Virtual Visit Technology Policy

Our Commitment to Your Privacy

Our Care Center is dedicated to maintaining the privacy of your individually identifiable health information (IIHI). In conducting our business, we will create records regarding you and the treatment and services we provide to you.

The technology we use to enable virtual visits with your provider **does not record your protected health information (PHI) in any way**. All documentation of your virtual visit will be completed in the same manner as an in-office visit, using your provider's electronic medical record (EMR) system. The same privacy practices that apply to an in-office visit apply to your virtual visit. Please review our **Notice of Privacy Practices** for additional detail.

Virtual Visit Technical Process

The Health Insurance Portability and Accountability Act (HIPAA) provides standards to protect the confidentiality, integrity and availability of protected health information (PHI), including electronic protected health information (ePHI). HIPAA provides guidance for protecting ePHI while giving healthcare providers access to information necessary to provide services.

Privia's virtual visit platform has been designed in such a way that healthcare providers may use our services for video communication in a manner that is consistent with their HIPAA obligations.

The virtual visit technology does not store or access the PHI of users. The technology uses encryption that is designed to protect the video streams during transmission so that no unauthorized parties can access a video conference while in session. Further, the technology does not permit either the patient or provider to record the videoconferencing sessions.

Access Authentication and Security Controls

All registered system users have a unique username and must authenticate with a password through their EMR in order to access the virtual meeting room as a provider.. Unique keys are generated for each scheduled visit. All meetings may be terminated by the provider, a designated moderator, or a system administrator.

Audit Controls

Failed authentication attempts to the system are recorded and monitored for signs of attempted unauthorized access. Configuration changes to the virtual visit systems are monitored and recorded to minimize the risk of unauthorized changes being made to the environment.

Transmission Security

Utilizing industry standard and proven technologies, the Privia virtual visit platform employs a variety of security measures at both the application level and the network level.

At the application level, Privia's virtual visit platform meets enterprise security standards with the use of TLS, SRTP, H.235 (where interoperability with legacy videoconferencing is supported), and AES 128-bit encryption for signaling and media.

At the network level, the videoconferencing hosting facilities utilized are SOC 2 compliant, with 24/7 protection to meet regulatory and best practice requirements. Firewalls are regularly assessed, configured, and updated to remain effective against intrusion. Leading edge filtering and advanced routing techniques help protect against Distributed Denial of Service (DDoS) attacks.