Distance Counseling, HITECH, and HIPAA: Navigating Compliance, the Law, and Ethics

AMERICAN COUNSELING ASSOCIATION

MARLENE M. MAHEU, PH.D.
Mmaheu@telehealth.org
Executive Director
TeleMental Health Institute

POLL QUESTION

WHO ARE YOU?
Disclaimer

• I am an MFT and clinical psychologist, not an attorney, physician or Information Technology specialist. I am agnostic in terms of associations and companies hired. At TMHI, we pull the best of what we see in all associations as they relate to legal, ethical and risk management related to using technology. My main focus is video-based care and not email.

• My goal is educational only. The information I present is my best attempt to bring you timely and relevant information in a rapidly evolving area. I therefore make no warranty, guarantee, or representation as to the accuracy or sufficiency of the information contained in my training.

• You are encouraged to seek specific advice related to your circumstance from your qualified authorities.

Benefits of Telehealth

• Increased client satisfaction
• Decreased travel time
• Decreased travel, child & elder-care costs
• Increased access to underserved populations
• Improved accessibility to specialists
• Reduced emergency care costs
• Faster decision-making time
• Increased productivity / decreased lost wages
• Improved operational efficiency

• Efficacy is on par with in-person care for many groups
• Decreased hospital utilization
Recent Supporting Research

- Godleski, Darkins & Peters reported in April of 2012 that hospital utilization in psychiatric populations at the Veterans Administration were decreased by an average of 25% since the use of telehealth. It is worthy of note, however, that:
  - This study focused on clinic-based, high-speed videoconferencing and did not include any home telehealth encounters. Mental health patients were referred for telecare by clinicians. Typically, telemental health services were provided remotely at community-based outpatient clinics by mental health providers of all disciplines located at larger parent VA hospital facilities.
Recent Supporting Research

Backhaus and colleagues (May, 2012) reported in their abstract of a meta-analysis that:

- 821 potential articles were identified, and 65 were selected for inclusion.
- The results indicate that VCP is feasible, has been used in a variety of therapeutic formats and with diverse populations, is generally associated with good user satisfaction, and is found to have similar clinical outcomes to traditional face-to-face psychotherapy.

— Videoconferencing psychotherapy: A systematic review. Backhaus, Autumn; Agha, Zia; Maglione, Melissa L.; Repp, Andrea; Ross, Bridgett; Zuest, Danielle; Rice-Thorp, Natalie M.; Lohr, James; Thorp, Steven R. Psychological Services, Vol 9(2), May 2012, 111-131. doi: 10.1037/a0027924

General Informed Consent Issues
ACA Code of Ethics (2005)

A.12.a. Benefits and Limitations

• Counselors inform clients of the benefits and limitations of using information technology applications in the counseling process and in business/billing procedures.

• Such technologies include, but are not limited to, computer hardware and software, telephones, the World Wide Web, the Internet, online assessment instruments and other communication devices.
### ACA Code of Ethics (2005)

A.12.g. Technology and Informed Consent

- As part of the process of establishing informed consent, counselors do the following:
  - 1. Address issues related to the difficulty of maintaining the confidentiality of electronically transmitted communications.
  - 2. **Inform clients** of all colleagues, supervisors, and employees, such as Informational Technology (IT) administrators, who might have authorized or unauthorized access to electronic transmissions.

### Privacy, Confidentiality, Diversity

- **Privacy & Confidentiality**
  - Understand your technology (email, texting, video) and its clinical repercussions related to privacy and technology

- **Diversity**
  - Multi-cultural, multi-lingual, religious, LGBT, and other issues
Service to the “Home”

- Scientific evidence base for contact to the home is much thinner, less reliable than traditional telehealth
- Risk management is a serious concern
- Likelihood of lurkers, intruders or interruptions is increased
- Develop signs, code words or phrases to signal something is amiss

TMHI Clinical Competence
Client Selection

- Study the evidence base (research)
- People with almost all diagnostic symptoms have been documented as successfully treated with traditional telehealth
- Clients experiencing severe anxiety, flagrantly psychotic symptoms or suicide/homicide intent may not be optimal choices while symptom patterns are exacerbated
TMHI Clinical Competence

Client Selection

• Most of the studies mentioned above include the assistance of a local collaborator
• Treatment to the home has not yet identified full range of risk
• Understand differences when delivering care to clients in different settings (hospital vs. car, park, bed etc.)
• Establish procedures to minimize attendance & compliance issues

Specific Informed Consent Processes and Documentation
TMHI Informed Consent Documentation Basics

- Date
- Diagnosis
- Outline of intervention
- Risks and benefits of each technology used
- Risks and benefits of competing approaches
  - Including no service

TMHI Informed Consent Documentation Basics

- Emergency Resources and Plan including names and contact information for local, trusted person(s) to be contacted at the discretion of the clinician
- Document advantages and disadvantages of using technology
- Document evidence-base supporting counseling plan
- Document client preferences re: technology
TMHI Informed Consent Documentation Basics

- Confidentiality and limits thereof as related to mandated reporting (suicide, homicide, abuse)
- Fees, if any
- Statements* similar to:
  - My questions have been answered to my satisfaction in language I understand
  - As of the time of my signing, all blanks have been filled in
- Document method & procedures for data storage
- Document adherence to local and distant regulations

* Obtain full legal review with a local telehealth attorney prior to using any TMHI sample wording with clients either verbally or in your informed consent document.

TMHI Informed Consent Documentation Basics

- Some risks may not yet be known*
- No physical exam*
- Identify both the clinician’s & client’s/patient’s physical location
- Statements* such as: Professional will rely on information provided by the client/patient and by any on-site practitioners or other sources
- Potential problems could arise with electronic transmission in telepractice:
  - distortion, delays, interceptions, interruptions
- Document all communications with client (written, audio, video or verbal)

* Obtain full legal review with a local telehealth attorney prior to using any TMHI sample wording with clients either verbally or in your informed consent document.
TMHI Informed Consent Documentation Basics

• Discuss the purpose of remote contact
• Inform clients of who will have access to their email address, phone number, or any other contact information
• Inform the client of who else might contact the client on your behalf
• Discuss multi-cultural and diversity issues

TMHI Informed Consent Documentation Basics

• Describe the specific roles of any consultant or local referring practitioner and who will have ultimate authority over the client’s treatment
• Discuss whether client information will be stored in a computerized database
• Provide written procedures for various types of follow-up when client does not appear for remote consultation
  – Time limit for non-response before collateral person will be contacted if professional is concerned
TMHI Informed Consent Documentation Basics

- Describe how deficiencies electronic equipment could possibly cause interference with diagnosis or treatment
- Make provision for non-receipt of email, delayed receipt, problems with servers, or unannounced changes in the schedule of email communications
- Mention how easily human error could lead to incorrectly delivered messages or other unforeseen events

Emergencies

Have a plan.

- Discuss carefully
- Write plan in your informed consent document
- Develop prior relationships with local community:
  - Physician
  - Family
  - School personnel
  - Other leaders (AA, religious?)
  - Emergency response team
  - Know community resources (hospitals, drug/alcohol treatment facilities, etc.)
  - Know your local collaborators

Know who and when to call for local assistance.

- Inform client of when you will contact local leaders, what you will tell them.
- Cover your termination procedure (i.e., “I will make 2 telephone calls, leave you 2 messages, send you a letter in surface mail with a copy to your physician.”)
Existing TeleMental Health Guidelines

- American Psychological Association. (2010). Ethical principles of psychologists and code of conduct
- British Psychological Society. (2009). The Provision of Psychological Services via the Internet and Other Non-direct Means

ATA Guidelines, 2013

- Consider other individual characteristics (e.g., psychological stability, physical/cognitive disability, personal preferences)
APA & ATA Guidelines, 2013

• Start sessions with an opening protocol
• Provide and discuss clear emergency plan with written instructions (e.g., suicide, homicide, abuse, other)

Opening Protocol* (Ongoing Informed Consent)

• Identify yourself and your geographic location
• Ask your client/patient to do the same
• Audio/video check (e.g., Do you hear & see me clearly?)
• Is there anyone in your room or within ear-shot today? (Agree on safety code words, signals or phrases)
• Is there anything else I might notice and find of interest if I were in the same room with you today?
• Has there been an emergency in your environment today?
• Is there anything else I should know about before we begin talking today?

* Obtain full legal review with a local telehealth attorney prior to using any TMHI sample wording with clients either verbally or in your informed consent document.
American Telemedicine Association

- Determine outside emergency coverage
- Establish guidelines for determining at what point other staff and resources should be recruited to help manage emergencies
- Be familiar with local civil commitment regulations and have arrangements where possible to work with local staff to initiate/assist with civil commitments

Local Collaborators or Champions
Levels of Security

Legal Issues

Discipline-Specific Issues

- **Scope of Practice**
  - Special informed consent laws
  - Special cases related to telehealth
- Oklahoma case of Dr. Trow
  - No in-person assessment
  - No informed consent
  - No HIPAA-compliant technology (he used Skype)
Informed Consent

- Definitions differ by state
- Represents a “meeting of the minds”
- Document only serves as important evidence

ACA Ethical Standards
A.2.b. Types of Information Needed

Counselors explicitly explain to clients the nature of all services provided. They inform clients about issues such as, but not limited to, the following: the purposes, goals, techniques, procedures, limitations, potential risks, and benefits of services; the counselor’s qualifications, credentials, and relevant experience; continuation of services upon the incapacitation or death of a counselor; and other pertinent information.
Mandated Reporting

Behavioral professionals are mandated reporters

- Duty to Report
  - Child abuse
  - Elder Abuse
  - Spousal Abuse
- Duty to Warn
  - Tarasoff

Licensure
ACA Code of Ethics 2005

1. Knowledge of Standards
   • Counselors have a responsibility to read, understand, and follow the ACA Code of Ethics and adhere to applicable laws and regulations.

Practicing Over State Lines

Licensing Boards that may assert jurisdiction:
   • The one in your state(s) of licensure
   • The one in the client/patient’s state of location at time of call
   • Both

Safest Practice:
   • Provide services only where licensed
   • Require client/patient to attest to his or her location on every call
Skype and Health Privacy

- Free
- AES 265-bit encryption
- Access to patient’s environment

**BUT**
- Skype makes no claim that its services can be used in a HIPAA-compliant manner
- Skype does not offer a BA Agreement
- Cannot verify transmission security
- Does not provide breach notification
- Does not provide technical support
- Frequently dropped calls
  - Emergencies?
- No audit trails
HIPAA requires an “audit trail.” Skype doesn’t provide audit trails – and isn’t obligated to ....

Read Skype’s Privacy Policy

• Skype may gather and use info about you...
  – Identification data (e.g. name, username, address, telephone number, mobile number, email address)
  – Electronic identification data (e.g. IP addresses, cookies)
  – List of your contacts and related data
  – Content of instant messaging communications, VMs, video messages
• Skype uses its own cookies for a variety of purposes, including to
  – Provide internal and customer analytics and gain statistics and metrics about our websites
• Skype’s analytics, ad-serving and affiliate partners may also set and access cookies on your computer
• Skype will take appropriate organizational and technical measures to protect the personal data and traffic data provided to it or collected by it with due observance of the applicable obligations and exceptions under the relevant legislation
Skype’s Hackings

Reported Security Issue - RESOLVED
By Leonas Sendrauskas on November 14, 2012.

[UPDATE:14/11/2012@15:28GMT]
Early this morning we were notified of user concerns surrounding the security of the password reset feature on our website. This issue affected some users where multiple Skype accounts were registered to the same email address. We suspended the password reset feature temporarily this morning as a precaution and have made updates to the password reset process today so that it is now working properly. We are reaching out to a small number of users who may have been impacted to assist as necessary. Skype is committed to providing a safe and secure communications experience to our users and we apologize for the inconvenience.

Is Skype Reliable?
Skype tiles & pixelates, the audio gets tinny, echoes develop, and often calls drop entirely. Sometimes consumers can see you and hear you, without your awareness.
Telepsychiatry: The Perils of Using Skype

First released in 2003, Skype offers free, worldwide video access to any patient with an Internet connection, either by mobile device or desktop computer. What it does not offer, however, is a norm of communication clearly available for clinical services—especially in mental health. According to estimates matched to groups such as the Meds for Behavioral Health telemedicine hotline, it grew by 50% in 2015 alone, and by 2017, it had crossed some of the same guidelines as others in Skype. Thus, it is proving to be a dangerous resource.

Ordinarily, neither federal nor state law is designed to regulate specific proprietary services such as Skype and its competitors. Video-chat platforms were developed for marketing to the general consumer, and not for healthcare. The Health Insurance Portability and Accountability Act (HIPAA) holds professionals responsible for conducting their own internal risk assessments regarding their chosen technologies. Before using any equipment, the professional should require documentation that explicitly prohibits “HIPAA compliance” or “HIPPA compliant.” One could take further comfort in a designation of federal Information Processing Standard (FIPS) certification, which is a standard that may meet and exceed HIPAA standards.

HIPAA requires the use of equipment that allows for audit trails. According to the American Health Information Management Association, audit trails allow breaches to be traced. Unlike proprietary platforms, Skype makes it impossible to conduct approved security audits via audit trails. Skype itself is not

Where to find HIPAA Compliant Video

- [www.telehealth.org/video](http://www.telehealth.org/video)
OCPM Step 3 Legal Issues: Which Technologies to Use?

• No Guesswork Needed

Question and Answers
OCPM: Online Clinical Practice Management

Telemental Health: HIPAA, HITECH & Your State Law

Three HIPAA Rules:

- Transmission
- Privacy
- Security
HIPAA Privacy Rule

• Data are “individually identifiable” if they include any of the 18 types of identifiers, listed below, for an individual or for the individual’s employer or family member, or if the provider or researcher is aware that the information could be used, either alone or in combination with other information, to identify an individual:

HIPAA Privacy Rule (cont.)

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city, county, zip code)
3. All elements (except years) of dates related to an individual (including birth date, admission date, discharge date, date of death and exact age if over 89)
4. Telephone numbers
5. Fax number
6. Email address
7. Social Security number
8. Medical record number
9. Health plan beneficiary number
10. Account number
11. Certificate/license number
12. Any vehicle or other device serial number
13. Device identifiers or serial numbers
14. Web URL
15. Internet Protocol (IP) address numbers
16. Finger or voice prints
17. Photographic images
18. Any other characteristic that could uniquely identify the individual
HIPAA “Final Rule”

- When HIPAA was first passed in 1996, most health care practitioners, hospitals and insurance companies scurried to bring themselves into compliance with the new standards. In the face of these final rules, business associates will have to engage in the same process.
- HHS is stepping up enforcement efforts.
- See Federal Register available online at http://federalregister.gov/a/2013-01073, and on FDsys.gov
What makes you a “covered entity”?

HIPAA Policies

- Use HIPAA compliant *technologies* and develop written *processes*
  - Document policies
    - Security & privacy policies
      - Repairs
      - Staff training
      - Breach notification, etc.
HIPAA “Final Rule”

- Infrastructure, documentation, and procedures for information privacy and security, and data encryption and disposal will have to be evaluated and brought into compliance.
- Companies need to provide formal security training to all employees, designate a security official and implement appropriate business associate contracts with their own subcontractors.

HIPAA “Final Rule” January 17, 2013

- Business associates of covered entities are directly liable for compliance with HIPAA Privacy and Security Rules’ requirements. Includes contractors, subcontractors and business service companies working for health care providers, (e.g., companies providing electronic health records software, teleconferencing, data back-up and storage, billing, transcription and other IT services).
- Raises the maximum penalty for data breaches from a previous cap of $250,000 to a maximum penalty is $1.5 million per violation.
HIPAA, Business Associates & HITECH

- All Business Associates in health care must sign an agreement stating their adherence to HIPAA standards
  - Transactions
  - Security
  - Privacy
- True for any service you hire
- It is now enforced by the HITECH ACT

HITECH

- If aware of a potential breach of protected health information:
  - Conduct risk assessment
  - Mitigate breaches
    - Purchase 1 year account to Equifax, Transunion or Experian
  - report breach to affected clients, the federal government, and in some cases, the media
HITECH

Implement or update privacy and security policies and procedures:

• Need policies to be written (a paragraph is ok)
• Staff education
• Breach procedures
  – Consult your attorney
  – 500 or more records
    → notify media

HITECH

Do not disclose treatment information to your client’s health insurance carrier if they are paying you out-of-pocket, unless the disclosure is required by law
HITECH

• Clients may ask for copies of their electronic health records in electronic form

Email

• Send PHI in unencrypted e-mail only if the client is advised of the risk and still requests use of email as a means of transmission
What are risks of sending unencrypted email?

HITECH

- There are additional new restrictions on marketing and sale of PHI, which should be included in counselors’ HIPAA policies and procedures and Notice of Privacy Practices if relevant.
HITECH

Update your Notice of Privacy Practices:

- OCR and the Office of the National Coordinator for Health Information Technology released a Model Notice of Privacy Practices, get it here:
  http://www.hhs.gov/ocr/privacy/hipaa/modelnotices.html

HITECH

Notice of Privacy Practices

- Make available to existing clients on request
- Post on your website
- Display in a prominent location in your professional premises
- Provide copy to all new clients
HITECH

Update Business Association Agreements (BAAs)

- Contractors & subcontractors
  - Billing
  - Data storage

HITECH

- Many states have their own privacy laws, which can be more stringent than federal law HIPAA & HITECH.
- Consider obtaining a legal review of your HIPAA policies, procedures and other documents by your local, informed attorney.
- Speak with ACA legal office.
Where can you get all the needed HIPAA forms?

Enforcement

The most common types of covered entities required to take corrective action:

• Private Practices
• General Hospitals
• Outpatient Facilities
• Health Plans (group health plans and health insurance issuers) and
• Pharmacies

http://www.hhs.gov/ocr/privacy/hipaa/enforcement/highlights/index.html
Myths vs. Realities for Distance Counseling

- **Not same**
- **No research**
- **Psychotherapy can’t change (resistance)**
- **We won’t need to change**
- **It’s too expensive**
- **No reimbursement**
- **It’s illegal or unethical**
- **All distance counseling involves direct care**
- **No guidelines**

- **Doesn’t need to be**
- **1000s of articles**
- **We can -- and already are change psychotherapy**
- **It has already happened**
- **Affordable**
- **Reimbursable**
- **Legal and ethical**
- **Self-help for billions of people worldwide**
- **Many guidelines exist**
Wish List of Next Steps

- Recognize Essential Differences:
  - traditional telepsychiatry vs. how most allied health professional are using telehealth
  - Outline clear statements of needed technology-based competencies
  - Develop distance counseling protocols for treatment in “unsupervised settings”
    - Find malpractice carriers who will carry our entire risk (both civil & regulatory)
- Advocate for our regulatory boards to
  - Post clear statements about, & enforce existing laws
  - Require technology-competencies be demonstrated as a condition for licensure
- Focus on other areas in addition to direct-care: self help, technology-assisted care
- Join us in LinkedIn by searching for the group called “TeleMental Health Institute”

The Future?

- Technology isn’t just the future – it’s here today
- It can already be used legally & ethically
- It’s the right thing to help grow our profession with with health care reform
- Get informed:
  - develop your competencies practice using the evidence base as your guide
  - obey the law
  - comply with ACA ethics standards
  - focus on proper documentation and
  - plan for emergencies
- You can do this!
Questions and Answers

TeleMental Health Institute, Inc.

Send email to: info@telehealth.org

Visit website: www.telehealth.org