Using  FaceTime for Telemedicine

HIPAA Guidelines on Healthcare Video Visits

SimpleVisit®
Telemedicine Made Simple.

Using FaceTime for Telemedicine

HIPAA Guidelines on Healthcare Video Visits

As the use of telemedicine applications increase in the United States, so does the concerns and regulations regarding patient privacy. Consumer demand for improved access and convenience to healthcare has resulted in a surge of technology innovations that must promise a secure exchange of patient health information. To ensure a secure exchange of sensitive data in digital healthcare delivery, federal standards have been set within the past 25 years; including the Health Insurance Privacy and Portability Act (HIPAA). Digital health innovators are then tasked with crafting solutions to improve access and experience of healthcare delivery while maintaining compliance to the standard protections outlined in HIPAA.

For telemedicine solutions including video visits, a major challenge is utilizing a reliable, secure, yet intuitive video client or network connectivity. Most televisit or video conferencing solutions center around a proprietary platform or software application that can ensure the exchange is encrypted and within federal regulations. There seems to be a general assumption that common commercial video clients, such as Apple's FaceTime, are automatically disqualified from use in telemedicine. This misguided perspective is likely due to fear of compromising HIPAA regulations on privacy. The following material addresses this assumption and definitively affirms that FaceTime can be "HIPAA-Compliant".

Overview

Apple's FaceTime service is categorized as a communications conduit under the federal regulations; therefore is not responsible as a business associate of a covered provider. Furthermore, the encryption, storage, and call recording expectations of HIPAA are met by FaceTime's default policies. There are no current regulations prohibiting its use, however, there are recommended practices to ensure the pursuit of protecting privacy and patient information.

Table of Contents

SimpleVisit®

Protecting Patient Privacy

Clarifying descriptors were added to HIPAA with the passing of the **OmniBus Rule in 2013**. This included relevant adjustments to the Privacy and Breach Notification portions of HIPAA. Under this rule, when a vendor is transferring, maintaining and/or keeping the health records from a covered entity then the vendor is considered a "Business Associate." To better explain, the Rule describes a Business Associate as follows:

> "On behalf of such covered entity or of an organized health care arrangement (as defined in this section) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, creates, receives, maintains, or transmits protected health information for a function or activity regulated by this subchapter, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing; or
>
> Provides, other than in the capacity of a member of the workforce of such covered entity, legal, actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of protected health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person."

If a covered entity is sharing protected healthcare information with a vendor or "Business Associate," they must enter into a Business Associate Agreement to comply with HIPAA. The Business Associate Agreement is meant to hold those with the information accountable for its protection.

A Business Associate Agreement is not necessary, however, for vendors who do not retain PHI in the healthcare exchange. There is a "communications conduit" clause to address the use of such services in relation to patient health information. The clause states that in order for vendors to be considered a communications conduit, they must transmit only and never record nor store data from the exchange:

> "The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the U.S. Postal Service or United Parcel Service and their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services."

The intent of the HIPAA and other regulations such as HITECH are to protect PHI and ensure there is accountability for any potential breach of personal health data. The clarification of what qualifies as a conduit and the role of a business associate provides a standard to determine whether FaceTime can be used for healthcare delivery.

FaceTime's Policy

When addressed with questions regarding privacy and security of FaceTime, Apple issued **the following statement**:

> "In addition to your existing infrastructure each FaceTime session is encrypted end to end with unique session keys. Apple creates a unique ID for each FaceTime user, ensuring FaceTime calls are routed and connected properly. No other user information is stored for FaceTime and Apple cannot retrieve the data for any other purpose (it is stored in a hash format). No location information is ever used or stored during FaceTime registration or a FaceTime conversation. Additionally, the entire FaceTime conversation stream itself is encrypted."

Apple's policy for FaceTime call handling retains no protected health information while assigning a unique ID over an encrypted call. As such, this video service is viewed as a "communications conduit" under the Health and Human Services guidelines. Therefore, Apple is not required to sign a Business Associate Agreement with healthcare providers using their service for patient care.

Healthcare providers using video services that meet the encryption, call handling, and storing criteria of the HIPAA regulations share no risk in exposing ePHI. The risk of non-compliance is found more so in the conduct of the healthcare provider surrounding the telemedicine appointment. Healthcare providers who abuse appointment requests, expose PHI of other patients during an exchange or even recklessly prescribe medications over a video visit are the culprits of non-compliance. The medium used for the telemedicine appointment holds no accountability to the abuse of the user.

Apple's FaceTime has been and continues to be utilized for telemedicine well within HIPAA's standards. Healthcare providers practicing medicine over this service can do so without fear of breaking the rules.

How SimpleVisit Uses FaceTime

The call handling over SimpleVisit further protects patient identifiable information even when using FaceTime for virtual care. The **SimpleVisit service** bridges qualified video platforms with any other qualified platform for use in telemedicine. For example, FaceTime can interoperate with other video services such as Skype and Google Hangouts connected over SimpleVisit.

This service works by bridging two separate communication channels into a secure session within a closed system. An outbound call is placed from a SimpleVisit workstation to a patient's preferred video platform (i.e. FaceTime). Once the call is answered, a connection is established between the patient's FaceTime ID and SimpleVisit's FaceTime ID. Another channel within the SimpleVisit system then establishes a connection with the provider on their preferred video platform (i.e. Skype). These two separate channels are assigned to a bridge without breaking or manipulating the current connection via a SimpleVisit video switch.

In this situation, the patient's contact ID is not directly associated with the provider's contact ID while the communications services maintain its encryption. Patient health information is never compromised in this exchange using FaceTime or any other qualifying video service. Any patient health information provided to the SimpleVisit service is the appointment time and contact ID of all parties. Covered entities using SimpleVisit would enter a Business Associate Agreement to extend accountability for handling what could be identified as sensitive data.

Conclusion

FaceTime is well-within HIPAA regulations for telemedicine-use as a communications conduit. The HIPAA rules are designed to protect health information that merits privacy. Those federal standards hold healthcare providers as well as any contracting vendors accountable to continue to secure any protected data transferred. A Business Associate agreement is encouraged for all vendors that acquire and store PHI. Exemptions of the Business Associate rule include communication platforms that are encrypted and transmit-only services. Since Apple's policies on call handling and storage meet the exemption criteria, FaceTime qualifies as a communications conduit with no business associates agreement required.

Using FaceTime for telemedicine is permissible in and of itself. Although, it is advised to consider internal policies to minimize abuse of the platform in care delivery. The SimpleVisit service is designed to avoid such abuse and further protect patient information with a video bridge connecting FaceTime and any other qualified video platform. The use of FaceTime through the SimpleVisit service mitigates risk of compromised PHI, insync with the intentions of the HIPAA guidelines.

About SimpleVisit

SimpleVisit allows healthcare providers to deliver secure, branded care to patients over any device using Apple's FaceTime, Google Hangouts, or Microsoft Skype. This service utilizes patented technology to connect healthcare providers and patients over common video communication applications. Request a demonstration to learn more at simplevisit.com or call (877) 83-VISIT.

Contact Us

SIMPLEVISIT
2144 Priest Bridge Ct Suite 5
Crofton, Maryland 21114

(877) 83-VISIT
info@simplevisit.com

@SimpleVisitMD

SimpleVisit®
Telemedicine Made Simple.