and client's location, type of service(s) provided the date of service, and duration of service.
The licensee shall inform clients of how records are maintained, type of encryption and security assigned to the records, and how long archival storage is maintained.

K. Teletherapy Supervision is defined as a method delivering counseling and clinical marriage and family therapy supervision as prescribed by R.S. 37:1116 using technology-assisted media that enables a supervisor and a supervisee separated by distance to interact via synchronous video and audio transmissions.
1. Teletherapy supervision may include but is not limited to, the review of case presentation, audio tapes, video tapes, and observation to promote the development of the practitioner's clinical skills.
2. Teletherapy supervision shall be provided in compliance with the same ethical and regulatory standards as in-person supervision.
3. The supervisor shall inform supervisees of the potential risks and benefits associated with telesupervision.
4. The supervisor shall determine if the supervisee may be properly supervised via teletherapy supervision. Supervisees who cannot be supervised via teletherapy supervision shall be restricted to in-person supervision, and/or properly terminated with appropriate referrals
5. The Supervisor shall affirm the supervisee's knowledge and use of selected technology-assisted media(s) (i.e., software and devices).
6. The Supervisor shall use technology assisted media(s) that is in compliance with HIPPA and HiTECH standards.
7. The Supervisor shall not use social media platforms or functions (tweets, blogs, networking sites, etc.) in the delivery of teletherapy supervision, and shall not reference supervisee generally or specifically on such formats.

Ethical Standards Governing Teletherapy

ACA Ethical Standards
NBCC Ethical Standards
AMFT Ethical Standards
AMHA Ethical Standards

ACA ETHICAL STANDARDS

Section H: Distance Counseling, Technology, and Social Media
Counselors must:

- Be knowledgeable about the laws governing distance counseling and social media.
- Only utilize distance counseling after gaining competence through training and supervised experience in this specialty area.
- Inform clients about the limits of confidentiality and potential Internet interruptions due to the nature of technology.
- Understand the benefits and drawbacks related to distance counseling
- Utilize a professional presence if they choose to use social media platforms
- Avoid disclosing confidential information through social media.
- Utilize informed consent to explain the boundaries of social media.

H.1.a.Knowledge and Competency
Counselors who engage in the use of distance counseling, technology, and/or social media develop knowledge and skills regarding related technical, ethical, and legal considerations (e.g., special certifications, additional course work).

H.1.b. Laws and Statutes
Counselors who engage in the use of distance counseling, technology, and social media within their counseling practice understand that they may be subject to laws and regulations of both the counselor's practicing location and the client's place of residence.
Counselors ensure that their clients are aware of pertinent legal rights and limitations governing the practice of counseling across state lines or international boundaries.

H.2.a. Informed Consent and Disclosure
Clients have the freedom to choose whether to use distance counseling, social media, and/or technology within the counseling process. In addition to the usual and customary protocol of informed consent between counselor and client for face-to-face counseling.

The following issues, unique to the use of distance counseling, technology, and/or social media, are addressed in the informed consent process:

- distance counseling credentials, physical location of practice, and contact information;
- risks and benefits of engaging in the use of distance counseling, technology, and/or social media;
- possibility of technology failure and alternate methods of service delivery;
- anticipated response time;
- emergency procedures to follow when the counselor is not available;
- time zone differences;
- cultural and/or language differences that may affect delivery of services; possible denial of insurance benefits; and
- social media policy.

H.2.b. Confidentiality Maintained by the Counselor
Counselors acknowledge the limitations of maintaining the confidentiality of electronic records and transmissions. They inform clients that individuals might have authorized or unauthorized access to such records or transmissions (e.g., colleagues, supervisors, employees, information technologists).

H.2.c. Acknowledgment of Limitations
Counselors inform clients about the inherent limits of confidentiality when using technology. Counselors urge clients to be aware of authorized and/or unauthorized access to information disclosed using this medium in the counseling process.

H.2.d. Security
Counselors use current encryption standards within their websites and/or technology-based communications that meet applicable legal requirements. Counselors take reasonable precautions to ensure the confidentiality of information transmitted through any electronic means.

H.3. Client Verification
Counselors who engage in the use of distance counseling, technology, and/or social media to interact with clients take steps to verify the client's identity at the beginning and throughout the therapeutic process. Verification can include, but is not limited to, using code words, numbers, graphics, or other nondescript identifiers.

H.4.a. Benefits and Limitations
Counselors inform clients of the benefits and limitations of using technology applications in the provision of counseling services. Such technologies include, but are not limited to, computer hardware and/or software, telephones and applications, social media and Internet-based applications and other audio and/or video communication, or data storage devices or media.

H.4.b. Professional Boundaries in Distance Counseling
Counselors understand the necessity of maintaining a professional relationship with their clients. Counselors discuss and establish professional boundaries with clients regarding the appropriate use and/or application of technology and the limitations of its use within the counseling relationship (e.g., lack of confidentiality, times when not appropriate to use).

H.4.c. Technology-Assisted Services
When providing technology-assisted services, counselors make reasonable efforts to determine that clients are intellectually, emotionally, physically, linguistically, and functionally capable of using the application and that the application is appropriate for the needs of the client. Counselors verify that clients understand the purpose and operation of technology applications and follow up with clients to correct possible misconceptions, discover appropriate use, and assess subsequent steps.

H.4.d. Effectiveness of Services
When distance counseling services are deemed ineffective by the counselor or client, counselors consider delivering services face-to-face. If the counselor is not able to provide face-to-face services (e.g., lives in another state), the counselor assists the client in identifying appropriate services.

H.4.e. Access
Counselors provide information to clients regarding reasonable access to pertinent applications when providing technology-assisted services.

H.4.f. Communication Differences in Electronic Media
Counselors consider the differences between face-to-face and electronic communication (nonverbal and verbal cues) and how these may affect the counseling process. Counselors educate clients on how to prevent and address potential misunderstandings arising from the lack of visual cues and voice intonations when communicating electronically.

H.5.c. Electronic Links
Counselors regularly ensure that electronic links are working and are professionally appropriate.

H.5.d. Multicultural and Disability Considerations
Counselors who maintain websites provide accessibility to persons with disabilities. They provide translation capabilities for clients who have a different primary language, when feasible. Counselors acknowledge the imperfect nature of such translations and accessibilities.

H.6.a. Virtual Professional Presence
In cases where counselors wish to maintain a professional and personal presence for social media use, separate professional and personal web pages and profiles are created to clearly distinguish between the two kinds of virtual presence.

H.6.b. Social Media as Part of Informed Consent
Counselors clearly explain to their clients, as part of the informed consent procedure, the benefits, limitations, and boundaries of the use of social media.

H.6.c. Client Virtual Presence
Counselors respect the privacy of their clients' presence on social media unless given consent to view such information.

H.6.d. Use of Public Social Media
Counselors take precautions to avoid disclosing confidential information through public social media.

PRACTICE GUIDELINES FOR VIDEO-BASED ONLINE MENTAL HEALTH SERVICES
American Telemedicine Association

Telemental health, like telemedicine, is an intentionally broad term referring to the provision of mental health care from a distance.

Telemental health (**TMH**) includes mental health assessment, treatment, education, monitoring, and collaboration.

Prerequisite Conditions
Prior to utilizing telemedicine the professional should ensure:

- That she/he have received training on how to conduct the a counseling session via telemedicine
- She/he are available to implement healthcare, identify where medical records generated by the visit are to be transmitted for future access, and provide or arrange back up, follow up, and emergency care to the patient
- She/he can provide or arrange periodic testing and maintenance of all telemedicine equipment
- That she/he has access to those portions of the patient's medical record pertinent to the delivery of services

Internet-based Telemental Health Models of Care

Sources of Technology: Personal computers, Internet, mobile devices and videoconferencing software/equipment.

- Commercial software downloaded from the Internet is used to provide direct care to patient at home or other non-institutional setting.

- Internet-based web sites serve as a conduit or portal for professionals and patients seeking treatment online. *Mental health practitioners* sign up with one/more web-based company and provide a professional profile that can be viewed online by prospective patients.

- Outsourcing - many companies contract with professionals, hospitals and other institutions to provide telemental healthcare. Some use technology maintained and provided by the company.

ATA CORE STANDARDS FOR **TELEMENTAL HEALTH**

ATA has developed core standards for telemedicine operations for:
A. Clinical Guidelines
B. Technical Guidelines
C. Administrative Guidelines

A. CLINICAL GUIDELINES

B. **Professional and Patient Identity and Location**
At the beginning of a video-based mental health treatment (i.e., unless subsequent encounter warrant) with a patient, the following essential information shall be verified:

1. Provider and Client Identity Verification
2. Provider and Client Location Documentation
3. Provider and Client Contact Information Verification
4. Verification of Expectations Regarding Contact Between Sessions

B. **Patient Appropriateness for Videoconferencing-based Telemental Health**

To date, no studies have identified any patient subgroup that does not benefit from, or is harmed by, mental healthcare provided through remote videoconferencing.

1. The clinician should consider the client's expectations and level of comfort with homebased care to determine the appropriateness of videoconferencing.

C. **Informed Consent**

Document the provision of consent to include all information :

- Scheduling
- Record Keeping
- Confidentiality
- Mandatory Reporting
- Procedures for Coordination of Care with other professionals
- Protocol for Contact Between Sessions
- Emergency Plan
- Conditions for Termination of Services and Referrals
- Potential Risks of counseling / use of technology / technical failure
- Nature of videoconferencing
- Billing

D. Physical Environment

- Both provide professional for standard **room/environment**.
- Ensure privacy so discussion cannot be overheard
- Both parties shall be made aware of and agree to the presence of other persons
- Seating and lighting should be tailored to allow maximum comfort
- Maximize clarity and visibility of each other, with cameras secure (stable platform, placed at the same eye elevation, etc).

E. **Emergency Management**

1. Education and Training
2. Jurisdictional Mental Health Involuntary Hospitalization Laws
3. Patient Safety when Providing Services in a Setting with Immediately Available Professionals
4. Patient Safety when providing Services in a Setting without Immediately Available Professional Staff
5. Patient Support Person and Uncooperative Patients
6. Transportation
7. Local Emergency Personnel

F. **Communication and Collaboration with the Treatment Team**

- Secure client Consent to Consult/Collaborate for coordination of care
- Arrange for appropriate/regular consults with other professionals involved in client care.
- When providing services to clients in settings without clinical staff immediately available, develop collaborative relationships with other professionals (client's PCP, Psychiatrist, etc.).

G. **Medical Issues**

- Professional should be familiar with whom the client is receiving medical services
- Professional should be familiar with the patient's prescription - in case of side effects, elevation in symptoms, and/or medication noncompliance
- Client should have an active relationship with a prescribing professional in their physical vicinity

H. **Referral Resources**

Professional shall be familiar with local mental health resources should a referral for additional mental health or other appropriate services are needed.

I. **Community and Cultural Competency**

- Professionals shall be culturally competent to deliver services to the populations that they serve
- Awareness of the client's language, ethnicity, race, age, gender, sexual orientation, geographical location, and socioeconomic and cultural backgrounds
- Knowledge of the community where the client resides, recent events and cultural traditions of that community

B. TECHNICAL GUIDELINES

A. Videoconferencing Application

All efforts shall be taken to use video conferencing applications that have the appropriate verification, confidentiality, and security parameters of HIPAA guidelines.

Video software platforms should not be used when they include social media functions that allows others to enter at will.

A. Device Characteristics
Cameras with pan, tilt, and zoom for maximal flexibility for viewing

Computer and/or mobile device shall have up-to-date antivirus software and firewall, with latest security patches and updates (third party applications that may be utilized).

Utilize device management software to provide consistent oversight of applications, device and data configuration and security devices used.

B. Connectivity

Videoconferencing software programs should provide a bandwidth of 384 Kbps or higher in each of the downlink and uplink directions; with a minimum of 640 X 360 resolution at 30 frames per second.

Video conferencing software (cable of adapting to changing bandwidth environments without losing connectivity), video/audio hardware, and software/hardware configuration considerations*

Pre-testing connection before starting, to ensure sufficient quality of link.

Use the most reliable connection method to access the Internet. Use wired connections if available (e.g., Ethernet).

D. Privacy

Special attention should be placed on the relative privacy of information being communicated over such technology.

- The videoconference software should be capable of blocking the provider's caller ID.

- Efforts shall be taken to make audio and video transmission secure by using point-to-point encryption that meets recognized standards.

- Professional should adequately restricted access to any patient contact information stored on mobile devices.

- Mobile devices shall require a passphrase or equivalent security before accessing device, with multi-factor authentication when available.

- Mobile devices should be configured to utilize an *inactivity timeout function* that requires a passphrase or re-authentication to access the device after exceeding the timeout threshold (not exceed 15 minutes).

- Mobile devices should be kept in the possession of the professional when traveling or in an uncontrolled environment.

- Unauthorized persons shall not be allowed to use the device to access sensitive applications or network resources; or have access to sensitive information stored on the device.

- Clinicians should have the capability to remotely disable or wipe their mobile device in the event it is lost or stolen.

- Videoconference software shall not allow multiple concurrent sessions to be opened by a single user.

- Session logs stored in 3rd party locations (i.e., not on clients' or Clinicians' access device) shall be secure.

- Protected health information and other confidential data shall only be backed up to or stored on secure data storage locations.

- Clinicals should monitor whether any of the videoconference transmission data is intentionally or inadvertently stored on the client or Clinical's computer hard drive.

- Pre-boot authentication should be used.

- Professionals and patients shall discuss intentions to record services, how information will be stored, and how privacy will be protected. Recordings should be encrypted for maximum security.

  Access to the recordings shall be restricted to authorized users only and should be streamed to protect accidental/unauthorized file sharing/transfer.

- The professional shall discuss with the patient his/her policy for sharing any portions of this information with the general public.

- Written agreements pertaining privacy, access, sharing, transferring information can protect both the patient and the professional.

C. ADMINISTRATIVE GUIDELINES

A. Qualification and Training of Professionals

- Establish guidelines for proper conduct of videoconferencing to both professionally supervised settings and those without available clinical staff.

- Determine if there are site-specific credentialing requirements where the patient is located.

- Provide services consistent with the jurisdictional licensing laws and rules for respective profession – in both the jurisdiction in which the professional is practicing and the jurisdiction where the client is receiving care.

- Clinicians should contact their licensing board to review practice regulations before starting any provision of telemental health services.

- Clinicians should contact their licensing board relevant to the client's location during treatment, to determine service jurisdiction and what, if any, restrictions exist.

B. **Documentation and Record Keeping**

- Clinicians shall maintain an electronic record for each client.

- A treatment plan based upon an assessment of the client's needs should be developed and documented.

- Services should be accurately documented as remote (telehealth) services and include dates, duration and type of service(s) provided.

- Documentation shall comply with applicable jurisdictional and federal laws and regulations.

- All communications with the client (e.g., written, audiovisual, or verbal) shall be documented in the client's record and stored in compliance with relevant government regulations.

- Requests for access to records shall require written authorization from the client indicating the types of data/information to be released.

- If storing the audiovisual data from the sessions, these cannot be released without the client authorization.

- All billing and administrative data related to the client shall be secured to protect confidentiality.

C. **Payment and Billing**

- Prior to the commencement of initial services, the client shall be made aware of any and all financial charges that may arise from the services to be provided.

- Arrangement for payment should be completed prior to the commencement of services.

PURPOSE OF THESE GUIDELINES

The purpose of these guidelines is to assist practitioners in pursuing a sound course of action to provide effective and safe medical care that is founded on current information, available resources, and patient needs.

The guidelines are not meant to be unbending requirements of practice and they are not designed to, nor should they be used to, establish a legal standard of care.

The American Telemedicine Association advises against the use of these guidelines in litigation in which the clinical decisions of a practitioner are called into question.

REFERENCE

Alabama LPC Board of Examiners

Florida LPC Board of Examiners

Georgia LPC Board of Examiners

Louisiana LPC Board of Examiners

Mississippi LPC Board of Examiners

American Telemedicine Association: PRACTICE GUIDELINES FOR VIDEO-BASED ONLINE MENTAL HEALTH SERVICES

Associated Underwriters Insurance - https://auiinfo.com/telemental-health-benefit-insight/

Federal Communications Commission

Public Law 109-417 Pandemic and All-Hazards Preparedness Act