ETHICS AND TELEMENTAL HEALTH

INSTRUCTORS

Claudia Dewane, D.Ed., LCSW is a retired Associate Professor in the School of Social Work, Temple University, Harrisburg, Pennsylvania. She received a Doctorate in Adult Education and Health Psychology from Penn State University, and a Masters in Social Work from Columbia University. She has a Certificate in Advanced Clinical Supervision from Smith College School of Social Work. She is the founder of Clinical Support Associates, providing supervision, consultation and training to professional social workers. She has presented numerous workshops on clinical, supervisory, and ethical issues in social work. She worked for the Department of Veterans Affairs (VA) for several years in clinical, supervisory and policy capacities. She currently works as a therapist and clinical supervisor.

Teresa Crowe, PhD, LICSW is a licensed clinical social worker in the District of Columbia and Maryland. She is a professor of social work at Gallaudet University and teaches practice, theory, and research in the MSW program. She coordinates a telemental health program for deaf children and adults through Arundel Lodge, Inc. in Edgewater, MD. Her recent research focuses on deaf and hard of hearing populations, especially in the areas of behavioral health, intimate partner violence, telemental health, well-being, and help-seeking.

SYLLABUS

Introduction
A Shift to Telehealth
Computer Basics
      Computer Terminology Basics
      Computer Security
Telemental Health Technology Basics
      Types of Technology
      Telemental Health Practice Technology Considerations
      Secured Versus Unsecured Technology
      Platforms
      Commonly Used Technology in Psychotherapy
Common Telehealth Ethical Encounters
      Challenges Unique to Telehealth Sessions
      Creating an Informed Consent Form for Telehealth
Best Practices in Telemental Health
      Offer Orientation to the Technology Before Beginning Treatment
      Video Etiquette
      Video Space
      Video Presentation Skills
      Risks of Teletherapy
      Multicultural Considerations

LEARNING OBJECTIVES

Upon completion of the course, learners will be able to:
1. Define terminology basic to telemental health, computers, and technology.
2. Differentiate types of computer security measures.
3. Identify common ethical nuances of telehealth service delivery.
4. Describe best practices in telemental health.
5. Recognize risk management and ethical conduct in telemental health with children, couples, families, and groups as well as in the provision of supervision via videoconferencing.
6. Identify relevant information related to telehealth from legislative bodies, professional standards, and ethics codes from the NASW, APA, ACA, and NBCC.

INTRODUCTION

Prior to the pandemic, telemedicine was gaining traction but usually only in select instances and geographic areas. The use of telehealth necessitated by the pandemic has transformed into a more permanent way of providing care in many settings.

The healthcare industry is widely experiencing a digital transformation. In one study of 12,828 mental health treatment facilities, telehealth services increased dramatically from 39.4% in 2019 to 88.1% in 2022 (McBain et al., 2023). As telemedicine grows in healthcare provision, an increase of access to health care in rural areas continues to be a common goal. According to the U.S. Department of Health and Human Services [HHS], "Telehealth is especially critical in rural and other remote areas that lack sufficient health care services, including specialty care" (Coverage to Care, 2023, p. 19).

Behavioral health practitioners are adjusting quickly to the demands of providing services via virtual platforms. Within the last decade, practitioners and systems have adjusted to electronic health records, which paved the way to patient portals. However, this type of service provision carries unique ethical challenges. Through the use of potential scenarios, literature review, and discussion, this learning material will address the specific ethical challenges, requirements, and demands of telemental health services.

There are close to twenty different terms that refer to the practice of telemental health services. This course is designed for human services and mental healthcare practitioners, including social workers, psychologists, counselors, and marriage and family therapists, and makes use of the terms telehealth, telemental health, and telebehavioral health interchangeably.

A SHIFT TO TELEHEALTH

The U.S. Department of Health and Human Services defines telehealth as the "use of electronic information and telecommunication technologies to extend care when you and the patient aren't in the same place at the same time" (Coverage to Care, 2023, p. 2). Video conferencing, Internet store-and-forward imaging, streaming media, and terrestrial and wireless communications (e.g., phone calls made using landlines, cellular data, or Wi-Fi) are all technologies available for telehealth. These telehealth technologies seem to be mainstays in healthcare due to the vast changes in services delivery prompted by the pandemic.

Historically, digital options for providing care existed but were used only as the exception due to implementation barriers such as digital illiteracy, broadband access, security concerns, and licensing or other regulatory requirements. The need for accessible and efficient care during COVID-19 broke these barriers and radically expanded telehealth. Cleveland Clinic, for example, performed 80% of healthcare visits via telehealth technology when the pandemic began (Cleveland Clinic, 2020) and continues to expand its reach by integrating telehealth into its newest hospital (Diaz, 2023). Mental health has seen tremendous shifts in service delivery as more and more mental health treatment facilities offer (McBain et al., 2023) and continue to deliver telehealth services (FAIR Health Inc, 2023).

This shift to increase virtual interactions between clients and clinicians forces providers to reexamine previous "ways of doing" certain components of care, such as building rapport and establishing trust through positive communication skills. In addition to managing all the practical transitions necessary to provide telehealth, providers must ensure that they are practicing within legal and ethical parameters.

Fortunately, both patients and providers experience benefits with the increased use of telehealth within mental and behavioral health services. Cost-effectiveness and expanded availability to services afforded by telehealth, for example, reduces some health disparity in psychiatric and mental health services. Some other benefits include the following (Coverage to Care, 2023):

- improved accessibility to treatment
- reduced cancellations and no-shows to appointments
- increased support for patients that struggle with tasks required for in-person visits
- reduced stigma related to treatment

Undoubtedly, compared to in-person appointments, some clinical nuance is lost. Some patients may not have a safe space for treatment and may not be able to disclose important information for fear of being overheard (Coverage to Care, 2023). A lack of physical presence can also affect treatment, as physical presence plays a role in the therapeutic relationship and the ability to read social and physical cues.

There comes a whole new set of ethical challenges as telehealth emerges as a larger source of healthcare delivery than it was pre-pandemic. Thus, the exploration of ethical encounters engendered by telehealth is more important than ever.

COMPUTER BASICS

A social worker in private practice has a client walk her through the needed technology changes to her videoconferencing set up to improve the video quality during their session. He works in tech and advises her on what security measures to take to ensure his privacy. He advises her to use an ethernet cable so that she is less reliant on Wi-Fi and recommends that she change platforms to one that his company uses.

Essential principles for ethical practice are that of competency and privacy. As many practitioners switch to providing telehealth services, having basic competency in using the technology becomes a central concern. As such, the technology involved in providing telehealth services is reviewed here. Computers use a combination of hardware and software components. Computer hardware is any part that has a physical structure, such as the internal parts, keyboard, or mouse. Software is the set of instructions that is used to obtain and use the information wanted by an individual. Word processing programs, games, Internet browsers, PowerPoint, spreadsheet programs, and other programs are examples of software. Individuals rely on both hardware and software. Below is a list of terms that are helpful to know.

Many people think of a personal desktop or laptop when they think of computers. However, computers come in diverse shapes and sizes and perform many different functions in daily lives. Several examples of different types of computers are ATM machines, automobile computer chips, smartphones, personal digital assistants (PDAs), tablets, game consoles, smart televisions, and wearable technologies, such as fitness trackers and smart watches.

Computer Terminology Basics

The following discussion is provided to help therapists become familiar with commonly used terms and their meanings. These terms relate to computer and Internet use.

Application: An application, or app, is a type of software or hardware system that allows a user to perform specific tasks (National Institute of Standards and Technology [NIST], n.d.a). If an application is for a desktop or laptop computer, it's called a desktop application (GCFGlobal, n.d.a). If it's used for a mobile device, it's called a mobile app. An application program can be self- contained or embedded within a group of programs. It uses the computer's operating system and other supporting systems, such as database programs, word processors, web browsers, social media platforms, wikis (website that visitors can edit), and spreadsheets. There are also many desktop applications. Some offer a variety of

features, such as word processing programs, like Microsoft Word, while others offer one to two features, such as a clock or a calendar app. Apps tend to be user friendly, unique, and focused.

Bandwidth: Bandwidth is a measure of the information capacity of a communication channel (Froehlich, n.d.). High bandwidth, which allows for fast Internet speed (i.e., high-speed Internet), is optimal for telemental health videoconferencing, whereas lower bandwidths (i.e., slow Internet speed) may result in quality issues like interrupted, slow, or "glitchy" video and audio.

***Bluetooth*:** Bluetooth is a technology for wireless communication over short distances (NIST, n.d.c). It is used to communicate with wireless devices, such as keyboards, mobile phones, laptops, PCs, digital cameras, mice, printers, speakers, and headphones (GCFGlobal, n.d.b). The communication connection that Bluetooth facilitates is over a secure, globally unlicensed short-range radio frequency and most devices have Bluetooth technology.

Broadband: This term refers to a high-capacity transmission technique using a wide range of frequencies that allows a number of electronic messages to be communicated simultaneously. It refers to the transmission of signals in a frequency-modulated way over a segment of the total bandwidth that is available from the Internet provider (Federal Communications Commission, 2022).

Central Processing Unit: The central processing unit (CPU) is also known as the computer's processor (GCFGlobal, n.d.d). It is located internally and connected to the motherboard. The CPU is the brain of the computer and carries out the commands of the user. When a user presses a key or clicks the mouse, she is sending instructions to the CPU. The CPU is usually a two-inch ceramic square with a silicon chip embedded in it. A processor can be different speeds. A higher speed processor is desirable for videoconferencing.

Cloud: The cloud, or cloud storage, refers to the Internet (GCFGlobal, n.d.c). When something is stored in the cloud, it means that the data are saved onto an Internet server rather than the computer's hard drive. All email services are web-based and are stored on an Internet server rather than a personal computer. When data are stored on the cloud (i.e., the Internet), they can be retrieved from any computer with an Internet connection. Individuals commonly use the cloud for file storage, file sharing, and backing up (saving) data.

Private Cloud

Company → Cloud

Public Cloud

Company 1, Company 2, Company 3, Company 4 → Cloud
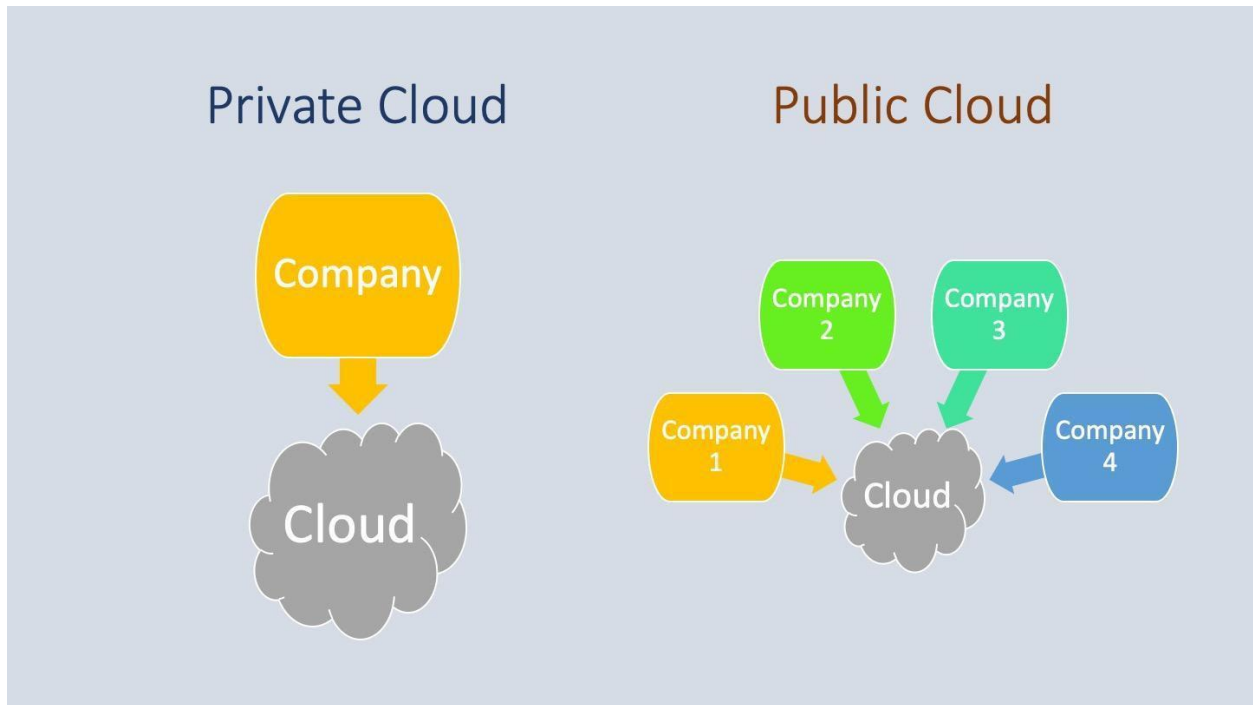
Cloud Computing: A model that enables on-demand access to computing resources that are delivered as a service over the Internet (NIST, n.d.d). These computing services include servers, storage, databases, networking, software, analytics, and intelligence (Microsoft Azure, 2023). Typically, a customer pays only for the cloud services used, which helps to lower operating costs, run infrastructure more efficiently, and scales up or down as the business changes.

Digital Signature: A digital signature is a mathematical process for authenticating digital messages or documents (Gillis, 2023). This digital signature gives the recipient of a document evidence that the message was created by a known sender and not altered in transit. In telemental health services, agency forms, such as consent for treatment, can be signed digitally by clients and then be entered into an electronic health record.

Encryption: Encryption is a process of encoding electronic data so the information cannot be retrieved or decoded by an unintended recipient (NIST, n.d.e). Only the person or computer system authorized can access encrypted data.

Encryption

Original Document (Plaintext) → Encryption Algorithm Software → Encrypted Document (Ciphertext)
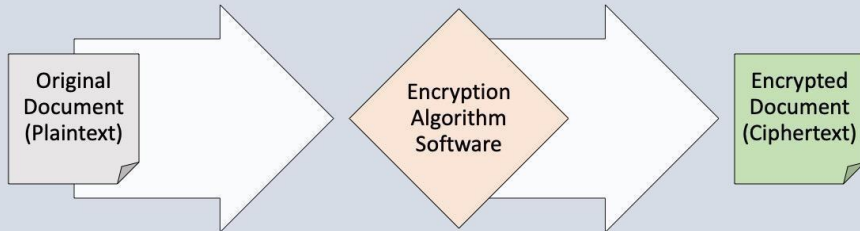
Firewall: A firewall is a part of a computer system that blocks unauthorized communications between a clinician's or agency's computer network and external networks (NIST, n.d.f).

Firewalls

INTERNET — FIREWALL — Router (Computer interface) — Device 1, Device 2, Device 3
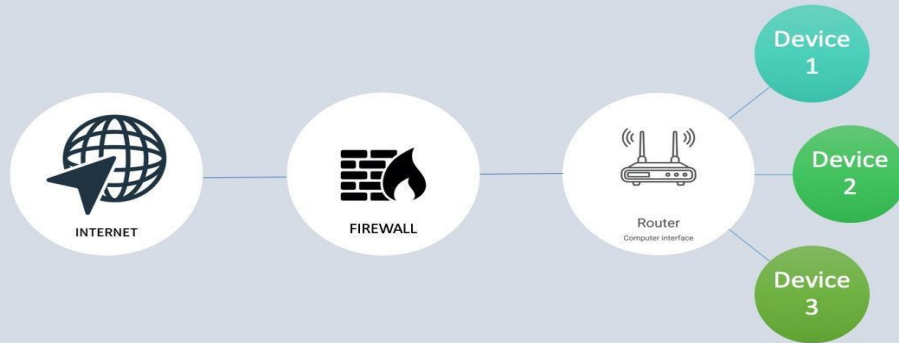
Graphics Processing Unit: A graphics processing unit (GPU) is an electronic circuit device that controls what the user sees on the monitor (GCFGlobal, n.d.d). Most computer GPUs are already built into the motherboard of different devices, such as computers, cell phones, and game consoles. Some GPUs are stored on small video cards that can be plugged into a computer GPU slot. The GPU handles video images while a sound card (i.e., audio card) manages audio and what the user hears in speakers or headphones.

Hard Drive: A hard drive is where software, documents, and other files are stored for long-term (GCFGlobal, n.d.d). When data on the hard drive are stored, they are saved even when the computer is turned off or unplugged.

Malware/Malicious Software: Malware, or malicious code, is a program that is designed to damage computers or steal computer files without the user's consent (NIST, n.d.h). It is a general term that can apply to specific types of threats, such as viruses, spyware, worms, trojans, and rootkits.

Mobile Applications: Mobile applications, or mobile apps, are used for devices, such as smartphones and tablets (GCFGlobal, n.d.a). Examples of mobile apps are Gmail and Instagram. There are thousands of mobile apps for different types of interests, such as travel, reading, games, navigation, and fitness. Mobile applications can include mental health-related programs, such as managing depression, anxiety, addiction, eating disorders, and post-traumatic stress disorder. Some applications are free while others charge users fees.

Mobile Device: A mobile device is a portable computing device that goes where the user goes (NIST, n.d.i). It has portable two-way communication devices, computing components, and the ability to connect to Internet networks. Examples of mobile technology are smartphones, tablets, and watches.

Modem: A modem connects a computer to the Internet through a wire (e.g., ethernet cable). Modems are essential for accessing the Internet connection and work with routers, which allow multiple computers and other devices to use the Internet connection all at once through wired connections or via Wi-Fi.

Motherboard: A motherboard is a thin plate that serves as the computer's main circuit board (GCFGlobal, n.d.d). It works by holding the connectors, memory, CPU, and other hardware, which controls the video, audio, and connections to the port. It contains the principal components of the device or computer and allows other connectors to other circuit boards.

Mouse: A mouse is a corded or wireless device that moves the computer cursor. Its name originated at the Stanford Research Institute because earlier models had a cord that resembled a mouse tail.

Network Card: A network card allows the computer to communicate over an Internet network (GCFGlobal, n.d.d). It can either connect with an Ethernet cable that is plugged into an ethernet port or through a wireless connection (i.e., Wi-Fi). Network cards can also be expanded and used in a dedicated computer slot.

Ethernet Port
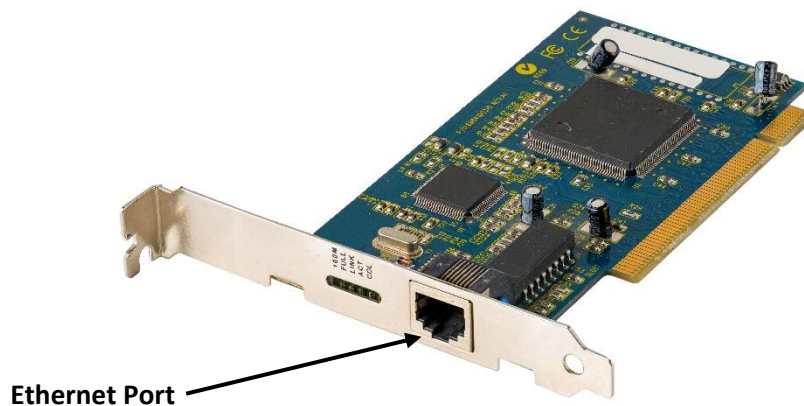
Operating System (OS): An operating system is the collection of software that runs on a computer (NIST, n.d.j). This system manages the computer's memory, processes, software, and hardware (GCFGlobal, n.d.e). This system allows a user to communicate with the computer without having to use computer code language. It coordinates all of the computer components in order to allow the user to complete desired tasks. Microsoft Windows, macOS, and Linux are the most common operating systems. Linux is an open-source operating system that is accessible to anyone in the world. Unlike Windows or macOS, Linux is free and has different versions from which to choose. Mobile devices, such as smartphones, tablets, wearables, and game players have different operating systems than computers or laptops. There are different operating systems for mobile devices. Two of the most popular ones are Google Android and Apple iOS.

Port: A computer port is a hole or connection on a computer that allows external devices, called peripherals, to be plugged in, such as a printer, an external drive, and a mouse (NIST, n.d.k).

SpicyTruffel/Shutterstock.com

Random Access Memory (RAM): Random access memory (RAM) is the computer's short-term memory (GCFGlobal, n.d.d). As the computer performs calculations, the resulting data gets stored in the RAM temporarily. Any data stored in the RAM disappears when the computer is turned off unless the user saves the data on a document, spreadsheet, or other type of file. The computer's RAM size directly correlates to its performance capabilities. The more RAM available, the more tasks a computer can accomplish simultaneously.

Router: A router is a device that allows multiple computers and other devices (e.g., printers) to simultaneously access the same Internet connection (established by a modem) via wires and wirelessly (using Wi-Fi).

Sound Card/Audio Card: A sound card is responsible for the audio sounds in speakers or headphones (GCFGlobal, n.d.d). Most motherboards have integrated sound cards, but the user can install an additional card to upgrade to a better-quality sound.

Tablet: A tablet is a mobile device that operates similarly to a personal computer while being smaller and more portable than a desktop or laptop (GFCGlobal, n.d.f). It often includes a touch screen, microphone, and web cam. Tablets are compatible with wireless

Internet connections and cellular data networks. They are lighter and easier to carry than laptops.

Uniform Resource Locator (URL): A uniform resource locator (URL) is a resource that specifies the address of a webpage on the Internet (NIST, n.d.l).
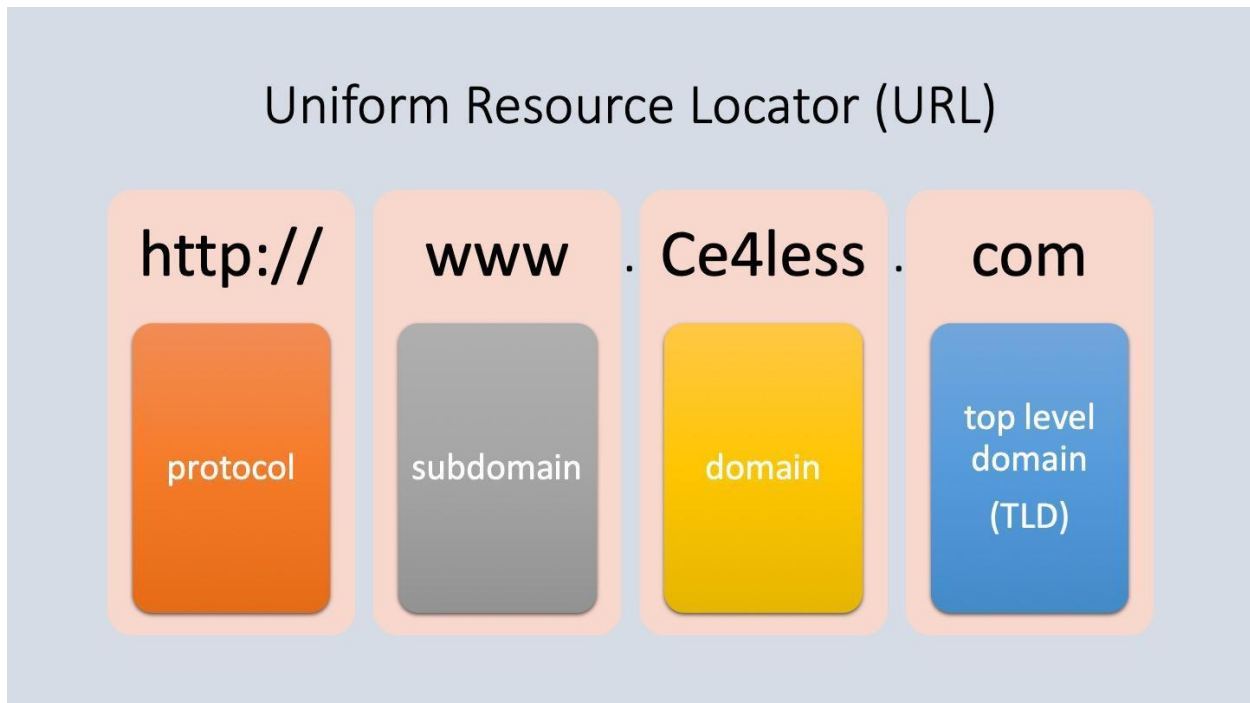
Virtual private network (VPN): A virtual network that provides secure communications for data that is transmitted between networks, such as a home network and corporate network (NIST, n.d.m).

Web browser: A web browser is a type of computer application that allows user to access the Internet and view its content (NIST, n.d.n). Most computers have web browsers pre-installed, but others can be downloaded. Examples of web browser applications are Internet Explorer, Mozilla Firefox, Google Chrome, and Safari.

Web camera: A webcam, or webcam, is type of camera that is either integrated into a computer or is plugged into a computer as an external device (GCFGlobal, n.d.g). It can record videos, take pictures, and transmit audio or video across the Internet in real time. The webcam is a required component for videoconferencing.

Wi-Fi: Wi-Fi is a wireless networking protocol that allows devices to communicate without having direct cable connections (Pinola, 2020). When not connected via direct cable, devices need Wi-Fi (usually sourced by a router) to access the Internet, which is then how teleconferencing and other technologies are facilitated for telemental health. In some instances, users can connect to Wi-Fi using their smart phone as the Wi-Fi source (i.e., by

turning on the phone's *hotspot* the phone can serve as a portable router). Wi-Fi allows for multiple devices (e.g., laptop, printer, tablet) to connect to the Internet. The image below shows the Wi-Fi router as the source in the middle connecting the Internet to a smart phone, laptop, desktop, and watch.

Jiw Ingka/Shutterstock.com

Computer Security

A computer that is attached to the Internet can potentially have many threats, including viruses, malware, and hard drive failure (GCFGlobal, n.d.h). Malware is a term used to describe any type of software that can damage computers or files, steal files, or track keystrokes without a user's consent. Most malware is distributed over the Internet and is bundled with other software. Antivirus software helps to prevent malware from being installed and removes it from a computer.

Many malware programs exploit the security flaws in other software programs (GCFGlobal, n.d.h). One way to help prevent this exploitation is to make sure the operating system, browser, and other programs are updated. These companies often send out security patches or updates in order to protect computers from these types of threats. Another way to avoid losing files because of malware is to back up computer files. A user backs up files by saving data on an external hard drive or online backup service. Then, if files are damaged or stolen, the user has them saved in another place.

Another way of preventing others from stealing or altering data is to create a strong password for files, programs, and applications (GCFGlobal, n.d.i). Passwords should be long, strong, and difficult for someone else to guess. Tips for creating strong passwords include the following (GCFGlobal, n.d.i):

- Do not use personal information, such as name, birthday, username, or email address.
- Use a password that is at least six characters long, includes numbers and symbols, and uses both uppercase and lowercase letters.
- Use different passwords for different accounts.

Some common mistakes with passwords are using family names, the same password on multiple accounts, simple patterns, and short passwords.

Malware systems often use deceptive web addresses to trick users into allowing access to their files (GCFGlobal, n.d.j). Sometimes the web address link will look similar to legitimate web addresses. Double-check the web address (i.e., domain name) for any alterations. A lock symbol in the address bar, usually followed by https://, usually means the website is using a secure connection, which makes it safer to enter information. Not all websites have the symbol. Use caution when a website does not have the lock symbol or the https://.

Avoid suspicious links because often there are malware programs hidden in them (GCFGlobal, n.d.k). Many malware programs require the user to click on a link or download and install a program that appears to be legitimate when it is not. Advertisements on websites that display boxes with "system messages" or "diagnostics" frequently contain malware. Other messages indicating that the user has won a prize or is being investigated often contain malware. Pop-up windows that attempt to lead the user to a different web site can sometimes be malware.
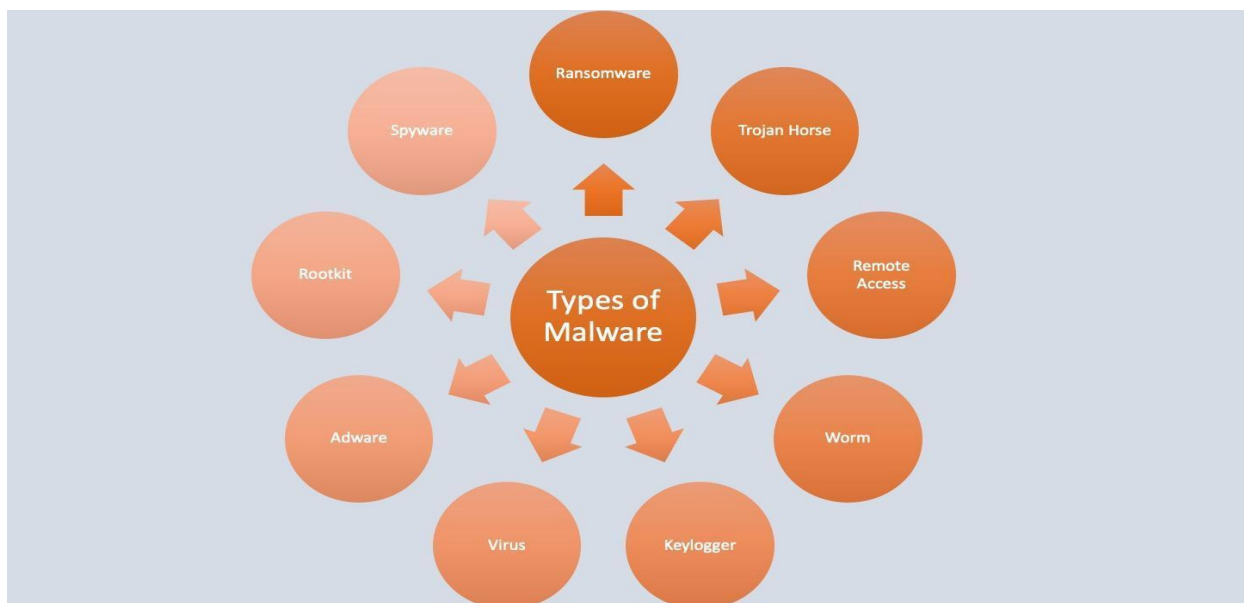
Using Wi-Fi can present a user with security risks. If a home Wi-Fi network is used, the user should make sure it is secure with strong passwords. The user should "disable SSID broadcasting" so that the home network name is not visible to others within the signal range (GCFGlobal, n.d.l). The user can "enable MAC (Media Access Control) address filtering" to prevent unauthorized wireless users from breaking into the home network. A service set identifier (SSID) broadcast can be disabled by changing the settings on a router or on the web by typing the router's IP address. Directions can be found in the router instruction manual. Make sure the network uses "WPA (Wi-Fi Protected Access)" or "WPA2." Public Wi-Fi is not as secure as a home network (GCFGlobal, n.d.l). Sometimes criminals on the Internet, called cybercriminals or hackers, can create seemingly legitimate network names like "Free Wi-Fi," but connect the user to a malware network.

Authentication

Authentication is a security process of verifying the identity of a person or a device sending or receiving information, with mechanisms such as username and password combinations, biometric devices (e.g., voice recognition, fingerprint, or face scan), and onetime passwords (NIST, n.d.o). It occurs when a user supplies credentials that the authentication process uses to decide whether to deny or grant access (Suleski et al., 2023). Unfortunately, traditional authentication (i.e., authentication via a single factor like a password) is a weaker option to security and can leave providers and clients vulnerable to cyberthreats. Instead, multifactor authentication provides security where it can often be overlooked (Suleski et al., 2023).

Multifactor authentication is a system that requires two or more factors to achieve authentication (NIST, n.d.p). These factors can include something the user knows (i.e., knowledge), something the user has (i.e., possession), and something the user is (i.e., inherence). Examples of these factors include the following (Suleski et al., 2023):

- **Knowledge:** passwords, security question/answer combinations, and PIN codes
- **Possession:** physical security keys and identification cards
- **Inherence:** fingerprint, face recognition, voice recognition, signature recognition

Examples of authentication practices are entering in a four- or six-digit passcode to unlock a device, having a username and password for an account, verifying an email at another location in order to enter into an account, or having a code sent to a phone via text message to be entered into a field to gain access.

The American Psychiatric Association (2022) acknowledges the importance of authentication and recommends that for synchronous videoconferencing-based telemental health, administrative and technical specifications should be followed to authenticate practitioners as well as the identity of patients. They specify that for telemental health services, the identities of persons at both sites (i.e., practitioners and clients) should be identified, verified, and documented. This documentation can include a) the name and credentials of the provider and the name of the client, b) the location of the client during the session, c) the immediate contact information for both the provider and the client (phone, text message, and/or email), and contact information for other relevant support people, including professional support and family members, and d) expectations about contact between sessions, including a discussion of emergency management between

sessions. Authentication considerations go beyond videoconferencing. Mobile health applications also require a security process of identification.

While the integration of mobile health applications (mHealth) with treatment has become widespread, these applications present unique challenges to security (Istepanian, 2022; Aljedaani & Babar, 2021). The small devices (e.g., smartphones and tablets) that contain mobile health applications can be easily stolen or lost, putting the sensitive information they store, such as passwords and usernames, at risk. According to Rezaee and colleagues (2023), one criterion that will improve the privacy and security of apps is the implementation of "rigorous authentication and authorization techniques" into mobile health applications.

There are currently no HIPAA requirements for specific authentication procedures, though Security Standard §164.312(d) does state that covered entities must "implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed" (Code of Federal Regulations, 2023). A behavioral health provider is responsible for protecting the confidentiality, security, and privacy of client information. Authentication for device access is one way to strengthen protective measures. Multifactor and "rigorous" authentication measures can be used to increase security for private data.

TELEMENTAL HEALTH TECHNOLOGY BASICS

Telemental health technologies are mechanisms to provide behavioral health services remotely.

Types of Technology

Live Videoconferencing

Live videoconferencing is a mechanism for providing synchronous services, meaning live interaction in real time (California Telehealth Resource Center [CTRC], n.d.). Videoconferencing is a way for a provider and client to see one another, interact, and engage on a live monitor or screen. Providers can use live videoconferencing to conduct screenings and assessments, render diagnoses, and provide treatment sessions.

Store and Forward

Store and forward, also known as asynchronous telehealth, is a mechanism that does not transmits information in real time, but rather allows for information, resources, images, or video clips to be saved, forwarded, and used whenever convenient (Health Resources & Services Administration [HRSA], 2023a). Examples of store and forward technology are patient data, video clips, photos, or other types of information that can be sent at a later time through texts or emails. These offer benefits in behavioral health; for example, clients engaged in cognitive behavioral therapy can use store and forward technology to track targeted behaviors.

Remote Patient Monitoring

Remote patient monitoring are devices that remotely collect and send data to providers at a remote location (HRSA, 2023b). Remote patient monitoring systems can help providers assess the health status of a client by collecting information, such as vital signs, weight, and blood pressure. Psychiatrists or prescribers may use remote patient monitoring to check health status before adding or changing medications.

Mobile Health Applications (mHealth)

Mobile health applications use the Internet and wireless devices, such as smartphones and wearable devices, for clients to obtain specialized health information, participate in online discussion groups, collect personal data, or receive health support (CTRC, n.d.; HRSA, 2023b). There are a number of mHealth apps that can be used for behavioral health services for a range of ages and conditions. Often behavioral health providers use a variety of approaches, which can now include these types of apps, to optimize client engagement and participation in treatment. An example of an mHealth application is AnxietyCoach, which is a self-help app that addresses fears and worries using cognitive-behavioral strategies. The app instructs clients through a variety of exercises from making a list of feared activities to making a plan and tracking anxiety levels to viewing progress. The app is offered free of charge, but only though the iPhone store (https://apps.apple.com/us/developer/mayo-clinic/id350350016). Another mHealth app is the CPT Coach for individuals suffering from symptoms of PTSD who are in active treatment with a professional. This app is designed to be used by a client while in active treatment. The app provides education about PTSD symptoms and step-by-step approach to assessments that align with face-to-face sessions. The app utilizes a number of approaches, including prompts and reminders for appointments and homework assignments. This app is available from the Apple iPhone store and Google Play (https://mobile.va.gov/app/cpt-coach).

Telemental Health Practice Technology Considerations

In general, telemental health technology services are commonly delivered through HIPAA-compliant, cloud-based telehealth sites. These services can be delivered through a variety of devices, including desktop computers, laptops, tablets, smartphones, and smart watches. Telemental health platforms can allow providers to conduct online assessments, secure document storage, schedule appointments, offer online billing, provide secure messaging sites, and offer pdf forms and the ability to sign the forms electronically (eSign).

Telemental health services can be offered in a variety of settings, including private practice, agencies, and large consumer systems, such as hospitals. The types of technologies that are most effective may vary depending upon setting. Telemental Health Comparisons is an independent website that provides comparisons for telemental health software (https://telementalhealthcomparisons.com/). This site can be used when a provider registers for a free account.

Practitioners who would like to establish a telemental health practice should keep a few things in mind. One primary issue is being reimbursed for services. It should be easy to use, HIPPA compliant, and include a variety of useful provider tools, such as e-prescribing, client custom folders, scheduling system, appointment alert, data export options, electronic health record

integration, and automated workflows. Providers should understand whether the telemental health system is cloud-based, compatible with provider equipment, such as computers or tablets, and incorporates adequate video resolution, full screen video options, mobile access, and camera abilities, such as tilting, rotating, and zooming. Finally, the technology a provider chooses should include, even if at an additional cost, technical support. Providers are responsible for maintaining their equipment and assisting clients when problems arise. Technical support is vital and should include a variety of mechanisms, such as phone support, email, chat, live video, and/or website support.

Secured Versus Unsecured Technology

There are many advantages to using telemental health technologies, including ease of delivering services, access to services that may otherwise be inaccessible, ability to receive specialized care, obtain consultations, cost-effectiveness, and increased collaboration among professionals. The COVID-19 pandemic revealed that patients and providers were willing to use telehealth, that patients perceived it as effective and were satisfied with it, and that clinicians saw its clinical advantages (Steidtmann et al., 2022; Goetter et al., 2022; Lipschitz et al, 2022).

However, clients and providers may be concerned about privacy and security of personal health information. Health data breaches and cyber-attacks targeting medical information is a widespread and disruptive situation for providers utilizing telehealth and the patients to which they provide care (Tin et al, 2023). In the United States, there were 3,822 reported breaches that affected 283,335,803 people from January 2011 to December 2021, with the most breaches occurring 2020, and the state with highest number of breaches being California. Breaches to protected health information (PHI) are costly and harmful for both service providers and clients. When breaches occur, the provider is responsible for conducting investigations, notifying clients, recovering data, subscribing to credit monitoring services for clients, hiring security personnel, and strengthening the security of the telemental health technology (Zhou et al., 2019). In order to provide education to consumers and engage in practices that protect clients, clinicians should be familiar with the security of the technologies they use.

An unsecured network refers to an Internet connection that does not require a secure authentication process. Unsecured networks are generally public free wireless Wi-Fi connections (WhatIsMyIPAddress.com, 2023). Free Wi-Fi access allows anyone to use a network without a special authentication system. While a public network is easy and convenient to use, it is unsecured and someone could breach the connection and obtain personal data without consent of the user. Some public connections, also called hot spots, will have a user acknowledge terms and conditions. However, this does not secure the network site.

Most home wireless networks have built-in security features in their routers. There are typically passwords that allow access. However, in order for a home network to be secure, individuals need to take steps to set this up (WhatIsMyIPAddress, 2023). To secure a home network, the user needs to enable security settings and create a router password. There are different levels of encryption, such as WEP, WPA2, and WPA1 and each offers a different level of security (WhatIsMyIPAddress, 2023). There are other simple but effective techniques that help reduce attacks on home networks. The National Security Agency (2023) recommends the following:

- upgraded and updated operating systems
- updated and secured routing devices
- WPA3 or WPA2 implementation on wireless network
- network firewalls
- security software
- frequent device reboots
- a [virtual private network](#) (VPN)

Platforms

A platform is a group of technologies that are used as a base for other applications, processes, or technologies and are commonly offered by a [managed service provider](#) (e.g., Theranest and Simple Practice) for use in telemental health (Techopedia, 2020). A platform uses the computer (hardware) and operating system (software) on which applications run. The platform has a set of standards and functions that are purchased by the user. There are a number of telemental health platforms from which providers can choose:

- **Doxy.me** is a cloud-based platform that does not require downloads. It is free to use and its website notes that it is compliant with several national standards. Website: https://doxy.me/

- **Secure Video** is a telemental health/telehealth platform that offers unlimited technology support, scheduling, branding, virtual waiting room, and a business associate agreement, which verifies that it complies with federal regulatory standards. Website: https://securevideo.com

- **Thera-link** is a telemental health platform that includes several features, such as scheduling, billing, progress notes, virtual waiting room, multiple device capability, and a business associate agreement verifying that it meets federal regulatory standards. Website: https://www.thera-link.com/

- **Vidyo** is a video-based telemental health platform that offers low costs, but does not include hardware and maintenance costs. Website: https://www.vidyo.com

- **VSee** is a platform that includes telemental health, telehealth, and telemedicine kits. Medical device kits can be used with this platform. Website: https://vsee.com/

- **WeCounsel** is a telemental health platform that offers a variety of features, including scheduling, assessments, billing, eSign capabilities, and video- or text-based counseling. Website: https://www.wecounsel.com/telemental-health-platform/

A managed service provider will commonly offer a platform with various applications on a central server. Customers generally pay a fee to access the applications over secure Internet connections or a private network. Customers do not need to purchase, install, or maintain the software themselves. Rather, they rent (e.g., monthly subscriptions) the applications that they need

from a managed service provider. The managed service provider generally handles software upgrades and software fixes. Mental health practitioners may already access these types of services if they use on-line billing applications or interact with particular applications when working with insurance companies.

Commonly Used Technology in Psychotherapy

There are two types of technology interactions that can occur between a clinician and client—synchronous and asynchronous communication. **Synchronous communications** are real-time interactions that transmit information in both directions at the same time (American Telemedicine Association, 2020). Examples of synchronous communication are speaking on the telephone or using video conferencing. **Asynchronous communication** is synonymous with "store and forward" transmission of images and/or data. The data transfer takes place over a period of time that is typically separate (e.g., email or texts). The transmission does not take place simultaneously. Asynchronous is contrasted to synchronous (CTRC, n.d.). Email is increasingly used between providers and clients but PHI is vulnerable to breaches through this medium. There is no control over the systems that maintain email. In addition, human errors can result in breaches such as sending emails to the wrong recipient. **Email phishing**, a technique that attempts to acquire sensitive data via deceptive means, is another threat to client data (NIST, n.d.q). One study found that 25% of psychologists surveyed reported some type of breach to their digital mailbox (Lustgarten et al., 2020). It is recommended that practitioners use encrypted email services. Practitioners should also inform clients about the potential risks in using email.

Apps are used in telemedicine and often serve as self-help tools for clients to record data or symptoms. Although incredibly convenient, and more and more a way of life for many, apps tend not to offer sufficient security to protect client data. For example, text messaging is widely used socially, particularly with teenagers and young adults. Commonly, clients expect to be able to use it for communicating about their therapy services. It can be used to schedule and remind them of appointments, send links to psychoeducation information, and sometimes even to suggest an interventive treatment. The ease of texting often results in clients, particularly young ones, expecting to use this as their sole form of communication. "Threats to text messaging privacy can emerge from individual, corporate, and government actors" (Lustgarten et al., 2020, p. 26). Individual's phones can be hacked, corporations may scan data for advertising or marketing purposes, and government agencies may intercept messages as part of surveillance programs. Therefore, clients should be informed that privacy is not assured with text messaging. Informed consents can include risks of texting and suggest that notifications be set to locked. "Providers concerned with compliance are encouraged to de-identify information when transmitting via text message" (Lustgarten et al., 2020, p. 26). Further, providers must be aware that recipients of texts may not be alone when they receive texts. Some providers use end-to-end encryption for the most security. End-to-end encryption encrypts data as it passes through a network while keeping routing information visible (NIST, n.d.r).

Finally, an integral part of technology in psychotherapy is the **electronic health record** (EHR), which is a digital collection of health information about individual patients that is recorded in electronic formats (The Office of the National Coordinator for Health Information Technology, 2023). An EHR is capable of being shared across health care settings throughout network-connected information systems. Electronic health records (EHRs) generally include:

- client demographic information
- intake forms, consent forms
- medical history
- medication
- allergies
- immunization status
- laboratory results
- medical test results
- collateral client data
- crisis plans
- progress notes
- intake assessments
- treatment plans
- financial information

Other terms for EHR are electronic medical record (EMR), personal health record (PHR) and electronic patient record (EPR). EHRs in telemental health and their storage are a possible service provided by managed service providers, including health record templates that clinicians or clients complete that are then stored in HIPAA compliant ways for the clinician's access and use.

COMMON TELEHEALTH ETHICAL ENCOUNTERS

Confidentiality is a paramount principle in the provider-patient relationship. Internet-related technologies have complicated privacy and confidentiality responsibilities. In fact, most ethical transgressions that occur in telehealth are related to confidentiality (Aboujadoude, 2019).

A clinician has a separate room for providing telehealth to his clients. His adolescent children are in the next room watching TV or playing video games. Although he wears headphones so they can't hear the clients talk, they can hear him through the wall. One of them later comments to him, "Jeez you are pretty repetitive, you say the same thing to different clients."

Since the kids have no idea who the client is and can't hear the client, does this situation pose an ethical violation?

A client is told that because of the pandemic the clinic where he receives therapy will be switching to a video conferencing platform to provide services. The client voices concern about privacy. He will only provide consent to have therapy by phone.

Self-determination is another guiding principle, particularly in the social work profession, thus we might just abide by the client's wishes. To take his concerns as a cautionary tale though

we might also want to reassure each client at the beginning of each session as to the setting and how privacy is protected.

Privacy is related to confidentiality and is also primary in serving clients. Lustgarten and colleagues (2020) expand the definition of telehealth privacy to include more than the client session. Technology use is described as progress in therapy services, emails, texting, telebehavioral health therapy, electronic medical records, cloud-based storage, application, and standardized assessments are increasingly used to expedite service provision and more efficient collaboration with payors. However, any of these uses can pose a threat of unintended breaches of confidentiality/privacy with untoward consequences.

Challenges Unique to Telehealth Sessions

A client comes to the telesession visibly agitated. She explains that she has just had an argument with her neighbor. As she is explaining it the neighbor comes in her door and says, "You better not be talking to your therapist about me." The client screams at her to get out of her house.

This type of unexpected intrusion would not happen in an office setting. While it does give in-vivo exposure to what the client is experiencing, it is also an example of sessions being "maliciously observed by outside parties" (Lustgarten et al., 2020, p. 26).

About forty-five minutes into the video session the client asks her clinician if she would like to see the room renovation project she has been working on. The clinician agrees and the client takes her on a "tour" of the work being done in her house. While she is walking around with her video phone, the clinician sees a man in the background. Immediately she asks the client who is also in the room with her only to learn it is the handyman who is helping her remodel! It becomes clear that this man was able to hear both client and clinician. The clinician expresses her concern and the client says "Oh, he's okay."

Clearly this situation represents a confidentiality breach but since the clinician was not told of the person in the background, is she at fault? Does ignorance of a breach exonerate one from sanctions? This above scenario points to the need to have an informed consent specific to the provision of telehealth which includes both the clinician's and the client's roles, rights, and responsibilities. Would it be appropriate to include in such consent the client's responsibility to inform the clinician if another person is in the room? Might it be a best practice to check each time with the client to see if they are in a private setting?

At the next video session with the same client the clinician notes that the client is in a different space than usual.

Clinician: "Where are you? I don't recognize the space you are in."

Client: "I'm in my bedroom upstairs with the doors shut because the carpenter is downstairs and I know how you feel about that!"

Clinician: "How do YOU feel about it? I am just trying to protect your privacy and confidentiality. Would you bring him to your session if we were meeting in person? [client laughs] He shouldn't be privy to our conversations unless you want him to be and then I need permission."

Client: "I know, I get it. I appreciate it."

The ethical breach became a teachable moment that the client absorbed both cognitively and behaviorally.

Preparation is an important step to setting up a telehealth practice. Preparation for telemental health includes choosing a secure platform, learning how to use it, and creating the necessary intake and informed consent paperwork. Receiving telemental health services is similar to face-to-face services in that treatment approaches, methods of engagement, setting goals, providing treatment, and monitoring outcomes may be similar. The context and environment in which these services are provided are different. There are potentials for different types of privacy breaches when technology is used. There may be unexpected disruptions or equipment failures. A client may decide to suddenly sign off of the technology without the clinician having a chance to discuss something further. Even the physical distance between the provider and client creates a need for planning and preparation in cases of emergency, like psychiatric hospitalization.

Telemental health adds a layer of considerations that is different than face-to-face sessions. Clinicians may need to practice first with a client before beginning regular therapy sessions. Both the clinician and client may need time to become familiar with the nuances of a specific software or application. They will likely need to discuss potential problems and solutions in order to reduce reluctance or anxiety about using technology. Having a client practice with the platform or other elements of technology also makes for a more robust informed consent; practice helps the client better understand the format that they are consenting to.

Telehealth etiquette skills are not necessarily intuitive and need to be taught (Gustin et al., 2020). Such skills "lay the foundation for a successful telehealth encounter with providers and patients" (Gustin et al., 2020, p. 91).

Consider these scenarios:

Client calls into the telehealth session while she is walking home from the grocery store. Should the clinician advise her to call back when she gets in a more private place?

Client tells the clinician to hold on a minute while she goes to the bathroom. Surprisingly. the client takes the phone into the bathroom with her.

Client asks the clinician to hold on because someone was at the door. Clinician hears her accepting a package. Client explains she just got a medication delivery.

Client does the telehealth session while she is driving. She has the video on the dashboard and reception varies. She tells the clinician to hold on because she has to stop and pick up her daughter.

Client puts the laptop on the kitchen counter during the session while she makes dinner.

Client in his wheelchair attends the video session shirtless.

These actual telehealth occurrences demonstrate how telehealth lends itself to an air of informality not usually seen in an office setting. The sometimes more casual nature of telehealth can have the benefit of increasing authenticity and "humanness" in the therapeutic encounter and also can be disconcerting to both clinicians and clients who prefer a relationship with distinct boundaries.

These scenarios demonstrate the potential for telehealth to take on a casual nature and raise other questions. Should there be a dress code? What are the norms in an office-setting and do violations of these create a problem? Should it be the same? Should clinicians dress professionally, casually, or in business casual? In instances where an agency is employing the clinician there may be formal platforms and policies that dictate the clinician's behavior while conducting telehealth. But even in scenarios where it is at the discretion of an individual clinician (e.g., when in private practice), that clinician should employ practices that demonstrate respect for the client and the process. In other words, regardless of setting, clinicians will still set the tone for their sessions when using telehealth.

Social platforms characteristically are informal and this informal approach can interfere with the development of professional interpersonal relationships (Gustin et al., 2020). "The casual use of technology for social connections can actually have a disinhibiting effect on behaviors" (Gustin et al., 2020, p. 88). In addition, the buffer of technology in interpersonal interactions can result in less empathic connection. Increasing reliance on the Internet may influence one's ability to pick up on behavioral nuances, non-verbal cues, and facial expressions. "Telehealth requires professionals to develop the patient-professional relationship in a different and more deliberate way than during in-person encounters...most failures with telehealth uses are associated with these human factors or soft skills" (Gustin et al., 2020, p. 89).

The pandemic resulted in an unusual shared stressor between client and clinician and telehealth may be commonly employed with community disasters (e.g., wildfires, hurricanes) where clinicians and clients are both affected by the disaster. How much emotional or other types of clinician self-disclosure is appropriate in such shared trauma?

Self-disclosure has always been a central topic for clinicians to consider ethically and one in which the clinician usually has control. In the face of telehealth, self-disclosure is increasingly evident and less control is maintained by the clinician.

A clinician is conducting video sessions from her home office. She has worked to make it private and professional looking so she is surprised when the client opens the session by saying, "Where are your dogs?" The clinician is a little uncomfortable thinking that perhaps their relationship has become too familiar. Her coworker suggests that it could be viewed positively as the client is reassured by their mutual like of dogs.

A clinician is forced to reschedule a session because her daughter is very ill. She has never cancelled a session with this long-term client and feels the need to explain

why to the client since it is so uncharacteristic. The client is very understanding and they are able to arrange a telehealth appointment in a private space in the setting where the clinician's daughter is receiving care. Two days later the client calls the clinician to let her know she is thinking of her and hoping all is well. She prefaces her voicemail with "I hope this is not too personal, but if you need someone to talk to or something, I just wanted you to know you could call me."

Has a seismic shift happened in their relationship and if so, was it the result of an ethical boundary breach by the clinician in sharing information that made the client feel she needed to take care of her therapist? Or has it equalized the relationship in an authentic show of concern?

A client and clinician have had a steady therapeutic relationship in-person for almost a year. They often start the session with "chit-chat" about current events or interesting experiences but have remained attuned to the client's clinical needs for the most part. At the start of the pandemic they quickly transitioned to telehealth and the chit-chat portion of their sessions grew longer. They shared the Netflix series each were watching and decided to watch particular episodes during the week so they could discuss it together at each session.

Has telehealth dissolved a therapeutic boundary in quest of a "just-like-me" connection, or has it equalized the relationship in a therapeutic way? Can it be said for certain whose needs this type of interaction is serving? Is it an example of a dual relationship blossoming? Is this self-disclosure on the therapist's part beneficial to the client?

Creating psychological and physical boundaries are another mainstay of the therapeutic relationship, which are affected by telehealth. The increased accessibility can result in text messages or calls outside normal business hours, blurring the physical boundary of the professional relationship and increasing the risk of boundary violations Strategies to curtail boundary violations can include setting clear parameters and rules for technology use in both verbal agreements and informed consents.

Confidence in addressing dilemmas demands that the clinician can identify whether the telehealth interaction poses a chance of client exploitation. For example, if a client begins to whisper during the session because a family member is in the next room and she doesn't want them to hear what she is saying, what does the clinician do?

A client explains to the clinician that she is in the garage because she doesn't want her abusive boyfriend to know she is in a session. In previous sessions he has made transparent excuses to be near her while she talks to clinician. The client asks the clinician to please "play along" and pretend she is her sister if the boyfriend walks in unexpectedly.

Doing a session from her bedroom, a client is describing to the clinician upsetting disagreements she has encountered with her roommates during the past week. Suddenly there is a loud banging on her bedroom door. A roommate bursts in and proceeds to scream at her and hurl insults. The client tells her to leave because she is in a therapy session but the roommate continues to barrage her with insults and

name-calling. Does the clinician handle it in the same way she might handle an argument in-person?

In the second example, the altercation is not really similar to an argument between partners in an office setting because one participant is not invited. Ensuring the client is both physically and emotionally safe would be the clinician's priority. In this actual case, the client often referred to the incident in subsequent sessions and the clinician continued to validate her responses and reassure the client. The client stated,

"I already thought you believed me but now you really believe me!"

In a different scenario:

During a session a client tells the therapist that he shared their last conversation with his partner so that the partner could understand him better. The therapist asks for clarification and learns that the client has been recording their sessions for subsequent review by the partner.

Clinicians are cautious to preserve a client's confidence, but what level of confidentiality can the clinician expect? Is sharing his expertise without his knowledge a form of plagiarism or theft of intellectual property? Some clinicians have written Right and Responsibilities for both parties in the therapeutic relationship. Minimally, an informed consent could include that recording of any kind is not to be done without the consent of all participants. As another risk management strategy, practitioners should ensure that their malpractice insurer covers cyber-liability and the provision of telebehavioral health services.

Creating an Informed Consent Form for Telehealth

Informed consent is typically obtained before or during the intake session that outlines in writing the client and clinician's plan and guidelines for treatment. Informed adult consents typically include treatment issues, such as:

- privacy and confidentiality (e.g., HIPAA)
- type/s of services that will be provided
- client rights and responsibilities
- clinician rights and responsibilities
- potential risks and benefits of services
- guidelines for appointments (e.g., scheduling and canceling)
- billing and fees associated with treatment
- insurance coverage
- record keeping
- rules governing disclosure
- clinician contact information
- other issues relevant to practice (The Center for Ethical Practice, 2020)

Informed consent forms for telemental health services will contain all of the elements typical for traditional consent forms, but with added information that relates specifically to telehealth technology. Informed consent for telebehavioral health should include risks associated with telebehavioral health, exceptions to confidentiality, backup plans for technological difficulties, interruption of service, and emergency plans. Some insurers require that a separate informed consent is signed for telehealth services as a condition of reimbursement (Felton, 2020).

Informed consent for telemental health services includes information that specifically relates to the risks, benefits, responsibilities, and roles of using technology. For a telemental health consent, clinicians may want to include:

- the name of the software, service, platform, or tool that will be used,
- the benefits (e.g., convenience, flexibility) and risks of using telemental health services (e.g., potential for faulty Internet connections or disruptions),
- conditions under which telemental health may be inappropriate and the rights of the therapist to make this determination,
- rights of the client to decide not to use telemental health technology,
- telemental health setting and environment (e.g., etiquette, space, video skills),
- back-up communication plan,
- information about scheduling and canceling appointments (e.g., reminders of the time zones for the client and practitioner, especially if each is located in a different time zone),
- safety and emergency plan,
- security and privacy concerns,
- whether or not video or audio recordings are allowed, and
- any other telemental health-related issues specific to a given circumstance.

Some telemental health technology providers offer electronic consent forms built-in to their platforms. Clinicians should review these forms and other documentation forms to ensure that they cover the scope of practice for telemental health. The most important feature of informed consent for treatment that a client signs is that it includes written protocols and procedures, including emergency situations. Providers should know the contact information for clinics and hospitals local to the client's physical location in case the client needs emergency intervention. Clinicians may need to establish collaborative relationships with local agencies so that crises are handled efficiently. All of this information should be included in an informed consent form.

There are various professional informed consent form templates available. The National Association of Social Workers (2020) offers a sample of an informed consent form as a template at https://www.socialworkers.org/LinkClick.aspx?fileticket=fN67-dWQReM%3d&portalid=0. Figure 1 provides another example of an informed consent form for telemental health services.

Video conferencing platforms (e.g., Skype, Zoom for Healthcare, Doxy.me, Inovalon, Google GSuite Hangouts) and agencies or sole practitioners are usually required to sign a Business Associate Agreement (BAA) to maintain HIPAA compliance. The need for clients to be aware of possible privacy concerns using these platforms should be included in any informed consent. Practitioners should also take every precaution when using these applications such as using password enabled connections.

Figure 1. Telemental Health Services Informed Consent Form Example

Client Name:

I, _____, agree to participate in teletherapy with a mental health provider at [Name of Agency].

This means that:

I authorize information about my medical and mental health care to be transferred electronically through an interactive video connection between [Originating Site Agency Name, if applicable] and [Distant Site Agency or Provider].

- I understand that I will be informed of the identities of all people who are present during the teletherapy session and informed of their purpose for attending the session.
- My provider has explained how the teletherapy system works and how it will be used for my treatment.
- My provider has explained how this service will differ from face-to-face sessions, including emotional reactions that may arise due to technology use.
- I understand that my provider will not be physically present during my teletherapy session. Instead, we will see each other electronically.
- I understand that teletherapy is an evolving modality for therapy. As such, there may be potential risks that may not yet be recognized.
- Potential risks include: a) at times the video image may be unclear or inadequate, b) a disruption in the connection may occur, or c) in rare circumstances, the information may be intercepted by unauthorized persons.
- I authorize the release of information pertaining to me determined by my mental health care providers or by my insurance company for the purpose of processing insurance claims.
- I understand that at any time, I may decide to discontinue teletherapy sessions with my provider. My provider will refer me to a local mental health provider who can provide face-to-face services.
- I agree to take every precaution to preserve the confidentiality of my sessions, such as ensuring that calls are taken in a safe and secure location to the extent possible.
- I understand that, under the law, my mental health provider may be required to report to the authorities any information suggesting that I have engaged in behaviors that are dangerous to myself or others.
- My provider has explained the risks and benefits of receiving teletherapy. I understand that I still may need to see a specialist in-person.
- I understand that information from my teletherapy sessions will be protected by HIPAA privacy laws. I may request a copy of my electronic record in writing.

The contact information for my provider is:

- Name:
- Email:
- Phone:

These are the names and phone numbers of my local emergency contacts:

- Local mental health provider:
- Primary care physician:
- Local hospital emergency room:

I voluntarily consent to participate in telemental health services using videoconferencing equipment for the care, treatment, and services deemed necessary and advisable under the terms set forth herein.

Name: Date:

Parent or Legal Guardian: Date:

BEST PRACTICES IN TELEMENTAL HEALTH

The National Association of Social Workers (NASW) advises that before providing telebehavioral health services social workers should check with their:

- state licensing board;
- client's state licensing board if it a different state from where the social worker is practicing;
- malpractice insurance/professional liability insurance carrier; and
- client's payor (e.g., private insurance, Medicaid, and Medicare; Felton, 2020).

Regulations and restrictions vary per state for telemedicine services. Most states require that the practitioner be licensed in the state where the client resides or receives services. However, some latitude was afforded during the pandemic with great variability among states with respect to the current status of these regulations. In addition, different payors have differing parameters regarding the use of telehealth. For example, at the start of the pandemic some payor regulations required that the provider use an interactive audio and video platform that afforded real- time communication. However, after public pressure and advocacy by organizations, such as the NASW, citing that many underserved populations have no access to the Internet, this requirement was lifted and audio only sessions are also permitted. Also, initially telehealth was only authorized by CMS to clients who had a prior relationship with the provider. Again, this restriction was lifted so that new clients needing services could obtain them via telehealth.

Several training programs in telebehavioral health have emerged offering suggestions and guidelines. Some even offer a certification in telemental health although not necessarily sponsored by accredited organizations. Anecdotally, the following tips to improve the effectiveness of telehealth encounters have been provided by telehealth platforms, trainers, and researchers. Clinicians should:

- familiarize themselves with the technology before sessions to avoid technical difficulties, such as glitches, muted microphones, lighting glares, video or audio failures, and too high levels of volume;
- maintain eye contact by looking into the camera, rather than the spot on the screen where the client's face appears;
- exaggerate facial expressions and other physical gestures to facilitate the client's sense of the clinician's engagement and key communications;
- communicate to the client verbally about what the clinician is doing if looking or moving away from the camera so that their actions are not misinterpreted; and
- take 10–15-minute breaks between telehealth sessions to move or stretch their body and clear their mind.

The scenarios presented earlier demonstrate the casual feel afforded to telehealth. Should there be a dress code? What is the norm in an office-setting? Should it be the same? Should clinicians dress professionally or casually or in business casual? Again, the tone set by the clinician during sessions should be one that shows respect for the client and the process.

Because telehealth has made engaging in services more accessible and convenient, many practitioners and patients have made telehealth their preferred, or even only, treatment option. Clinicians should not delegitimize telehealth by calling in-person therapy "real therapy" or, for clinicians in fee for service models, by charging less for virtual sessions (although some 3rd party payors do still reimburse teletherapy at lower rates than office visits). Describing telehealth services on a website is also important. The APA (2023) created a checklist to help determine whether telehealth is a suitable option. Some items on this checklist include:

- considering the client's cognitive and clinical status (including suicidality, community safety, and health concerns);
- inquiring if there will be an adult on location and what consents are needed if a minor is involved; and
- evaluating the client's access to the resources necessary to conduct on going telehealth sessions (e.g., Internet access, reliable access to devices and private spaces).

In addition, clinicians should evaluate any cultural, symptomatic, or countertransference elements related to the context of telehealth use that are relevant in determining the appropriateness of telemental health treatment. Although these areas are important in any clinical assessment, they are particularly important in telebehavioral health encounters because of the heavier reliance on verbal contributions.

Offer Orientation to the Technology Before Beginning Treatment

Clinicians should first know how to operate the equipment and use the telemental health platform before beginning work with actual clients. Practitioners should provide an orientation to clients about what telemental health is and how it is to be provided. This orientation can include reviewing intake paperwork, obtaining informed consent, explaining emergency protocols, and teaching clients how to physically use the equipment and/or telemental health software platform. If teleconferencing systems are used (e.g., Polycom), clinicians should know how to operate the equipment and assist clients if they are using a similar system at a remote location. Clinicians can experiment with video displays, video lag, eye contact, picture-in-picture display, and other elements before beginning a session. Orientation to the technology can include walking clients through the use of links or sending screen shots about entering URLs or using links to access the virtual waiting room, enter the virtual session room, explain privacy precautions, emergency protocols, and explain about the importance of lighting, audio, and connectivity. For example, some systems will cut video in order to improve the audio by increasing bandwidth if connectivity is an issue. The platform the clinician or agency chooses to use will likely offer some type of client orientation.

Video Etiquette

Videoconferencing requires certain knowledge and skills that may be unfamiliar to practitioners who only provide face-to-face treatment. Being on camera may make providers and/or clients feel uncertain and uncomfortable seeing themselves in a picture-in-picture display. A client will rely on the clinician to know how to use the equipment and may need guidance about

video etiquette as well. There are several basic rules for videoconferencing (George, 2020; Hart, 2020; Mendoza, 2020):

- Use the mute feature when not speaking, if necessary, to minimize background noise and feedback.

- Be on time or log-on a few minutes before the session is to begin.

- Ensure that the technology works correctly. Practice beforehand to avoid problems. Make sure the computer camera, speakers, and microphone work.

- Choose the proper software and hardware for telemental health services. Have a back-up plan for contact if the software and/or hardware fails.

- Wear work-appropriate professional clothing and expect the client to wear what they would to an office visit.

- Frame the camera correctly. Ensure that the camera is positioned so that the client has the feel of direct eye contact during the session.

- Have the right lighting. Make sure that both the client and clinician are clearly visible.

- Pay attention during the session. This may seem like a basic idea, but in a telemental health environment there is the potential for a significant number of distractions during a session. For example, if dogs start barking that someone is at the front door, how does the practitioner handle this in the middle of a session? If a child enters the session room and waves on camera to the client, how does the clinician handle this?

- Take into account there may be lag time in visual and audio transmission. Allow for sufficient time to receive and express information without overlap or interruption.

- Use a direct, wired connection (e.g., ethernet) rather than Wi-Fi if available. This will reduce the risk for transmission disruption by an Internet glitch.

- Download all materials needed for the session in advance. Many software platforms have a screen-sharing function that allows a practitioner to show the client what is on the computer screen. This could be a resource website for the client, a chart of progress throughout therapy, or an example of a visual reference. When clinicians use the screen-sharing function, it is important that they know the clients will be able to see everything on the screen, including browser tabs, website names, and other information that may be personal or otherwise inappropriate to share with clients.

- Choose an appropriate virtual background. Some platforms allow for the individual users to change the background image for videos. A clinician may want to change the background if video conferencing is in a cluttered room or office. Users can choose a blank

background or one that has animation or images. Whatever background is chosen, it should not be distracting.

Video etiquette is an important part of conducting an effective session. Clients may not have the skills or experience with telemental health technology. So, it is important for the practitioner to have mastery in order to guide the client toward proper use. In addition to practical matters of communicating, seeing and hearing clearly, appropriate etiquette of video conferencing conveys to the client that this type of contact is professional and structured. Often practitioners need to practice their skills, especially when learning a new platform or platform features. During the session with the client is not the appropriate time to try different functions and features.

Video Space

When clinicians offer telemental health services, they should be cognizant of the nuances of the virtual office (i.e., the video space). The video space is the visual area in both the client's and practitioner's screen. Video space that is cluttered or interrupted by passersby can distract from the focus of the session. There are several components about video space about which clinicians should be aware. Preparation and planning are key tools in helping to make sure that video conferencing telehealth is a success.

A clinician should make sure that everyone is clearly seen in the video space. In order to do this, the equipment and office surroundings must work together to increase compatibility and comfort for the client. This can mean choosing a particular space that is free from distractions or that has walls that are coated in soothing colors rather than stark white. A smaller room may help to make the client feel more secure; it may feel more like an actual therapy room. A clinician can evaluate the field of view (i.e., the view that is captured by the camera angle) to make sure that there is a wide enough visual space so that each person, or group of persons, is seen clearly. Some cameras have remote automatic focus functions that can track the movements of a person and keep the image clear. Some cameras can be configured to accommodate different amounts of people. If a clinician does a lot of group work, this type of camera could be helpful. This camera feature enables the clinician to easily adjust the angle and lens and with facial recognition features, can create the ideal zoom and focus.

Another aspect of video space is audio. Some microphones are better than others. Inexpensive or out-of-date microphones and speakers may have trouble filtering out ambient noise. Microphones and speakers can create an overlap effect when multiple people are talking at the same time. A quality sound system can filter or reduce noise while enhancing voice clarity. Microphone noise range can vary depending upon the product. The direction of the microphone is important as well. If you have clients seated in a group around a table, then a 360-degrees microphone may be more helpful than one that is unidirectional.

The space where the session takes place is an important consideration. Excess sunlight or sunlight facing into the camera can affect picture quality (Barr, 2020). A balance of natural lighting with ceiling light can reduce shadows that can create distractions during a session (Barr, 2020). Use curtains or soft lighting to help enhance picture quality. Uncovered or cement floors can create excessive echo and sound distortion (Barr, 2020). Softening floors and walls with rugs and wall-hangings can help reduce echo.

Lighting is a crucial element of video conferencing. Barr (2020) offers tips about how to improve lighting to enhance videoconferencing:

- Avoid illuminating the surrounding walls too much; this makes faces appear darker on camera.

- Try to keep the contrast less than 1:1.5. In other words, keep the brightness lower on the faces than on the table or surroundings.

- Reduce sunlight to a comfortable level; excessive sunlight makes faces difficult to see and can be reflective in a camera.

- Adjust the brightness to a lower intensity on faces; work towards illuminating faces that feel comfortable to the viewer.

The room where the session is held is an important factor, but in practical terms, a room may be used for more than one type of activity. If the clinician is providing services from home, the "therapy room" may also serve as a dining area or living room. If the therapy room is in an agency, it may also be used as a conference room. When a clinician uses a space for telemental health services, prior to beginning a session, she may want to create a therapeutic space. Furniture placement is an important part of video space (Barr, 2020). A comfortable chair or sofa will have a different effect than a metal office or fold-away chair. Comfortable surroundings can provide both the clinician and the client and enhance the therapeutic value of the space. Pay attention to the location of the door and the impact on the display. An opened door that impedes the camera view is less than ideal. Similarly, the camera view should not be angled where people can enter the visual space or see the face of the other person.

The size of the video screen can impact a session. If the clinician uses a smaller screen, such as a cell phone screen, visual comfort may be difficult. A larger screen may be more comfortable; some video set-ups include multiple screens (Barr, 2020). However, client privacy and comfort are of key importance. Clinicians may want to avoid a larger screen if it is easily seen by people passing by.

Video Presentation Skills

Some clinicians may be more comfortable with video conferencing than others. Prior experience with these technologies and an evolved skill set can help individuals feel more confident and competent. However, most individuals must go through a learning curve and develop skills in order to become comfortable and competent. Video communication skills are important because a clinician's comfort and competence with the technology can put a client at ease. Some clients (and clinicians) may feel uncertain or insecure with their communication skills or appearance on a screen.

Basic therapeutic communication skills transfer easily from the face-to-face environment to the video conferencing work environment. Active listening involves paying close attention to what the other person is saying (Doyle, 2021). In face-to-face sessions, a clinician shows active listening by asking clarifying questions, maintaining eye contact, paraphrasing, and reflecting. In

video sessions, the subtle movements that are seen in a face-to-face session may not be easily seen by the client. The clinician's eye contact may be focused on the screen, rather than the camera depending upon its location. If the practitioner's sight line is skewed from the camera, the view on the client's screen may convey distraction or disinterest. The camera should be positioned so that the clinician's line of sight appears as much as possible to align with the client's sight line. The clinician can use conscious body movements, such as head nodding, to show attention. She can ask clarifying questions while being careful not to talk over the client with an awareness of lag time between video capture and voice.

Nonverbal language that is so essential in traditional services is also important in telemental health. Body language, such as eye contact, hand gestures, tone of voice, may be altered when using video conferencing technology (Doyle, 2021). Eye contact that is off-center with certain cameras can make either or both the clinician's and client's view appear slightly askew. If correcting the camera angle is difficult, other body language can be added, such as leaning forward and using facial expressions, which serves to convey the message that the clinician is listening closely.

Doyle (2021) offers specific suggestions for using body language and body position to enhance therapeutic presence. Clinicians should:

- Avoid slouching in the chair; rather, they can lean forward to encourage engagement.

- Use hand animation and facial expressions to project presence and attention.

- Avoid drinking, eating, or looking at their phone during the session.

- Take care to eliminate fidgeting or trembling limbs, such as bobbing legs or repetitive hand movements, in order to create a "quiet" visual presence.

- Observe the client's reactions to your statement to detect understanding or misunderstanding.

- Ask clarifying questions, if needed.

- Encourage the client to ask questions and let the practitioner know when something is not understood.

- Avoid looking at the clock or phone during a session. The clinician can set a timer or glance at the clock on the computer screen.

Practitioners may recognize that video conferencing is not the ideal option for a particular session. If Internet connection is poor on either the clinician's or the client's end, a forced telesession may be frustrating and counterproductive. If a client seems distracted, for example if their children are home from school, it may be better to reschedule the session for a time when there are less distractions. Sometimes a client's body language will display disinterest or distraction, such as yawning, looking at a phone, or broken eye-contact. A practitioner can inquire about these nonverbal cues to see whether another time would be better.

Appearance is an important factor for video presentation. Both practitioners and clients should dress as they would for an in-person meeting, following the workplace's dress code (Chaudhry, 2020). When at home, one may be inclined to dress informally, but care and attention should be given to dress. If a client is dressed inappropriately for a video session, the clinician should address this as they would for an in-person session, perhaps asking the client to change or put on a sweater. Clothing patterns, such as stripes or polka dots, may be distracting in a video session (Chaudhry, 2020). The camera may or may not automatically adjust if the individual wears a bright white or black shirt, causing shadows or lack of lighting on the face. Plain, neutral colors may be a good choice for video.

During a video session, the clinician should be aware of the need to signal when she wants to talk. Typically, in face-to-face situations, there are small and subtle visual cues to let individuals know who wants to speak. These cues may be less obvious on a video call, especially when there is sound delay. A clinician can raise her hand or use a chat function to let an individual know that she has a question (Chaudhry, 2020). The speaker should speak clearly and at a normal volume; there is typically no need to raise the volume because the microphones are usually sensitive. A speaker may want to adjust the pace of speech, opting for a slightly slower rate since the interaction occurs across video and may have lag.

If the clinician wants to share her screen or pull up a document or email for reference, she should explain that to the client beforehand (Chaudhry, 2020). Remember when a person shares their screen, the entire screen is shared including bookmarks, browser tabs, and other images. Long stretches of silence may indicate that the Internet connection has been lost. Communicating one's intentions and actions is important. In a video conference, it is difficult to differentiate when someone is looking at the video or looking at another screen on the computer.

The following scenario demonstrates the utility of all these tips:

During a session the discussion topic reminded the clinician of a relevant graphic that he wanted to share with the client. He only had a paper copy of the graphic so while the client was talking, he surreptitiously tried to open his file drawer and retrieve the paper.

As he was doing so the wires on his headset connected to his laptop got entangled and the headset went flying off his head. The client of course stopped talking and tried to suppress a giggle. The therapist apologized and explained what he had been doing and, luckily, they both got a laugh out of his clumsiness. With a different client his actions could have just as easily turned into an irritation or even an empathetic failure.

Another scenario speaks to immediate ethical decision-making sometimes encountered in telebehavioral health:

A new client is smoking cannabis, during a session. It is over Zoom, so the therapist is not personally/ directly impacted by it. The client doesn't feel like they have a problem with substances, but they do identify a history of self-medicating and low motivation.

This scenario raises several questions:

- Is the cannabis medically prescribed? If so, is it comparable to a client taking a pill during an in-person session?
- How would the client answer if asked 'would you smoke cannabis if we were meeting in the office?'
- If it is not prescribed what is the reason for the obvious action? Should it be addressed clinically or legally?
- Is the client a teen? If so, does the incident reflect an act of defiance, power-seeking, or self-soothing? Do parents need to be notified?
- Does the therapist view it the same as drinking a beer during a session?
- Does such behavior need to be included in a practice policy or a patient's bill of rights/responsibilities?
- Does the therapist document the behavior in the chart notes?

Risks of Teletherapy

To better identify best practices in teletherapy it is important to anticipate some of the inherent risks of and ethical arguments against providing services online. Stoll and colleagues (2020) found that some of the top ethical arguments against online psychotherapy were issues related to privacy and confidentiality, technological competence, communication, and crisis care.

Privacy, Confidentiality, and Data Security

Protection of confidentiality is important for both client and clinician. Implicit in this assumption is also the protection of privacy. In many cases the clinician has less control over the setting where services are received, therefore must make reasonable attempts to replicate the privacy that is offered by an in-office setting. Risk-management strategies include ensuring the video platform is HIPAA compliant and having a discussion with clients about what they can do to ensure safety in their setting. It must be recognized that confidentiality is less protected in teletherapy thus having a separate informed consent acknowledging this fact is an optimal practice.

> *For an initial telehealth session, a clinician asks the client where she is and if she is in a place where their conversation is going to be private. The client ensures that she is in a room in her cousin's house and no one can hear. However, the clinician thinks she hears people talking in the background. To be safe, she puts her headphones on as the client begins talking to a woman off screen. They start making plans for the evening interrupting the session for about two full minutes.*

Most breaches of confidentiality are not with the platforms, but rather with ordinary situations like public or non-related exposure. For example, a client calls in to a session via FaceTime sitting in a Starbucks, using ear buds. She insists she feels safer and more "anonymous" there than in her home. Should the clinician insist she go somewhere else more private or accept the client's perceived sense of comfort? The answer is 'it depends' and requires documentation. Some clients may not have access to more private settings, for example, a client in a group home

who shares living and sleeping space with other residents. Brainstorming with the client to ensure more secure confidentiality is recommended. Using earbuds or headphones is one way to partially ensure confidentiality. If the clinician deems that the optimal situation is not available but clinical intervention is still warranted, documentation of the setting in which it occurred and attempts to ensure privacy and confidentiality is paramount. There may be situations where the clinician just does not feel comfortable in proceeding with the session and that too should be documented.

Technological Competence

Yet another situation over which clinicians have little control is the technology itself. According to Stoll and colleagues (2020), "Online psychotherapy creates new challenges to therapist competences which brings about the need for new forms of training and education, especially technological competences… [which] is not only needed by the therapist, but also by the patient" (p. 9).

Even with the best of technological training on the clinician's part, there are at least two devices involved that increase the possibility of tech fails because they can happen on the clinician's end, the client's end, or both. Best practice requires clinicians to create a backup plan for technology failures and to inform the client of the backup plan at the beginning of session or even written in the informed consent or policies. Backup plans should address who will initiate another platform or call to continue the session. Clinicians should have the client's contact information (e.g., phone number) on hand during a telehealth session so that it is immediately available to the clinician in the event of a technology failure.

Communication Issues

Telehealth may not be appropriate for all clients as therapeutic interaction can vary greatly between in-person and online care (Stoll et al., 2020). Possible differences include difficulty expressing empathy and feelings, time lag and lack of spontaneity, and absence of non-verbal cues, which can cause misunderstanding, miscommunication, empathetic failures, and impaired intervention. Communication issues may also arise due to privacy, confidentiality, and technological issues.

It is best practice for clinicians to assess the appropriateness of telehealth for a client at each session. Does a different symptom presentation preclude telehealth? Are they in a safe private area? Is available technology sufficient? Are they sufficiently adept with technology use? For example, a client who suffered a stroke or traumatic brain injury may have aphasia residuals that make communicating via telehealth more frustrating. Teletherapy may be contraindicated if a client or clinician have strong accents that make it difficult or impossible to communicate. Additionally, clients who have thought disorders may find the process suspicious. Teletherapy may also be contraindicated if clients are actively abusing substances or if a couple asking for teletherapy has a history of interpersonal violence. Any situation in which the clinician feels an unmanageable ability to intervene, protect clients, or control the process may preclude the use of telemental health.

Crisis Care

Many clinicians understandably feel the lack of control inherent in the teletherapy platform and may question if crisis situations are detectable and addressable via technology (Stoll et al., 2020). If a client experiences a crisis during or after a session, what might happen?

Although there are some additional considerations, the approach to a client crisis via telehealth is fundamentally the same as in-person (e.g., safety plans with the names and numbers of collateral contacts) with some preventive risk management strategies to mitigate the circumstances created by the distance. Crisis resources in the community should be readily identified and a crisis plan in the informed consent for teletherapy is advisable. Telehealth is also beneficial in addressing some crises as "…it may provide more immediate access to services and disclosure of suicidal or homicidal tendencies may be easier online" (Stoll et al., 2020, p. 6).

In addition to a crisis plan, the risk for suicide can also be assessed and mitigated in the telehealth environment. A comprehensive suicide prevention plan via telehealth:

- identifies the physical location of the client;
- determines the client's local crisis numbers;
- assesses the client's social support system and makes specific suggestions;
- uses evidence-based suicide risk assessments; and,
- has a back-up plan for reestablishing contact if technology fails.

A clinician had been seeing an adolescent (17 y.o.) with a history of depression and self- injury (in the form of cutting) for about a year. Half of their treatment had been conducted in-person prior to the pandemic then switched exclusively to telehealth, usually via video, sometimes by phone. One hour prior to a scheduled video session the client called the clinician crying hysterically. She had experienced some "mean girl" bullying at school. The client told the clinician she was sitting in a drugstore parking lot. The clinician inquired as to what she needed to get at the drugstore and was told "scissors for a school project". The answer seemed highly unlikely and with probing the client said she had already purchased the scissors and was cutting her thighs. The clinician advised the client to drive home where she resided with her parents and text or call her as soon as she was there. No consent to talk to her parents existed and state law gave mental health consent to teens at fourteen years old. As soon as they hung up the clinician second-guessed her instruction to the client and decided to call the police to do a wellness check since the client had reported furtherance of the intent to harm. A short time later the client texted the clinician and said she was home. The clinician was reluctant to believe her until the client sent her an angry text, acknowledging that the police were there and told the clinician in no uncertain terms that they were "done". The clinician's decision to err on the side of the client's safety ended in an irreconcilable therapeutic rupture.

Did the clinician do the right thing? If she was sued by the client could she justify the breach of trust? Is there anything that could have prevented this outcome? Had this session occurred in-person it seems clear that it could have been handled more adeptly and certainly points to a risk of telemental health. Reviewing limits of confidentiality is always wise, and particularly important when sessions are not held in-person and the adequate assessment of the crisis may be compromised. A specific informed consent could be applied to this situation and such consents specific to telehealth should include crisis plans.

Multicultural Considerations

Cultural considerations are those practices that encompass cultural humility and/or a client's preferences, beliefs, values, rituals, customs, and differing world views. Culture is embedded in personal identity and defines group membership and behaviors. Many individuals have intersectional identities that are part of macro- and micro-cultures. These cultures include gender, gender expression, sexuality, ethnicity, race, religion, and socioeconomic status (Stubbe, 2020).

Cultural humility is a term that addresses the challenges of becoming fully competent in a culture of which one is not a member (Johnston et al., 2018). Because an individual who is not part of a particular culture cannot fully understand what it is like to be a member of a particular culture, s/he must assume a stance of openness and an acknowledgment of inherent personal biases. Cultural humility is process-oriented while cultural competence is destination-oriented. Clinicians who practice cultural humility know they can never be fully competent, but commit to learning and interacting in ways that are respectful of another's culture. Cultural humility appreciates the cultural experiences of others, recognizes power imbalances, and acknowledges implicit biases (Scult, 2021).

Using technology to interact can be a complicated endeavor when working with clients who are members of different cultures. Technology presents greater risks for misunderstandings and miscommunication between providers and their clients (Johnston et al., 2018). To improve the chances of clear communication, a provider can take into consideration several issues. Johnston and colleagues (2018) provide several examples of ways that practitioners can convey cultural humility while using technology. A clinician can:

- Adapt clinical style and process to accommodate different communication styles.
- Wear proper attire and have an appropriate room set-up for direct in-home videoconferencing.
- Be aware of different understandings and uses of voicemail, return calls, and texts.
- Be cognizant that clients may not understand text message abbreviations, such as lol (laughing out loud) or smh (shaking my head) or that usings all capitalized letters may be construed as shouting or yelling at the person receiving the text.
- Understand that there are different understandings and expectations regarding the immediacy of response to emails.

Telepractitioners who practice cultural humility are aware that they may be prone to specific assumptions about culture and environment based upon the clinical setting or client's home (Johnston et al., 2018). For example, they will refrain from particular assumptions, if a client who lives in a rural setting has hunting paraphernalia in the background. They incorporate contextual knowledge of a client's environment, culture, and resources into treatment approaches.

There are benefits to the cross-cultural service telehealth service provision. Telemental health services provide increased access to care and can be used to reach a wide range of diverse populations, such as Native Americans and Alaska Native communities, Latino populations, and international clients (Johnston et al., 2018). It allows providers to offer services to diverse age groups, settings, communities, and environments. Individuals from underserved and marginalized communities can have access to services that were previously inaccessible. Telebehavioral health practitioners can provide outreach, education, and community engagement in creative ways to

address the needs of communities. They can target specific populations through an array of culturally-specific platforms. Also, because of limitations related to distance and availability clients using telehealth services will possibly have access to greater choices of clinicians and may choose to connect with a clinician from a similar cultural background (e.g., ethnicity, sexual orientation) if so desired or deliberately choose a clinician from a different background if so desired. Finally, technology now provides greater access to translation services. Videoconferencing platforms as well as text-based, mobile, and voice recognition services can help bridge language barriers that can inhibit service provision.

Communities that have difficulty with access to services due to geographic, economic, or medical limitations can be served in their homes by providers who practice cultural humility and are culturally competent and who may not be in the immediate area. However, there can be challenges as well. Communities whose members are underserved or remote may be reluctant to try services with unfamiliar technologies. There may be limited connectivity, such as in rural areas. In this case community members can invest in the process as peers or advocates to help others obtain needed services and resources.

Further, clinicians can advocate for greater inclusion of diverse populations and perspectives in the development and implementation of mental health technologies and promote cultural relevance in the selection of certain technologies (Scult, 2021). While many technologies can have a far reach to multiple client populations, telepractitioners are still responsible for practicing with diverse populations within the parameters of their knowledge, values, and skills. When treating diverse individuals, it is not appropriate for teleclinicians to expect their clients to speak English fluently. Knowing one's own abilities and limits of working with specific populations is not only a part of regular clinical practice, but also telepractice. For example, it may not be appropriate for a telepractitioner to use the automatic closed-captioning with a deaf individual as a replacement for American Sign Language. A telepractitioner may need to make referrals to other providers who are better prepared to deal with specific needs of a particular individual.

Risk Management in Documenting Encounters

Many ethical risks occur in the documentation or lack of documentation of clinician encounters. Essentially, documenting telebehavioral encounters is the same as recording in-person encounters; however, more contextual documentation is prudent, such as where the client was during the encounter, or if there was someone else accompanying the session, either intentionally or unintentionally.

When working with a client, there should be no information in the client's chart that either the client or another professional or regulatory body would be surprised by. For example, there should be nothing in the chart about yourself ("I wasn't feeling too good during our session so couldn't give the client much attention") or your personal feelings about the client ("This client is really frustrating"). Documentation is open to public and client review. Documentation is always for an audience. The four features to consider for risk management and documentation (explained in Figure 2) are

- content,
- language,

- credibility, and
- access.

Figure 2. Documentation Strategies for Risk Management

Content	Language	Credibility	Access
Should have a clear, readable structure.	Use easily understood language.	Provide evidence for statements and outcomes.	Write for an audience.
Balance between too much and too little information.	Avoid repetition.	Avoid spelling and grammatical errors.	Remember personal (shadow) notes are not confidential.
Include sufficient detail to enable service delivery.	Avoid defamatory or dehumanizing language.	Provide timely documentation.	Be familiar with legal, regulatory and agency mandates governing release of records.
Avoid excessive detail, over-documentation or extraneous information.	Use clear, unambiguous and specific wording.	Acknowledge and notate errors.	Provide security for records, physically and electronically.
Use separate notes when seeing couples or families.	Do not use casual language or excessive professional jargon.	Do not speculate without substantiation.	Ensure and monitor client access to records as requested.

ETHICAL ISSUES IN TELEHEALTH WITH CHILDREN, COUPLES, AND GROUPS

Working with Children Virtually

Citing an increasing evidence base, the American Psychiatric Association (2023a) has promoted the use of telepsychiatry with children and adolescents. Evidence shows that parents, teens, and referring providers are highly satisfied with telepsychiatry and telemental health and that various disorders (e.g., anxiety, obsessive-compulsive disorder, oppositional defiant disorder) have been successfully treated via this method of service delivery. The American Psychiatric Association (2023a) highlights the following regarding youth and telemental health care:

- Telepsychiatry may provide a more desirable alternative to the traditional clinic setting for youth who pose challenges (e.g., behavioral).

- Although school-based telepsychiatry is not well detailed in literature, its use is increasing quickly. It allows for more youth in need to obtain services and allows parents more opportunities to be involved.

- Telepsychiatry allows assessment of youth in a naturalistic and ecologically valid setting. It also minimizes disruptions to the family's day.

- The use of child and adolescent telepsychiatry in correctional settings is growing and its benefits are twofold. First, youth in correctional settings have high rates of under-diagnosed and/or untreated psychiatric disorders and telepsychiatry offers needed care. Second, correctional staff can learn about the role of mental health disorders in adolescents' conduct problems.

- Technology use in youth is prevalent, so researchers are looking into how technology could positively and negatively change care. However, comfort in the use of technology to access care is evident.

Engaging children and teens in treatment in-person can be challenging, and, for some, the element of virtual engagement and frustration increases for both child and clinician. As such, teletherapy now includes teleplay therapy, which was used occasionally before the pandemic and now is recognized as a viable approach. Filial therapy (i.e., therapy that teaches parents how to engage with their children in ways that are therapeutic) may be easily adapted to the online environment and is a collaborative way to encourage a child's engagement. Adapting play therapy to a virtual environment raises both ethical and clinical questions.

What is teleplay therapy and what is it not?

> "…teleplay therapy refers to the use of a systematic approach to play therapy using play and play therapy interventions in a virtual context by a professional mental health practitioner expressly trained in play therapy. Teleplay would refer to use of the systematic approaches to play therapy and use of play therapy interventions, the difference in teleplay is that the clinician has not been specifically trained in play therapy" (Fazio-Griffith et al., 2020).

Play therapy and supervision of teleplay requires attention to the ethical situations that can occur working exclusively with children and/or adolescents. A variety of ethical concerns can become present during the play therapy process, which, in turn can influence the supervision process. Ethical issues salient in teleplay therapy primarily speak to clinician competence, record-keeping, and confidentiality.

Working with Couples and Families

Couple counseling provided outside the office setting can be conducted via telehealth video platforms, audio only, or even via texting, email, or chat as some of the therapy subscription businesses provide.

Gould (2021) summarizes the pros and cons of virtual couple counseling, which is illustrated in Figure 3. Topping the positive aspects of couple counseling online is the convenience and accessibility factor. Scheduling is easier for busy couples, especially if childcare poses another barrier. In some cases, the comfort of clients being in their own home lends itself toward sharing

personal matters more readily than being in an unfamiliar setting. Sometimes, the goal of couple counseling is "to do something different" to break patterned problematic couple behavior. Learning new skills in the office does not always carry back to the home setting. Practicing skills in the home setting may help them "stick". Certainly, the online format is perfect for couples in long-distance relationships since it puts them together for counseling.

Drawbacks include the inability to read non-verbal cues or body language for both client and clinician. Similarly, it might be more difficult to establish a personal connection or therapeutic alliance. Interruptions are bound to occur from technology or kids or pets. Finally, the lack of physical presence makes it harder for a therapist to control or intervene with behavioral or emotional outbursts (Gould, 2021).

Figure 3. Couples Counseling Online

Benefits	Drawbacks
Convenient and Accessible	Can't read body language
Comfortable	Interruptions
Easier skills learning in vivo	Less personal
Available to long-distance relationships	Harder to control

In the rare peer-reviewed literature regarding telehealth and couples and family counseling, Wrape & McGinn (2019) reviewed the unique clinical, ethical, and practical considerations of using telehealth to provide couple or family therapy. These areas of concern were categorized into five domains:

- confidentiality/privacy,
- safety,
- managing multiple patients in session,
- therapy process, and
- logistics for treatment planning (Wrape & McGinn, 2019, p. 297).

The usual privacy and confidentiality concerns are magnified when providing couple or family therapy.

> "…having multiple members participate meant that some common methods for increasing privacy (i.e., the use of headphones) are not readily available…if members are connecting from different locations, there is the possibility that someone else may be present outside the view of the screen without the other family member's knowledge" (Wrape & McGinn, 2019, p. 297).

Additionally, therapist awareness of this possibility may inhibit their willingness to provide open and honest feedback or contribute to avoiding certain areas of discussion.

As previously mentioned, an informed consent is the best means a clinician can use to address these elements. Sharing the responsibility for their own privacy and confidentiality is clearly indicated and stipulated in an informed consent for telebehavioral health. Documenting any

inadvertent potential confidentiality risks (e.g., other family members walking in and out of the room in which the couple is taking the video telehealth session) is further protection and a solid risk management strategy.

Safety is another ethical and clinical consideration that is heightened in couples or family counseling. Even just having to sit closer together to be seen simultaneously on the screen could make for uncomfortable scenarios. In an office setting the therapist could interview partners separately to assess for safety or ask one to take a "time-out" in the waiting room or walk around the parking lot to cool down if tensions escalate. The same physical separation may not be so easily enforced in a telehealth session. Wrape and colleagues (2019) recommend that therapists establish where couples are at the beginning of each session in the worst-case scenario that police might have to be called. Some therapists ascribe to the view that this modality is contraindicated when severe violence or substance abuse is present and will refuse to treat couples and rather choose to work exclusively with one individual or the other. Others assess that some intervention where the therapy is not escalating the situation is safe to provide in certain situations (e.g., it is the only help the couple will receive). Decisions about teletherapy in families where there is violence must be made in consultation with experts on family violence intervention.

Managing multiple patients in session is another concern inherent to couple/family therapy, both in-person and online. Imagine four people in family therapy squished on a couch where they cannot sit comfortably in view of the camera. If emotions get intense, will the physical proximity become problematic? Novice and seasoned therapists alike can easily envision an angry teenager leaving the session to the sound of a slamming door as he locks himself in his bedroom. This escape might not happen as easily in an in-person session particularly when the angry teen needs a ride home.

Couples may also split their attention in session as one may be answering kids' homework questions or another is folding laundry, which would not happen in-person. Situations like these can be curtailed with limit-setting and a mutual expectation that the session should be treated no differently than an in-person session as much as possible. Wrape and colleagues (2019) see such examples as teachable moments in which problem-solving and communication skills can be assessed or practiced as couple work to set the parameters demanded of the therapy process.

There are certain elements of the conjoint therapy process that are altered dramatically if not totally missing in a telehealth platform. Subtle interpersonal or body language can easily be missed. The intimacy and vulnerability evoked in particular marital therapy approaches (e.g., Imago, Emotion Focused Therapy, Gestalt) require attention to mind-body connections and body awareness, which is much more difficult to observe and use through a screen. The techniques of Structural Family Therapy or Transformative Systemic Therapy, such as joining, positioning, or posturing are also not easily accomplished via video. Additionally, in-home family therapy is severely limited by telehealth. Therapists cannot as easily provide in-vivo parenting or communication guidance when much of the interaction is taking place off screen. Conversely, techniques such as reenactments could translate well to a virtual platform where participants can "perform" for the camera.

Group Counseling via Telehealth

Possible breaches to confidentiality could stem from a member attending in a non-secure location where others could see or hear group members, members recording or taking a picture of

the group or leader and using the information for unethical or illegal purposes. A separate signed informed consent spelling out do's and don'ts of participating in a group via teletherapy is a necessary safeguard.

Despite increased risk to members and clinicians, "online groups also offer[ed] therapists an efficient and effective way to support the mental health of the larger community during the COVID-19 epidemic" (Whittingham & Martin, 2020).

Suggested rules for clients attending group are similar to expectations for individual sessions.

- Be in a safe, secure space where the client can be free of distractions and speak freely.
- Clothing worn should be similar to what is expected in an office setting.
- Be familiar with the technology necessary to participate in the group fully, such as secure Internet, no other devices being used.

Group members must have the technological means to attend the group. This includes being on a secure Internet connection, rather than public or free Wi-Fi. The clinician and group members should keep the video on and do their best to be attentive and engaged. Phones or computers should be put on airplane mode to minimize interruptions. If the privacy of the client's location is an issue, wearing headphones or keeping the volume low can prevent sound from travelling to another room.

Follow any group-established policy regarding if a member, or the entire group, gets disconnected. If the group agrees, this may include having a member call in for the remainder of the session. Adhere to the group policy about how to handle a breach in confidentiality, such as a nonmember bystander witnessing the group or someone walking into a room while the group is meeting. For more information the American Group Psychotherapy Association (AGPA) provides specific tips on using technology for group therapy (AGPA.org).

The American Group Psychotherapy Association (AGPA, n.d.) provides a quick start guide for facilitating virtual groups. They encourage providers not to be daunted, stating "getting started in telehealth practice is not as difficult as it might seem so long as you take your time to understand the ins and outs of providing mental health services utilizing online tools and platforms." They direct providers to assess the following prior to starting a telehealth group:

- **Client suitability:** Make clinical determinations on a client's suitability for group and, separately, telehealth services considering cognitive functioning, clinical presentation and risk level, and level of independence operating technology and technology literacy.

- **State laws and licensing regulations about providing telehealth:** An app related to telemental health laws is provided via Epstein Becker Green.

- **Provider access to the proper telehealth technology and necessary equipment:** The AGPA advises that a computer or tablet with an Internet connection is the bare minimum required to begin a telehealth group, but that clinicians should also consider the quality of their microphone, camera, speakers or headphones, Internet speed, and the platform they will use to facilitate their groups (e.g., some platforms charge more for the multidevice use necessary to facilitate a group).

- **Provider's familiarity with the ethical issues associated with telehealth practice:** Clinicians are responsible for knowing the risks and benefits of providing services in a group modality via telehealth (and communicating these to clients), state laws and statutes governing the practice, and ethical guidelines from their professional organizations.

- **Client access to technology, necessary equipment, and appropriate setting:** Clinicians must assess each group member's access to the technology and Internet strength. In order to engage in effective telehealth, a private space to use for the sessions, and each group member's ability to address any confidentiality issues for the group as a whole (e.g., roommates or family members, thin walls where people can be overheard, device used) is necessary.

- **Provider tasks necessary to reduce and manage risks associated with telehealth practice:** Clinicians must consider how they will implement their practice in ways that manage risk, ensure their competence, establish crisis plans for each group member (especially considering each client's physical distance, risk level, and appropriateness for the group, emergency contacts, and emergency procedures for the client's location), ensure security and privacy of provider and each group member in relation to physical location and the software used to facilitate group sessions, explain risks to confidentiality and privacy inherent in the use of the technology, and obtain informed consent that acknowledges those risks.

SUPERVISION VIA VIDEOCONFERENCING

This quote provides an optimistic viewpoint of the changes in supervision with telehealth: "…the experiences grappling with ethical consideration within an ever-evolving clinical and global landscape will inform how these trainees operate as future supervisors, with an enhanced awareness of the challenges trainees may face" (Desai et al., 2020, p. 10).

As did the delivery of behavioral health services, the provision of clinical supervision abruptly switched to a telehealth platform when the pandemic forced social isolation. Even the best clinical supervisors may not be prepared or trained in this modality. Ethically this situation speaks to the competence standard in most codes of ethics. The NASW (2021) stipulates competence according to sufficient training and specifically addresses the issue of technology use:

> *1.04 Competence*
> (a) Social workers should provide services and represent themselves as competent only within the boundaries of their education, training, license, certification, consultation received, supervised experience, or other relevant professional experience.
> (b) Social workers should provide services in substantive areas or use intervention techniques or approaches that are new to them only after engaging in appropriate study, training, consultation, and supervision from people who are competent in those interventions or techniques.
> (c) When generally recognized standards do not exist with respect to an emerging area of practice, social workers should exercise careful judgment and take responsible steps

(including appropriate education, research, training, consultation, and supervision) to ensure the competence of their work and to protect clients from harm.

(d) Social workers who use technology in the provision of social work services should ensure that they have the necessary knowledge and skills to provide such services in a competent manner. This includes an understanding of the special communication challenges when using technology and the ability to implement strategies to address these challenges.

(e) Social workers who use technology in providing social work services should comply with the laws governing technology and social work practice in the jurisdiction in which they are regulated and located and, as applicable, in the jurisdiction in which the client is located. (NASW, 2021)

The NASW Code of Ethics also addresses technology in supervision.

Supervision and Consultation

(a) Social workers who provide supervision or consultation (**whether in-person or remotely**) should have the necessary knowledge and skill to supervise or consult appropriately and should do so only within their areas of knowledge and competence.

While the NASW Code weaves technology use into different sections, The American Counseling Association (ACA; 2014) Code of Ethics devotes an entire section to Supervision and one entirely for distance technology. Section F addresses Supervision, Training and Teaching.

F.2. Counselor Supervision Competence

F.2.a. Supervisor Preparation
Prior to offering supervision services, counselors are trained in supervision methods and techniques. Counselors who offer supervision services regularly pursue continuing education activities, including both counseling and supervision topics and skills.

F.2.c. Online Supervision
When using technology in supervision, counselor supervisors are competent in the use of those technologies. Supervisors take the necessary precautions to protect the confidentiality of all information transmitted through any electronic means.

Section H addresses Distance Counseling, Technology and Social Media.

Introduction
Counselors understand that the profession of counseling may no longer be limited to in-person, face-to-face interactions. Counselors actively attempt to understand the evolving nature of the profession with regard to distance counseling, technology, and social media and how such resources may be used to better serve their clients. Counselors strive to become knowledgeable about these resources. Counselors understand the additional concerns related to the use of distance counseling, technology, and social media and make every attempt to protect confidentiality and meet any legal and ethical requirements for the use of such resources.

H.1. Knowledge and Legal Considerations

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).

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 award of pertinent legal right and limitations governing the practice of counseling across state lines or international boundaries.
(ACA, 2014)

Of course, by extension the supervisor may be supervising the supervisee's own provision of telehealth. Thus, conveying these competency standards to the trainee is incumbent on the supervisor. It is the supervisor's responsibility to address the supervisee's competency in the provision of telehealth services and its concomitant challenges; however, in some instances, trainees may be more literate in the use of technology, which may evoke varied feelings about competence between the supervisor and the trainee.

The American Psychological Association (APA) Code of Ethics (2017) is less specific. The only mention relevant to supervision and telehealth is found in Section 2 addressing competence.

(c) Psychologists planning to provide services, teach, or conduct research involving populations, areas, techniques, or technologies new to them undertake relevant education, training, supervised experience, consultation, or study.
(e) In those emerging areas in which generally recognized standards for preparatory training do not yet exist, psychologists nevertheless take reasonable steps to ensure the competence of their work and to protect clients/patients, students, supervisees, research participants, organizational clients, and others from harm.

The APA published Guidelines for the Practice of Telepsychology (2013) because "…telecommunication technologies in the provision of services and the continuous development of new technologies that may be useful in the practice of psychology support the need for the development of guidelines for practice in this area" (2013, p. 792). They also recognized the opportunity of increased client/patient care via telecommunication. Although the APA guidelines do not reference the use of technology for supervision, the standards of competence and confidentiality addressed in the document can be applied to telesupervision.

The National Board for Certified Counselors (NBCC) Code of Ethics (2023) is also vague when discussing supervision and telehealth. The code of ethics standards regarding competence say:

81. Counselor educators shall stay current with, and be well informed about, counseling-related professional issues and developments.

82. Counselor educators shall engage in teaching and student supervision activities only with respect to their areas of professional knowledge and competence.

The NBCC standards regarding telemental health do not address supervision specifically, but they do say:

91. Counselors shall provide only those telemental health services for which they are qualified by education and experience.
92. Counselors shall carefully adhere to legal requirements when providing telemental health services. This requirement includes legal regulations from the State(s) in which the counselor and client are located. Counselors shall document relevant State requirements in the relevant client record(s).

The American Association of Marriage and Family Therapists (AAMFT) Code of Ethics addresses the provision of online therapy or supervision in Standard VI. In particular, Standard 6.1 outlines the steps MFTs should take before commencing therapy or supervision services through electronic means. In addition to Standard VI, the remaining provisions of the AAMFT Code of Ethics also apply to online therapy or supervision.

For social workers, counselors, psychologists, and marriage and family therapists adjusting supervision to an online platform could include addressing the setting, expectations of both supervisor and supervisee, and the potential differences from in-person supervision. Consideration needs to be given to protecting the confidentiality of supervisee, supervisor, and any client information being discussed.

A supervisor providing telesupervision ensures that she is in a private setting with no distractions for the session. Although the supervisee is wearing headphones so that the supervisor cannot be heard by anyone but her, her husband frequently walks by and is seen in the background making dinner. What is the expectation? If her husband's presence doesn't bother the supervisee should the supervisor say anything? Would the supervisee bring her husband along to supervision in-person?

During their meeting, a contracted fee-for-service supervision session, the supervisee mentions that she replayed their previous session because it was so helpful and even shared it with a colleague during the past week. The supervisor asks for clarification only to find out the supervisee had recorded their previous supervision session. There are ethical transgressions here. First, the supervisee recorded the session without the supervisor's knowledge and secondly, she shared it with a colleague, without the supervisor's permission. Although the supervisee might consider it flattering, the supervisor's expertise has been provided gratis.

Adjusting the structure and process of supervision includes developing some type of hybrid format in which there is remote live supervision with additional "homework" for the supervisee. Telesupervision can be provided via various video platforms. In rare circumstances, supervision may be provided via audio only platforms; however, it is prudent to check to ensure that audio only hours count toward licensure as some states require live video sessions.

When taking an ethical approach to online supervision, it is important to assess preparedness to do so. Thinking about legal and competency issues can help with this. Some questions for supervisees and supervisors to ask themselves when contemplating online supervision include:

- Is online supervision legally permitted where I practice?
- What is my profession's ethics code regarding use of technology?
- Is the supervisor required to complete training about providing supervision online?
- Have I received proper training in the technology that I will use?
- Do I have the competency skills required to participate in online supervision?
- Can the supervisor adequately assess if a potential supervisee is appropriate for telesupervision appropriately?
- Can the supervisor teach any skills that are lacking with respect to the use of telesupervision?
- Have I considered ways of assessing performance and providing constructive criticism online?
- Has the supervisor developed policies and procedures specific to telesupervision?
- Have the roles and responsibilities of each person involved in the telesupervision relationship been clearly communicated?
- In what ways are client and supervisee privacy and confidentiality in the provision of telesupervision ensured? What are the limitations?
- Does the written supervisory contract address some of the differences and expectations for telesupervision?
- Does my client informed consent form indicate that supervision may be provided online, which may add another security risk?
- Is my virtual platform HIPAA compliant? Do I need a Business Associates Agreement (BAA)?
- Can I ethically provide or participate in group supervision with my current platform?

Skills of telesupervision demand creative ways of building rapport, providing a holding environment, attending to expressive cues, both verbally and physically. It also may require self-reflection about performance anxiety. What is the supervisor's own comfort level providing supervision in this way? Does the supervisor find it a watered-down version of clinical supervision, and easier to cut sessions short? Does the supervisor deal with explorative questions, non-participation, or silence differently? What is the expectation of supervisees' behavior and participation in telesupervision (e.g., dress code, distractions, multi-tasking)?

Group supervision via videoconferencing platforms presents exponential challenges described previously. Each issue previously discussed can pose a security or confidentiality risk for each member and their clients; however, with proper protocols confidentiality can be maintained and videoconferencing technology can confer all the benefits of group supervision and peer group consultation.

STANDARDS PERTINENT TO TELEHEALTH

> Establishing sound standards of care is an essential feature of professional practice. Standards of care constitute the measuring rod with regard to acceptable practice in a profession (Reamer, 2018, p. 258).

To keep up with the ever-changing landscape of cybertechnology in behavioral health, standards have emerged in three areas: (a) regulatory law: government regulations, either through legislation or through licensing boards; (b) codes of ethics: standards promulgated by national professional associations (e.g., ACA, APA, NASW, NBCC); and/or (c) standards of professional practice: best practice standards or guidelines adopted by professional groups and associations (Reamer, 2018).

Several states have adopted telehealth legislation. In the absence of legislation, licensing bodies have also established standards as their mission is to protect the public. The APA, NASW, ACA, and NBCC all have codes of ethics that have enforceable rules and aspirational guidelines for best practice. Several categories relevant to telehealth include those dealing with competence, privacy, confidentiality, conflict of interest, boundaries, social justice, practice settings, self-determination, and supervision. In addition, the NASW has revised their Code of Ethics and in collaboration with the Association of Social Work Boards (ASWB), the Clinical Social Work Association (CSWA), and the Council of Social Work Education (CSWE) has established specific standards and guidelines to address the use of technology in clinical care (NASW, 2017). Standards of care are meant to guide professional behavior and provide a basis for adjudicating sanctionable offenses or lawsuits. Standards regarding telehealth have emerged in most health care professions. The NASW published Technology Standards (2017) which includes a total of 55 standards integrated into four sections of the technology standards:

- Provision of Information to the Public,
- Designing and Delivering Services,
- Gathering, Managing, and Storing Information, and
- Social Work Education and Supervision.

The American Medical Association (AMA) and APA have also published standards specific to the use of cybertechnology. In addition, the American Psychiatric Association has developed an extensive and evolving "Telepsychiatry Toolkit" to inform psychiatrists about legal, financial, and ethical use of remote or distance psychiatry, which cognate professionals may find pertinent to the provision of telemental health (American Psychiatric Association, 2023b).

Practicing Across State Lines

The ease of access afforded by telehealth would imply that services could be provided to anyone anywhere. However, practitioners generally cannot practice across state lines. As of this writing, no federal provisions allow mental health professionals to practice teletherapy over state lines; clinicians must register or be licensed in their client's state to provide teletherapy. The

general directive is that treatment can only be provided to a client who is currently residing in the state where the clinician is licensed. Therefore, a client must be receiving services while physically located in a state where the clinician is licensed and the clinician has to be licensed in the state where the clinician is physically located while delivering services.

A frequently asked question is what if the client or clinician is temporarily out of state on vacation or business? Can therapy be provided? No clear guidance exists, some states specify, some don't. It is a risk to do so and safely handled by providing only short-term consultation. To be on solid ground clinicians should check the licensing board and relevant legislation in the state where they practice or where the client resides. However, some states waived licensing requirements to practice across state lines, with some time restrictions or other variability in implementation.

Telehealth Training

Many states do not require training in telehealth but, again, checking specific state requirements is recommended, as well as making sure that telehealth is included in a practitioner's liability insurance coverage.

Some states have additional requirements that apply to therapy or supervision through electronic means. Some professional standards strongly suggest it. The NASW, ASWB, CSWE, and CSWA Standards for Technology and Social Work Practices (2017) states in Standard 1.01:

> Social Workers who choose to provide electronic social work services shall do so only after engaging in appropriate education, study, training, consultation and supervision from people who are competent in the use of this technology to provide social work services.

Subsequent standards emphasize the need for continuing education to keep current with emerging knowledge related to the delivery of electronic social work services. Members should check their state's licensure law or contact their state licensure board.

SUMMARY

The previous slow growth of telebehavioral health experienced a rapid increase necessitated by the COVID-19 pandemic shut-down. Behavioral health practitioners adjusted quickly to the demands of providing services via virtual platforms and continue to do so. This type of service provision carries unique ethical challenges.

Common telebehavioral encounters have been identified with suggested best practices and tips for effective and ethical service delivery, acknowledging risks and situations specific to specific modalities and populations. Relevant professional association guidelines and codes of ethics and standards have been reviewed.

Telebehavioral health, along with clinical supervision via telehealth, currently take center stage in the delivery of mental health services and its permanence in the field seems highly likely. Ensuring ethical and effective practice requires awareness, training, and a multi-layered level of competence.

REFERENCES

Aboujaoude, E. (2019). Protecting privacy to protect mental health: The new ethical imperative. *Journal of Medical Ethics, 45* (9), 604–607.

Aljedaani, B. & Babar, M. A. (2021). Challenges with developing secure mobile health applications: Systematic review. *JMIR mHealth and uHealth*, 9(6), e15654. https://doi.org/10.2196/15654

American Counseling Association. (2014). 2014 ACA Code of Ethics. https://www.counseling.org/resources/aca-code-of-ethics.pdf

American Group Psychotherapy Association. (n.d.) Internet, Social Media, & Technology *Quick Start Guide to Telehealth.* https://www.psychiatry.org/File%20Library/Psychiatrists/Practice/Ethics/APA-COVID-19-Ethics-Opinions.pdf

American Psychiatric Association. (2021, October 1). COVID-19 related opinions of the APA Ethics Committee. https://www.psychiatry.org/File%20Library/Psychiatrists/Practice/Ethics/APA-COVID-19-Ethics-Opinions.pdf

American Psychiatric Association. (2022, October). *Resource document on best practices in synchronous videoconferencing-based telemental health.* https://www.psychiatry.org/getattachment/b87211d5-81bb-4d4f-af73-9caa738c2a1c/Resource-Document-Telemental-Health-Best-Practices.pdf

American Psychiatric Association. (2023a). *Child & adolescent telepsychiatry.* https://www.psychiatry.org/psychiatrists/practice/telepsychiatry/toolkit/child-adolescent/introduction

American Psychiatric Association. (2023b). *Telepsychiatry toolkit.* https://psychiatry.org/psychiatrists/practice/telepsychiatry/toolkit

American Psychological Association. (2013). *Guidelines for the practice of telepsychology.* https://www.apa.org/pubs/journals/features/amp-a0035001.pdf

American Psychological Association. (2017). *Ethical principles of psychologists and code of conduct.* https://www.apa.org/ethics/code/ethics-code-2017.pdf

American Psychological Association. (2023). Office and technology checklist for telepsychological services. https://www.apa.org/topics/disasters-response/telepsychological-services-checklist

American Telemedicine Association. (2020). ATA's Standardized Telehealth Terminology and Policy Language for States on Medical Practice. https://www.americantelemed.org/wp-content/uploads/2020/10/ATA-_Medical-Practice-10-5-20.pdf

Barr, S. (2020, February 6). How to design a killer video conference room. *LookingPoint.* https://www.lookingpoint.com/blog/video-room-design

California Telehealth Resource Center. (n.d.). *What is telehealth.* https://caltrc.org/featured/what-is-telehealth/

Chaudhry, A. (2020, March 19). The do's and don'ts of video conferencing. *The Verge.* https://www.theverge.com/2020/3/19/21185472/video-confere-call-tips-zoom-skype-hangouts-facetime-remote-work

Cleveland Clinic. (2020). *COVID-19 is igniting a redesign of healthcare communication.* https://consultqd.clevelandclinic.org/covid-19-is-igniting-a-redesign-of-healthcare-communication/

Code of Federal Regulations. (2023). *45 CFR §164.312.* https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

Coverage to Care. (2023). *Telehealth for providers: What you need to know* (Publication No. 12121). U.S. Department of Health and Human Services, Center for. https://www.cms.gov/files/document/telehealth-toolkit-providers.pdf

Desai, A., Lankford, C., & Schwartz, J. (2020). With crisis comes opportunity: Building ethical competencies in light of COVID-19. *Ethics & Behavior*, 1–13. https://doi.org/10.1080/10508422.2020.1762603

Diaz, N. (2023, July 17). *Cleveland Clinic bets on telehealth to reduce costs, reach younger patients.* Brecker's Hospital Review. https://www.beckershospitalreview.com/telehealth/cleveland-clinic-bets-on-telehealth-to-reduce-costs-reach-younger-patients.html

Doyle, A. (2021, March 13). Communication skills for workplace success. *The Balance.* https://www.thebalancecareers.com/communication-skills-list-2063779

FAIR Health, Inc. (2023). *Monthly telehealth regional tracker, May 2023, United States.* https://s3.amazonaws.com/media2.fairhealth.org/infographic/telehealth/may-2023-national-telehealth.pdf

Fazio-Griffith, L. J., Marino, R., & Leeman, M. (2020). Ethical considerations for play therapy supervision. In *Techniques and Interventions for Play Therapy and Clinical Supervision* (pp. 1–16). IGI Global.

Federal Communications Commission. (2022). Getting broadband Q&A. https://www.fcc.gov/consumers/guides/getting-broadband-qa

Felton, E. (2020, March). *Telemental health*. Office of General Counsel. National Association of Social Workers. https://socialworkers.org/LinkClick.aspx?fileticket=evgx77RtVLI%3d&p ortalid=0y8i8M%3D&portalid=0

Froehlich, A. (n.d.). Bandwidth (network bandwith). https://www.techtarget.com/searchnetworking/definition/bandwidth?Offer=abt_pubpro_AI-Insider

GCFGLobal. (n.d.a). What is an application? https://edu.gcfglobal.org/en/computerbasics/understanding-applications/1/

GCFGLobal. (n.d.b). What is bluetooth? https://edu.gcfglobal.org/en/mobile-device-tips/what-is-bluetooth/1/

GCFGLobal. (n.d.c). What is the cloud? https://edu.gcfglobal.org/en/internetbasics/understanding-the-cloud/1/

GCFGLobal. (n.d.d). Inside a computer. https://edu.gcfglobal.org/en/computerbasics/inside-a-computer/1/

GCFGLobal. (n.d.e). What is an operating system? https://edu.gcfglobal.org/en/computerbasics/understanding-operating-systems/1/

GCFGLobal. (n.d.f). What is a mobile device? https://edu.gcfglobal.org/en/computerbasics/mobile-devices/1/

GCFGLobal. (n.d.g). Computer basics: Buttons and port on a computer. https://edu.gcfglobal.org/en/computerbasics/buttons-and-ports-on-a-computer/1/

GCFGLobal. (n.d.h). Protecting your computer. https://edu.gcfglobal.org/en/computerbasics/protecting-your-computer/1/

GCFGLobal. (n.d.i). Creating strong passwords. https://edu.gcfglobal.org/en/internetsafety/creating-strong-passwords/1/

GCFGLobal. (n.d.j). Your browser's security features. https://edu.gcfglobal.org/en/internetsafety/your-browsers-security-features/1/

GCFGLobal. (n.d.k). Internet safety: How to avoid malware. https://edu.gcfglobal.org/en/internetsafety/how-to-avoid-malware/1/

GCFGLobal. (n.d.l). Internet safety: Wi-Fi security. https://edu.gcfglobal.org/en/internetsafety/wifi-security/1/

Gillis, A. S. (2023). Digital signature. https://www.techtarget.com/searchsecurity/definition/digital-signature?Offer=abMeterCharCount_var2

George, A. (2020, March 27). The do's and don'ts of video conferencing etiquette. *ABC News.* https://abcnews.go.com/Technology/dos-donts-video-conferencing-etiquette/story?id=69836253

Goetter, E. M., Iaccarino, M. A., Tanev, K. S., Furbish, K. E., Xu, B., & Faust, K. A. (2022). Telemental health uptake in an outpatient clinic for veterans during the COVID-19 pandemic and assessment of patient and provider attitudes. *Professional Psychology: Research and Practice, 53*(2), 151–159. https://doi.org/10.1037/pro0000437

Gould, W.R. (2021). Pros and cons of online couples' therapy. *Verywell Mind.* https://www.verywellmind.com/the-pros-and-cons-of-online-couples-therapy-4843717

Gustin, T. S., Kott, K., & Rutledge, C. (2020). Telehealth etiquette training: A guideline for preparing interprofessional teams for successful encounters. *Nurse Educator*, *45*(2), 88–92. https://doi.org/10.1097/NNE.0000000000000680

Hart, M. (2020, March 25). Video conferencing etiquette: 10 tips for a successful video conference. *OWL Labs.* https://www.owllabs.com/blog/video-conferencing-etiquette

Health Resources & Services Administration. (2023a). *Medicaid and medicare billing for asynchronous telehealth.* Department of Health and Human Services. https://telehealth.hhs.gov/providers/billing-and-reimbursement/medicaid-and-medicare-billing-for-asynchronous-telehealth

Health Resources & Services Administration. (2023b). *Telehealth and remote patient monitoring.* Department of Health and Human Services. https://telehealth.hhs.gov/providers/preparing-patients-for-telehealth/telehealth-and-remote-patient-monitoring

Health Resources & Services Administration. (2023c). *Getting started with telehealth.* Department of Health and Human Services. https://telehealth.hhs.gov/providers/getting-started#types-of-telehealth

InstaMed. (2020). *Telehealth and the digital healthcare experience during COVID-19.* https://www.instamed.com/blog/covid-19-increases-demand-for-telehealth/

Istepanian, R. S. H. (2022). Mobile health (m-Health) in retrospect: The known unknowns. *International Journal of Environmental Research and Public Health 19*(7), 3747. https://doi.org/10.3390/ijerph19073747

Johnston, B., Shore, J., & Rabinowtitz, T. (2018). Clinical settings and models of care in telepsychiatry. In P. Yellowlees & J. Shore (Eds.), *Telepsychiatry and health technologies: A guide for mental health professionals* (pp. 97–136). American Psychiatric Association.

Lipschitz, J. M., Connolly, S. L., Van Boxtel, R., Potter, J. R., Nixon, N., & Bidargaddi, N. (2022). Provider perspectives on telemental health implementation: Lessons learned during the COVID-19 pandemic and paths forward. *Psychological Services.* https://doi.org/10.1037/ser0000625

Lustgarten, S. D., Garrison, Y. L., Sinnard, M. T., & Flynn, A. W. (2020). Digital privacy in mental healthcare: Current issues and recommendations for technology use. *Current Opinion in Psychology*, *36*, 25–31. https://doi.org/10.1016/j.copsyc.2020.03.012

McBain, R. K., Schuler, M. S., Qureshi, N., Matthews, S., Kofner, A., Breslau, J., & Cantor, J. H. (2023). Expansion of telehealth availability for mental health care after state-level policy changes from 2019 to 2022. *JAMA Network Open, 6*(6), e2318045. https://doi.org/10.1001/jamanetworkopen.2023.18045

Mendoza, N. (2020, March 23). 13 etiquette tips for video conference calls. *TechRepublic.* https://www.techrepublic.com/article/13-etiquette-tips-for-video-conference-calls/

Microsoft Azure. (2023). What is cloud computing. https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

National Association of Social Workers. (2017). *NASW, ASWB, CSWE, & CSWA standards for technology in social work practice.* https://www.socialworkers.org/LinkClick.aspx?fileticket=bq9JrB-oVm4%3d&portalid=0

National Association of Social Workers. (2021). *Code of Ethics of the National Association of Social Workers.* https://www.socialworkers.org/About/Ethics/Code-of-Ethics/Code-of-Ethics-English

National Board for Certified Counselors (2023). *National Board for Certified Counselors, Inc. Code of Ethics.* https://nbcc.org/Assets/Ethics/NBCCCodeofEthics.pdf

National Institute of Standards and Technology. (n.d.a). Application. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/application

National Institute of Standards and Technology. (n.d.b). Authenticate. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/authenticate

National Institute of Standards and Technology. (n.d.c). Bluetooth. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/bluetooth

National Institute of Standards and Technology. (n.d.d). Cloud computing. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/cloud_computing

National Institute of Standards and Technology. (n.d.e). Encryption. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/encryption

National Institute of Standards and Technology. (n.d.f). Firewall. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/firewall

National Institute of Standards and Technology. (n.d.g). Internet protocol. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/internet_protocol

National Institute of Standards and Technology. (n.d.h). Malware. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/malware

National Institute of Standards and Technology. (n.d.i). Mobile device. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/mobile_device

National Institute of Standards and Technology. (n.d.j). Operating system. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/operating_system

National Institute of Standards and Technology. (n.d.k). Port. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/port

National Institute of Standards and Technology. (n.d.l). Uniform resource locator. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/uniform_resource_locator

National Institute of Standards and Technology. (n.d.m). VPN. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/vpn

National Institute of Standards and Technology. (n.d.n). Web browser. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/web_browser

National Institute of Standards and Technology. (n.d.o). Authentication. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/authentication

National Institute of Standards and Technology. (n.d.p). Multi-factor authentication. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/ multi_factor_authentication

National Institute of Standards and Technology. (n.d.q). Phishing. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/phishing

National Institute of Standards and Technology. (n.d.r). End-to-end_encryption. In National Institute of Standards and Technology glossary. Retrieved August 3, 2023, from https://csrc.nist.gov/glossary/term/ end_to_end_encryption

National Security Agency. (2023). *Best practices for securing your home network.* https://media.defense.gov/2023/Feb/22/2003165170/-1/-1/0/CSI_BEST_PRACTICS_FOR_SECURING_YOUR_HOME_NETWORK.PDF

Pinola, M. (2020, March 9). Understanding Wi-Fi and how it works. *Lifewire.* https://www.lifewire.com/what-is-wi-fi-2377430

Reamer, F. G. (2018). Evolving standards of care in the age of cybertechnology. Behavioral sciences & the law, 36(2), 257–269.

Rezaee, R., Khashayar, M., Saeedinezhad, S., Nasiri, M., & Zare, S. (2023). Critical criteria and countermeasures for mobile health developers to ensure mobile health privacy and security: Mixed methods study. *JMIR mHealth and uHealth, 11*, e39055. https://doi.org/10.2196/39055

Scult, M. (2021). Cultural humility in digital mental health. *Psychology Today.* https://www.psychologytoday.com/us/blog/the-big-reframe/202108/cultural-humility-in-digital-mental-health#:~:text=Don't%20make%20assumptions.,cultural%20 identity%2C%20and%20their%20goals

Steidtmann, D., McBride, S., Mishkind, M. (2022). Patient experiences with telemental health during the COVID-19 pandemic. *Journal of Patient Experience, 9.* https://doi.org/10.1177/23743735221145077

Stoll, J., Müller, J. A., & Trachsel, M. (2020). Ethical issues in online psychotherapy: A narrative review. *Frontiers in Psychiatry, 10*, 1–16. https://doi.org/10.3389/fpsyt.2019.00993

Stubbe, D. E. (2020). Practicing cultural competence and cultural humility in the care of diverse patients. *Focus, 18*(1), 49–51. https://doi.org/10.1176/appi.focus.20190041

Techopedia. (2020). Platform. https://www.techopedia.com/definition/3411/platform

The Center for Ethical Practice. (2020). Informed consent for therapy services – Adult. https://centerforethicalpractice.org/ethical-legal-resources/practice-resources/sample-handouts/informed-consent-for-therapy-services-adult/

The Office of the National Coordinator for Health Information Technology. (2023). *Frequently asked questions.* Department of Health and Human Services. https://www.healthit.gov/faq/what-electronic-health-record-ehr

Tin, D., Hata, R., Granholm, F., Ciottone, R. G., Staynings, R., & Ciottone, G. R. (2023). Cyberthreats: A primer for healthcare professionals. *The American Journal of Emergency Medicine, 68,* 179–185. https://doi.org/10.1016/j.ajem.2023.04.001

Torous, J. & Wykes, T. (2020). Opportunities from the Coronavirus disease 2019 pandemic for transforming psychiatric care with telehealth. *JAMA Psychiatry, 77*(12), 1205–1206. https://doi.org/10.1001/jamapsychiatry.2020.1640

WhatIsMyIPAddress.com (2023). Unsecured network risks: How to stay safe online. https://whatismyipaddress.com/unsecured-network-2

Whittingham, M. & Martin, J. (2020). How to do group therapy using telehealth. *American Psychological Association.* https://www.apaservices.org/practice/legal/technology/group-therapy-telehealth-covid-19#:~:text=At%20a%20time%20when%20social, during%20the%20COVID%2D19%20epidemic

Wrape, E. R. & McGinn, M. M. (2019). Clinical and Ethical considerations for delivering couple and family therapy via Telehealth. *Journal of Merital and Family Therapy, 45*(2), 296–308. https://doi.org/10.1111/jmft.12319

Zhou, L., Thieret, R., Watzlaf, V., Dealmeida, D., & Parmanto, B. (2019). A telehealth privacy and security self-assessment questionnaire for telehealth providers: Development and validation. *International Journal of Telerehabilitation, 11*(1), 3–14. https://doi.org/10.5195/ijt.2019.6276