

# Apple Health (Medicaid) telemedicine & telehealth brief

\*\*\*Effective 7/1/2021\*\*\*

## Introduction

In response to the COVID-19 pandemic, the Health Care Authority (HCA) and the Apple Health (Medicaid) managed care organizations are allowing the use of a variety of telehealth technologies to meet the healthcare needs of providers, clients and families. In the health care community the words telehealth and telemedicine are often used interchangeably. However for Apple Health, telemedicine is defined in a very specific way.

## An overview of HCA's telemedicine policy

Telemedicine is a form of telehealth that supports the delivery of health care services. HCA has covered telemedicine for many years. HCA's policy for using telemedicine to deliver services is consistent with Medicaid state and federal requirements. RCW 74.09.325 defines telemedicine as the delivery of health care services through the use of interactive audio and video technology, permitting real-time communication between the patient at the originating site and the provider, for the purpose of diagnosis, consultation, or treatment.

The RCW states:

- The technology used to provide the health care service must meet the standards required by state and federal laws governing the privacy and security of protected health information (HIPAA compliant);
- It does not include the use of audio-only telephone, facsimile, or email; and
- The health care provider who can be reimbursed for services provided using this technology must be:
  - A person regulated under Title 18 or chapter 70.127 RCW, to practice health or health-related services or otherwise practicing health care services in this state consistent with state law; or
  - An employee or agent of a person described in (a) of this subsection, acting in the course and scope of his or her employment.

Telemedicine is covered as an alternative means to provide care in all Medicaid benefits, including behavioral health.

Regarding facility fees, for telemedicine services (i.e., delivered through HIPAA-compliant, interactive, real-time audio and video telecommunications), the originating site is the physical location of the client at the time the service is provided. If the originating site is a qualified site, an originating site facility fee may be paid. Qualified originating sites are listed in the physician related services billing guide. An originating site facility fee will not be paid if the originating site is not a billable location, such as home. If the provider is in the same location as the client, an originating facility fee will not be paid. Further policy for originating site reimbursement is found in the [physician related services billing guide](#) on pages 86-87.

## An overview of HCA's telehealth policy

HCA's Apple Health fee-for-service program and the managed care organizations have also implemented temporary policies to expand the type of telecommunications that can be used to provide covered services. For the duration of the pandemic, telehealth can be considered an umbrella term that includes telemedicine as well as these temporary policies, some of which are reimbursed at rates comparable to in-person visits. In contrast to telemedicine, some telehealth technologies may not be HIPAA compliant and some are not conducted through interactive audio-video exchange. Under telehealth, HCA is standardizing the application of these policies with our partners, the managed care organization (MCOs) and the Administrative Service Organizations (ASOs) to:

*(Revised 5/10/2021)*

- Reduce the administrative burden on providers
- Increase client access to care during the pandemic
- Help providers maintain delivery of services when social distancing is essential
- Rapidly increase telehealth innovation and access

Telehealth is the use of electronic information and telecommunications technologies to support distant primary health and behavioral health care; patient and professional health-related education; public health, and health administration. HCA is using telehealth modalities to provide assessment, diagnosis, intervention, consultation, supervision and information in lieu of an in-person visit. telehealth allows health care services to be provided in a variety of ways to provide health care service, including:

- Audio only (telephone calls)
- Email
- Texting
- E-consults

When providing services using a non-HIPAA compliant telehealth technology, providers are encouraged to try to assure the client's privacy in a HIPAA compliant-like manner. See the section below on "Privacy" for applicable policies and tips.

## Further billing guidance

For additional detail on providing services using telemedicine and telehealth technologies, please see [HCA's COVID-19 information webpage](#) which provides guidance on how to bill.

The managed care organizations also have their specific billing instructions at the links below:

- [Molina Healthcare](#)
- [Coordinated Care](#)
- [United Health Care](#)
- [Community Health Plan of Washington](#)
- [Amerigroup](#)

Please keep in mind that billing for HIPAA-compliant and non-HIPAA compliant audio/video technologies may be different; have your billers reference our FAQs for further information.

## Best Practices

When conducting telehealth services, it is important to ensure that the standard of care for telehealth is the same as that for an in-person visit providing the same health care service. Best practices may include but are not limited to:

- Consider the patient's resources when deciding the best platform to provide telehealth services.
- Test the process and have a back-up plan; connections can be disrupted with heavy volume. Communicate a back-up plan in the event the technology fails.
- Introduce yourself, including what your credential is and what specialty you practice. Show a badge when applicable.
- Ask the patient their name and verify their identity. Consider requesting a photo ID when applicable/available.
- Inform patients of your location and obtain the location of the patient. Include this information in documentation.
- Inform the patient of how the patient can see a clinician in-person in the event of an emergency or as otherwise needed.
- Inform patients they may want to be in a room or space where privacy can be preserved during the conversation.

Documentation requirements for telehealth services are the same as those for documenting in-person care and, at a minimum, should also include:

- Date of the service, including start and stop time or duration of service
- The names of all participants in the encounter, including other patients and providers involved
- The location of the client and a note of any medical personnel with the client, as well as location of the provider
- That the encounter was conducted via telehealth, which telehealth platform was used, and whether it is HIPAA compliant
- If a physical exam is conducted, whether vital signs and exam findings are self-reported or obtained under direction
- If applicable, documentation that the patient consented and mode of consent (written vs. verbal vs. electronic, unless documented elsewhere).

## Resources

There are many resources available for providers to get started with telemedicine and telehealth. Examples of resources are listed below. (Please note that inclusion in the list below does not reflect an endorsement or verification of complete accuracy by HCA.)

- [Washington State Telehealth Collaborative](#)
- [Northwest Regional Telehealth Resource Center](#)
- [Telemental Health Toolkit from NRTRC](#)
- [Washington State Dental Association](#)
- [University of Washington Behavioral Health Institute](#)

Additionally, many professional societies have telehealth guidelines that may provide valuable care-specific information for health care professionals.

## Privacy

### HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) was passed by Congress in 1996. HIPAA-compliant telemedicine technology is covered by a Business Associates Agreement that provides protections for personal health information and data privacy. Recognizing that the COVID-19 public health emergency has created an immediate need for delivery of health care services in a new way, the Department of Health and Human Services Office for Civil Rights (OCR) has issued a Notification of Enforcement Discretion for Telehealth Remote Communications during the COVID-19 Nationwide Public Health Emergency. Similarly, Washington also received a waiver (via an 1135 waiver request) from CMS that waives security requirements for video communication in a telehealth visit during the emergency period. These allow a health care provider using audio or video communication technology to provide services to patients during the COVID-19 nationwide public health emergency to use any non-public facing remote communication product that is available to communicate with the patient.

**However, HCA is beginning the transition to a post-pandemic telehealth policy and will no longer allow services to be provided via a non-HIPAA compliant audio-visual modality.**

The [Office of Civil Rights](#) (OCR) at HHS will exercise its enforcement discretion and will not impose penalties for noncompliance with the regulatory requirements under the HIPAA rules against covered health care providers in connection with the good faith provision of telehealth during the COVID-19 nationwide public health emergency. The OCR notes that the following vendors offer HIPAA compliant services and are able to enter into HIPAA business associate agreements (BAAs):

- Skype for Business
- Updox

- VSee
- Zoom for Healthcare
- Doxy.me
- Google G Suite Hangouts Meet

Facebook Live, Twitch, TikTok, and similar video communication applications are public facing, and should not be used in the provision of telehealth by covered health care providers.

Providers are still responsible for ensuring patient privacy to the best of their ability and to retain responsibility with respect to patient privacy, only sharing or communicating personal health information with individuals authorized to receive the information. Providers should enable all available encryption and privacy modes when using such applications.

When using non-HIPAA compliant audio/video technologies, it is best practice to disclose to patients that these third-party applications potentially introduce privacy risks. For example, a provider may disclose that, “Due to the urgency of the care being provided, I am not using a HIPAA-compliant platform and therefore cannot guarantee the security of the technology being used. I will ensure your privacy to the best of my ability. I need to ask for your verbal consent that you understand this risk and are willing to proceed with this service.”

### **Considerations for Substance Use Disorder Services**

Federal regulations (42 CFR Part 2) address the provisions for Confidentiality of Substance Use Disorder Patient Records. SAMSHA issued guidance for managing the release of records during this pandemic to support access to continued treatment and services. In this document, SAMSHA acknowledged it may not be possible to obtain written consent for release of records and, therefore, the provider could determine that in the case of medical emergency such as the current national emergency, written patient consent is not required. If possible to obtain written consent through email and scan functionality this would be the first option, but if this is not feasible, verbal consent could be documented and the records be requested without written consent. It is suggested the provider site the reason written consent cannot be obtained in the request for records.

Further resources include:

- [SAMSHA guidance](#)
- [HCA guidance](#)