OptiMantra

TELEHEALTH HIPAA CHECKLIST

This checklist is a general guide to HIPAA compliance measures and should not be considered legal advice. Completing this checklist does not guarantee or certify that your organization is HIPAA compliant.

SECTION 1: TELEHEALTH PLATFORM AND TECHNICAL SAFEGUARDS

1. **Platform Selection:** Are you using a HIPAA-compliant telehealth platform that is specifically designed for healthcare? This includes features like secure messaging and video conferencing. ☐
2. **Encryption:** Is all PHI encrypted both "at rest" (when stored) and "in transit" (when being transmitted over the internet)? The platform should use strong encryption protocols to prevent unauthorized access. ☐
3. **Access Controls:** Does the platform use authentication methods such as multi-factor authentication (MFA) to restrict access to PHI to only authorized personnel? ☐
4. **Audit Controls:** Does the platform log all user activity, including who accesses patient records and when? These audit trails are essential for tracking compliance and investigating potential breaches. ☐
5. **Secure Remote Access:** Do providers use a secure, encrypted network, such as a VPN, to connect to the organization's network from home? PHI should not be stored on personal devices. ☐
6. **Workstation Security:** Are all workstations and devices (e.g., laptops, tablets) used for telemedicine protected with up-to-date antivirus software, firewalls, and security patches? ☐

SECTION 2: TELEHEALTH ADMINISTRATIVE POLICIES

1. **Risk Analysis:** Have you conducted a thorough risk assessment that specifically identifies and evaluates the new risks and vulnerabilities introduced by your telehealth operations? ☐
2. **Business Associate Agreements (BAAs):** Do you have a signed BAA with every third-party vendor that handles PHI on your behalf, including your telehealth platform and any cloud storage providers? ☐
3. **Patient Consent:** Do you have a process to obtain and document informed patient consent for telehealth visits? The patient must be informed of the benefits, potential risks, and their right to an in-person visit. ☐
4. **Workforce Training:** Have all staff members involved in telehealth operations been trained on how to handle PHI in a remote setting? Training should include proper use of the platform, identifying privacy risks, and reports ☐
5. **Physical Environment:** Are there clear policies requiring providers to conduct telemedicine sessions from a private, secure location to prevent PHI from being overheard or seen by others? ☐
6. **Breach Notification Protocols:** Is your breach notification plan updated to address security incidents or data breaches that may occur with a telehealth platform or remote device? The plan should outline how to investigate. ☐

OptiMantra's built-in telehealth solution is designed with these safeguards in mind, offering a secure, all-in-one platform for your practice management, EHR, and virtual visits. Our commitment to compliance, in partnership with the expertise of The HIPAA Journal, helps your practice focus on what matters most: providing quality care.

THE HIPAA JOURNAL