AFLP FAQ: Televisits during COVID-19

Maternal, Child and Adolescent Health
Center for Family Health

This frequently asked questions (FAQ) sheet was designed to help guide your virtual AFLP visits (televisits) during the COVID-19 state of emergency to maintain youth's safety, privacy, and security. Televisits include visits conducted on the phone or through video. This information should complement your organizations' policies and AFLP guidance on these topics. If working with youth new to AFLP, review Consent (see page 3). Please reach out to your AFLP Program Consultant if you have questions.

Televisit Tech and Data Security Requirements

What Tech is needed to provide televisit services?

Both case managers and youth should have:

- Access to reliable internet or phone connection.
- Hardware that meets televisit requirements (see details below).
- Downloaded/updated necessary software and accounts.

What are the hardware requirements for televisits?

Electronic devices such as a laptop, tablet or smart phone should**:**

- Require a password, passcode, or biometric data (e.g., thumb print, facial recognition) for access.
- Use timeout protections to protect privacy if the device is lost or stolen.

Important tips when using devices:

- Keep mobile devices in your possession or in a secure place, such as a locked cabinet (not a car), at all times.
- Avoid using a **shared device** if possible. If you are using a shared device, make sure any youth information/files/communication are password protected.
    - How to protect Word documents from Microsoft
    - How to protect PDF documents from Adobe
- To ensure youth privacy, be sure to always logout or "lock" documents/communications when you walk away from the shared device.

What are key considerations across different platforms for conducting televisits?

When deciding on appropriate televisit platforms, agencies should make all efforts to ensure youth privacy and confidentiality according to standards set forth in the CDPH/MCAH Information Privacy and Security Requirements (IPSR) - Exhibit G. Additional considerations include:

1. Using platforms that are secure with end-to-end encryption capability to protect the confidentiality of youth.
2. Ensuring no personal information is exchanged through email or text communications that could result in a breach as noted in the CDPH/MCAH IPSR.
3. Making all efforts to utilize platforms that can offer Health Insurance Portability and Accountability Act (HIPAA) compliance and that have a history of entering into HIPAA Business Associate Agreements (BAAs).
4. Exploring the use of BAA with your televisit platform provider, particularly for long-term use. See U.S. Department of Health and Human Services (US DHHS) BAA resources.
5. Utilizing all available options to ensure confidentiality for youth, including use of teleconference passwords, meeting entry restrictions, headphones, and private locations away from other household members.
6. Consulting with your agency's local IT department before utilizing a new televisit platform.

Below is a list of communication platforms providing remote services that have been listed by the U.S. DHHS. For more information, see U.S. DHHS COVID guidance: HIPAA Flexibility for telehealth technology. Platforms are identified as: ✓ U.S. DHHS HIPAA compliant; ⚠ Deemed acceptable by U.S. DHHS during COVID-19 national emergency; or * Platform provides this service, but U.S. DHHS did not specify this mode of communication. The table does not constitute a CDPH/MCAH endorsement, certification or recommendation of any of the platforms listed by U.S. DHHS.

Platform	Text / chat	Voice / audio	Video
Zoom for Healthcare	✓	✓	✓
Zoom	⚠	⚠	⚠
Google G Suite Hangouts	✓	✓	✓
Google Hangouts	⚠	⚠	⚠
Skype for Business / Microsoft Teams	✓	✓	✓
Skype	⚠	⚠	⚠
Apple Facetime & iMessage	⚠	⚠	⚠
Facebook Messenger	⚠	⚠	⚠
Updox	✓	✓	✓
Vsee	✓	✓	✓
Doxy.me	✓	✓	✓
Cisco WebEx Meetings / WebEx Teams	✓	✓	✓
Amazon Chime	✓	✓	✓
GoToMeeting	✓	✓	✓
WhatsApp	⚠	*	*
Cisco Jabber app	⚠	*	*
Signal app	⚠	*	*

May 6, 2021, version 2

The table above does not constitute a CDPH/MCAH endorsement, certification or recommendation of any of the platforms listed by U.S. DHHS.

What are some special considerations I should be aware of while working from home?

We want to ensure the **privacy** of youth. Case managers should make sure physical documents and devices with youth information are stored in a secure location that other in your home cannot access when not in use. To further protect confidentiality, use the youth's ID number, rather than name, on physical materials. Use of headphones for both case managers and youth may be helpful to protect privacy if others are nearby.

Consent

For new youth, what are acceptable ways to obtain consent?

The enforcement of HIPAA regulations have been temporarily eased by the U.S. DHHS Office of Civil Rights. Below are the acceptable forms of obtaining consent from youth newly enrolling in AFLP. As always, please defer to your agency's specific guidelines on obtaining consent.

Written consent	Electronic consent	Verbal consent
Post mail: Your agency can mail the consent form to the youth, with a self-addressed and pre-paid envelope. **Physical drop off/pick up:** You have the option to physically drop off the consent forms to the youth and pick them up once the youth has signed the forms, following guidelines for safety (agency, county, state, CDC).	**Electronic signature:** HIPAA-compliant options for electronic signatures include DocuSign and Adobe. Follow your agency's guidelines.	**Verbal consent** is acceptable during this time: • Review all consent information with youth. • Parents or legal guardians *cannot* act as substitutes for youth consent. • On forms write in "verbal consent" next to the date.

Televisit Preparation

What should I do to prepare for providing televisits?

In addition to your in-person procedures, the following will improve the success of your televisits:

1. Determine each youth's **preferred communication platform**.
2. **Check** that you have all necessary materials and a working, secure connection.
3. Familiarize yourself and **test** the chosen platforms/devices to make it a more seamless experience.
4. Have paper copy of forms as a **backup,** in case you encounter technical issues during the televisit.
5. Plan for extra time with youth, especially if televisits are new to either of you.

6.   Check your surroundings. Be sure that no one is in the background, can walk in, or overhear you during your televisit. Turn off voice-activated devices that can record (e.g., Alexa and Google Dot).

7.   If it is necessary to exchange any documents containing sensitive information, send using a secure (encrypted) e-mail. Defer to your agency's IT department for proper procedure for sending secure e-mail.

8.   If using the chat functions on the Zoom platform, adjust settings to ensure any messages are only stored for the minimum amount of time possible. The minimum amount of time a message can be stored on Zoom is 1 day. This must be put into effect by the account owner manually:

- Sign into the Zoom web portal
- In the navigation menu, click on **Account Management**, then **IM Management**.
- Select the **IM Settings** tab.
- In the **Storage** section, change these settings:
- **Cloud Storage:** If this setting is enabled, Zoom will automatically save all chat messages to the cloud. Specify the time period to store message (1 day), then click **Save**. After the specified cloud retention period, Zoom will remove all the chat messages and its metadata from the cloud.

Televisit Format

How can I better support the youth while I'm conducting a televisit?

To support youth during the televisit especially if they are new or if this is their first televisit, consider the following:

- Ask the youth about their preferred communication platform among those acceptable for use by your agency.
- Encourage the youth to become familiar with how to properly use the communication platform.
- Make sure you and the youth are both in a private space to engage in the televisit.
- Remind the youth to turn off any voice activated devices (e.g., Alexa, Google Dot).
- Clearly identify yourself. If using video, make sure your face is fully visible.
- Check for comprehension by asking them questions about what was said.
- Remind the youth of their rights as it relates to televisits.
- Give plenty of time for them to ask follow-up questions.

Approach visits with compassion

- During this difficult and potentially traumatic time, youth behaviors and emotions (and yours) may vary. Be responsive to the youth's needs and make adaptations to meet the youth where they are emotionally.

May 6, 2021, version 2

- Youth may be exposed to increased risk of violence or other safety risks due to shelter in place. Be familiar with policies and practices in explaining confidentiality and your role as a mandated reporter.
- During COVID-19, make needs assessment and referrals a priority. Start each visit with an assessment of essential services to ensure youth and their families have stable housing, food and other necessities, including mental and physical wellness (see guidance on suicide screening during COVID-19). Make referrals and provide resources when needed. Spend time talking through how accessing a service may be different, what challenges might come up, and problem solve those with the youth. Document visits that focus on providing essential services as Anytime: Life Planning Visits on the Face-to-Face Visit Summary. Document referrals on the youth's Case in Penelope.
- Remind youth about their strengths, skills, and supports.

Additional Resources

Resources listed below provide links to source material for further context and explanation as well as supplementary information in case agency staff have questions that go beyond the scope of the FAQ.

Government resources

Federal guidelines for telehealth during the pandemic:

- Notification of Enforcement Discretion for Telehealth Remote Communications During the COVID-19 Nationwide Public Health Emergency - U.S. DHHS
- Telehealth FAQs - U.S. DHHS
- HealthIT.gov technical assistance on telehealth
- U.S. DHHS COVID guidance: HIPAA Flexibility for telehealth technology

State resources for telehealth during the pandemic:

- California Telehealth Resource Center
- Telehealth 101 video: How Do I get Started During COVID 19
- Telehealth Best Practices for Providers video

AFLP resources

- Data Collection Manual
- Information Privacy and Security Requirements from AFLP RFA 20-10014 Exhibit G

Telehealth and cybersecurity resources

American Telemedicine Association

- Operating Procedures for Pediatric Telehealth
- Practice Guidelines for Telemental Health with Children and Adolescents
- Answers to questions about using technology safely compiled by the National Network to End Domestic Violence, Safety Net Project