CourtCall® and HIPAA

OVERVIEW

The Health Insurance Portability and Accountability Act (HIPAA) sets rules and regulations regarding privacy and security standards designed to protect the confidentiality of patient health information. CourtCall has taken the necessary steps with our platforms and procedures to secure Protected Health Information (PHI) and electronic Protected Health Information (ePHI) to the extent required under HIPAA.

PHI refers to all "individually identifiable health information" that is created, used, or disclosed in the course of providing a health care service that is held or transmitted by a covered entity or its Business Associate, in any form or media, whether electronic, paper, or oral. ePHI is individually identifiable information that is sent or stored electronically. ePHI does not include paper-to-paper faxes, person-to-person telephone calls, video teleconferencing, or messages left on voice-mail as these do not exist in electronic form before the transmission.

Covered entities that partner with CourtCall can rest assured knowing that we help our partners remain in complete compliance with the rules and regulations of HIPAA.

HIPAA's general requirements state that covered entities must:

1. **Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;**
2. **Identify and protect against reasonably anticipated threats to the security or integrity of the information;**
3. **Protect against reasonably anticipated, impermissible uses or disclosures; and**
4. **Ensure compliance by their workforce.**

CourtCall, as a trusted partner and Business Associate, does what is necessary to comply with HIPAA. To ensure our purpose as a remote appearance provider is clearly defined, we will offer or sign a Business Associate Agreement (BAA). Furthermore, CourtCall encrypts and protects all transmitted data or information used for scheduling purposes and has no additional access to PHI/ePHI.

More Specifically, CourtCall's Platform is securely encrypted using the latest technology. When scheduling cases that may include medically sensitive information, CourtCall takes care to avoid the use of any specific indentifying information. Only general information is used throughout to help protect the identity and PHI of any individuals. CourtCall has developed an additional list of "best practices" that should be used to avoid the accidental disclosure of any PHI while using the CourtCall Platform. In the event PHI is disclosed erroneously, CourtCall will report the breach in accordance with the terms of any BAA.

COMPLIANCE, BEST PRACTICES AND SPECIFICATIONS

- CourtCall takes care to avoid the use of specific identifying information when scheduling cases and/or appearances that may include medically sensitive information.

- CourtCall will comply with the terms of a Business Associate Agreement (BAA) and agrees, or will agree, to be responsible for keeping patient information secure and will report any breach of PHI in accordance with the terms of HIPAA or any signed BAA.

- CourtCall has developed additional "best practices" that should be observed to avoid the accidental disclosure of PHI while using the CourtCall Platform.

    - **Do not enable or have CourtCall enable recording or storage of audio and/or video or for sessions involving PHI/ePHI**
        - **CourtCall will automatically delete and purge its system of any PHI/ePHI inadvertently shared**
    - **Do not share PHI through CourtCall's document sharing feature**
    - **Do not use CourtCall's chat feature to discuss any PHI in writing**

- CourtCall's Platform is securely encrypted using the latest technology, transmitting its data over a peer-to-peer architecture.

    - **Meets the minimum required specifications found in FIPS 140-2**
        - **Symantec Class 3 Secure Server**
        - **TLS 1.2 Protocol**
        - **ECDHE_RSA Key Exchange**
        - **AES_256_GCM Cipher**