Telehealth Privacy Considerations for Behavioral Health Providers

Telehealth has become a key tool for delivering behavioral health treatment. This resource offers practical guidance for evaluating telehealth vendors and technologies, establishing appropriate safeguards, and supporting patients in protecting their privacy before, during, and after a telehealth encounter.

What you need to know

What is telehealth?

The U.S. Department of Health and Human Services (HHS) Substance Abuse and Mental Health Services Administration (SAMHSA) defines telehealth as the use of two-way, interactive technology to provide health care and facilitate patient-provider interactions.[1]

How is telehealth provided to patients?

Synchronous Telehealth

Synchronous telehealth uses interactive audio and video telecommunications systems to facilitate real-time communication between a healthcare provider and the patient when located at separate, remote locations.

Funded by Substance Abuse and Mental Health Services Administration

Asynchronous Telehealth

Sometimes called "store-and-forward," asynchronous telehealth uses telecommunication systems to enable healthcare providers to review information sent by patients without a real-time interaction.

Examples of asynchronous telehealth include:

- Uploading patient images, medical reports, lab results, digital medical imaging, or health histories to a patient portal that allows providers to review and prepare for upcoming consultations.
- Communicating with a healthcare provider via a secure messaging platform regarding health status and questions.
- Using digital devices to collect health information from patients for or on behalf of healthcare providers (also called remote patient monitoring):
  - Smart pill bottles and mobile apps to track medication adherence
  - Digital psychometric assessments and patient-reported mood tracking
  - Wearable devices that collect physiological data like heart rate variability, resting heart rate, and physical activity to accompany patient-reported data like mood.

Why is privacy important when providing telehealth in behavioral health settings?

Using telehealth technology without adequate privacy and security safeguards in place to prevent and protect against the exposure of health information can put patients and providers at significant risk. Privacy concerns can deter patients from talking about sensitive health information (e.g., their mental and emotional health) during a synchronous telehealth visit, potentially impacting the provider-patient relationship and treatment adherence and effectiveness.[2] Storage and transmission across technology platforms during asynchronous telehealth encounters can create multiple points of potential exposure after health information is collected from the patient. Health information stored in or transmitted via an unsecured telehealth modality can be shared accidentally with unintended recipients, such as a family member or different patient of the same provider. Bad actors can also intercept or steal health information from unsecured telehealth technologies to commit fraud against the patient (e.g., identity theft, insurance fraud, extortion, etc.).

Like in-person visits, most health information shared during telehealth interactions is protected by federal privacy laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and/or 42 CFR Part 2 (Part 2).[3] Some states have enacted laws protecting health information that apply to entities not subject to HIPAA or Part 2. These laws require providers and their organizations to implement reasonable

safeguards to protect patient health information and failure to comply can result in civil and criminal penalties.[4]

Implementing reasonable safeguards in the context of telehealth requires collaboration between the provider, patient, and the vendor who provides the technology. The following tip sheet is intended as a guide for providers in collaborating with patients and vendors.

PLEASE NOTE: The following tip sheet does not and is not intended to provide a comprehensive checklist of necessary steps a provider or their organization must take to comply with applicable legal and/or regulatory requirements. Resources, training, technical assistance, and any other information provided through the Center of Excellence for Protected Health Information do not constitute legal advice. For legal advice, including legal advice on other applicable state and federal laws, please seek out local counsel.

Tip Sheet

Before deciding to provide services via telehealth:

□ Consult with patients about their need for telehealth and any concerns they may have regarding telehealth, including the privacy and security of available telehealth technologies.

□ Determine legal and regulatory obligations applicable to the use of telehealth technologies by your organization (e.g., HIPAA, Part 2, and state health data privacy laws, rules, and regulations).

□ Develop a standardized process to evaluate digital technology and telehealth platform vendors and their products. Some considerations may include:

- The care setting in which the tool will be used, the target population, and the conditions the tool will be used to treat.
- The organization's network infrastructure (e.g., hardware and software) and connectivity (e.g., availability and bandwidth of secure Wi-Fi connection).
- The vendor's data collection, use, and disclosure practices.
- Capability to integrate tools with existing systems (e.g., electronic health record).
- Whether the vendor and/or the tool comply with applicable health data privacy laws, rules, and regulations.
- Whether the vendor and/or the tool has undergone a third-party security audit (e.g., SOC2, HITRUST) and the vendor's process for addressing security breaches.

Before using selected telehealth technologies:

□ Require vendors to agree to:

- A Business Associate Agreement (BAA) **if** you or your organization qualifies as a HIPAA covered entity. A BAA requires the vendor to protect patient health information, defines permissible uses and disclosures, and establishes other responsibilities between the parties.
- A Qualified Service Organization Agreement (QSOA) **if** you or your organization qualify as a Part 2 program. A QSOA is like a BAA in that it requires a vendor providing services to a Part 2 program to comply with 42 CFR Part 2 with respect to the Part 2 records the vendor receives from the organization.
- For sample contract provisions that satisfy both the BAA and QSOA requirements, please see our resource: Sample Provisions for Integrated QSOA/BAA to Disclose PHI with Contractors.

□ With your legal counsel or compliance professional, review the Terms of Use (sometimes referred to as the Terms of Service or Terms and Conditions) and any privacy documentation published by the technology vendor about the selected telehealth technology.

- Identify whether the vendor collects health information via the technology and whether the vendor uses or shares such information to provide the technology or for other business purposes.
- If the vendor intends to use and/or share health information for a business purpose other than providing the technology to you and your patients, require the vendor to limit such uses and sharing to only health information that has been de-identified in accordance with the HIPAA de-identification standards.[5]

□ With the technology vendor or an information technology (IT) professional, establish a plan for addressing technical and other support issues that occur while using the technology.

□ Develop, maintain, and enforce an organization-wide device policy. This policy should consider:

- Device privacy and security measures that must be in place before telehealth services are delivered using a device (e.g., multi-factor authentication, password protection, remote wipe capabilities, etc.).
- Prevention of and protection against the unauthorized or improper collection, use, disclosure, alteration, or destruction of a patient's health information.

□ Engage with an IT professional to implement privacy and security measures on every device used for telehealth, including:

- End-to-end encryption.
- Password protection with a strong PIN or password.
- Configuration to lock devices automatically after a period of inactivity.
- Capability to remotely delete all data stored on a device in the instance the device is lost or stolen.
- Storage of all information securely behind firewall protection.
- Safeguards to protect privacy and security of networking technology (e.g., Wi-Fi networks).

Before using telehealth to provide care to a patient:

□ Discuss with the patient whether they can obtain or use a secure, private device for the purpose of receiving telehealth services. It is preferrable that a patient receives telehealth services or uploads their sensitive information using a device to which only they have access.

- Instruct the patient to remove health information (e.g., messages, photos, videos, etc.) that they no longer need from their devices.
- If a patient receives telehealth services using a device they share with a family or household member, remind the patient that any sensitive information they upload, store, or communicate via the device may be accessible to others.

□ Understand whether the patient has access to secure, private networking technology that allows devices to connect to the Internet. Private networking technology includes the patient's home Wi-Fi or cellular data available on the patient's phone. Public networking technologies may expose a patient's data to hackers through unencrypted connections, rogue networks, and malware attacks. Examples of public networking technology include Wi-Fi accessible in a public space like a coffee shop, library, or airport.

□ Explain the importance of communicating health information via telehealth platform(s) vetted and approved for use by your organization rather than through communication channels that may not be secure. For example, patients should send health information they wish to communicate to their provider through a designated secure messaging platform instead of via a standard SMS text message.

While providing care using telehealth technology:

□ Ask the patient to:

- Find a place away from others where the patient can control who hears or sees the information they share.
- Consider wearing headphones and avoid using the speakerphone for synchronous telehealth visits.
- Use a personal device, if possible.
- Turn off other devices around them so those devices don't overhear or record the information they share (e.g., smart speakers, voice assistants, or other recording-enabled devices).

□ Avoid recording synchronous telehealth visits unless it is necessary.[6]

- If recording is necessary and before recording or transcribing any synchronous telehealth visit, inform the patient of the recording or transcription, how and where that information will be stored, and how the patient's privacy will be protected (e.g., recordings will be accessible only to authorized individuals).

PLEASE NOTE: Legal and regulatory requirements applicable to the recording and/or transcription of calls, including synchronous telehealth visits, vary by state. For legal advice, including legal advice on other applicable state and federal laws, please seek out local counsel.

□ Answer the patient's questions about the privacy and security of the telehealth technologies in use.

□ Be prepared to assist the patient in troubleshooting common issues that may arise when using telehealth technology.

- Collaborate with the patient to develop a back-up plan if technology fails.

For More information

Resources: This resource is one of many that are available within the CoE-PHI's resource library, which can be found at coephi.org.

Training/Technical Assistance: You can request brief, individualized technical assistance and join our mailing list for updates, including news about the publication of new resources and training opportunities on our website.

Date: September 2026

This resource was authored by:
Ashleigh Giovannini, J.D., LL.M., CIPP/US

References

1. *U.S. Substance Abuse and Mental Health Services Administration, SAMHSA Publication No. PEP21-06-02-001, Telehealth for the Treatment of Serious Mental Illness and Substance Use Disorders (2021).*
2. *Id.*
3. *For more information on federal privacy laws, please see our resource titled About the Laws: Making Sense of Federal Privacy Laws for Substance Use Disorder (SUD) and Mental Health Treatment.*
4. *U.S. Department of Health and Human Services, Privacy and security for telehealth (2024).*
5. *45 C.F.R. §164.514(a)-(b).*
6. *U.S. Department of Health and Human Services, Develop a privacy and security telehealth strategy (2025).*