TDC BRIDGE™
HIPAA COMPLIANCE STATEMENT

SUMMARY

TDC BRIDGE™ is a Communications as a Service offering that enables mobile customers to have the same conversational experience with businesses that they have with their friends. TDC BRIDGE™ implements the modern call model: conversations start with messaging, then are escalated into voice or video conversations if appropriate. Mass personalization for the mobile customer are enabled by integrations with corporate data sources, artificial intelligence and multiple messaging networks enable, without the requirement for any mobile application development. The results are great conversations, better outcomes and the best relationships.

INTRODUCTION TO HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) established standards for the transfer of electronic health information. More specifically, under Title II of HIPAA, these standards protect the transfer of electronic protected health information (ePHI).

TEN DIGIT Communications LLC (TEN DIGIT) understands that the character of these standards is to protect the privacy of individuals, and are compliant with HIPAA requirements as so outlined within this document.

HIPAA has identified three categories of data safeguards that must be established to prevent privacy violations, with regards to, protected health information.

Administrative Safeguards – "The administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information."

Physical Safeguards – "The physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Technical Safeguards – "The technology and policy and procedures that protect electronic protected health information and control access to it (the ePHI)".

Technical safeguards pinpoint specific standards that are required for HIPAA compliance for the transfer of ePHI. These include Access Controls, Audit Controls, Integrity, Person or Entity Authentication, and Transmission security.

ADMINISTRATIVE SAFEGUARDS

The TEN DIGIT Bridge Platform provides functionalities that aid in the execution of administrative safeguards. However, administrative responsibilities for HIPAA compliance in regard to ePHI will belong to the Registered Users of TEN DIGIT.

Risk

Monitoring systems, including end-to-end testing, are in place to ensure platform reliability. Alerts are monitored by the TEN DIGIT operations team 24/7. All TEN DIGIT systems are managed nodes and receive all relevant system and application security updates in regular intervals. TEN DIGIT understands the sensitivity of ePHI and the need for this information to be risk averse. Their security measures work to ensure the Administrative Safeguard requirement of HIPAA.

Access

Login access to the TEN DIGIT Bridge platform is restricted to members/employees only. All member/employee access is restricted to secure IPSec VPN with individual login. The platform will automatically log out after a set amount of inactivity to prevent unwanted access to the platform should a user step away from the desktop without logging out. Access to individual systems is restricted to SSH Private key that is unique per accessing employee. Upon leaving the TEN DIGIT Platform, VPN credentials and SSH private key access is immediately removed.

Privacy

All customer data stored within the TEN DIGIT cloud is treated as confidential and is only accessible by the Registered Account Holder. Registered Account Holder passwords are encrypted and salted.

Backup

TEN DIGIT adheres to industry best practices regarding the backup and retention of data. All backup data is handled with the same regard for privacy and security as live production data.

Disaster Recovery

All components within the TEN DIGIT infrastructure are deployed redundantly. Failover procedures are maintained in Method of Procedure (MOP) documents published within the TEN DIGIT operations department.

PHYSICAL SAFEGUARDS

Data Center

TEN DIGIT employs servers which are stored in secure datacenters with access control policies in place. Biometric and keycard access are required to gain access to all facilities. Physical cabinets are locked and require facility escort. All access control measures follow standards and procedures set forth in both SSAE 16 Type II and ISO- 27002 as well as industry best practices.

Corporate Office

No registered user account data is stored onsite at the TEN DIGIT corporate offices. This includes all internal workstations, servers, or laptops.

TECHNICAL SAFEGUARDS

Technical Safeguards

Technical requirements that pertain more specifically to texting platforms and electronically transferred sensitive patient information demand further procedural specifications to ensure adequate privacy and security.

Access Controls

TEN DIGIT takes precautions to safeguard personal information against loss, theft, and misuse. In addition, unauthorized access, disclosure, alteration, and destruction are also safeguarded. These access controls are facilitated by unique user identification. Unique user identification is created using the landline phone number and a user generated password. Users are required to keep their own passwords secure.

Ultimately, it is the responsibility of the business and the registered user to maintain proper technical policies and procedures for user security. This includes, but is not limited to, password length requirements, sharing user credentials, and protection against password interception.

Audit Controls

TEN DIGIT's cloud storage servers keep a secure record of message activity accessible only to authorized individuals. Message storage allows activity to be traced and retrieved for audit purposes. Although TEN DIGIT does archive messages, message activity is still subject to data purges as necessary. Responsibility for maintaining software that records and has capabilities to examine activity in systems containing ePHI will fall upon the Registered

Account Holder, not TEN DIGIT. Although TEN DIGIT has cloud capabilities to store data, TEN DIGIT reserves that the liability for such audit controls belongs to the Registered Account Holder.

Integrity

TEN DIGIT understands the sensitivity and importance of security when transferring ePHI through electronic portals. We work in full faith in compliance with HIPAA guidelines that protect the privacy of both the healthcare entity and the patient. As a result, our operation procedures are designed to prevent and deter improper and unauthorized compromise, alteration, or destruction of Registered User data.

Person or Entity Authentication

Messages sent via the TEN DIGIT Bridge Platform cannot be altered once the customer has sent the message. Authentication is required on all TEN DIGIT services in order to access messages history or send and receive new messages.

Transmission Security. In compliance with HIPAA requirements to ensure the security of data while in transit, TEN DIGIT uses 256-bit Secure Sockets Layer (SSL) to encrypt all communication between the client devices and the TEN DIGIT Platform.

SUMMARY

At TEN DIGIT, we work to make it easier to align Administrative, Physical, and Technical Safeguards.

We have taken measures to ensure that our operations align with HIPAA requirements for Technical Safeguards that specifically address electronic transfer of ePHI.

TEN DIGIT understands the nature of the HIPAA requirements to protect the privacy of those involved. The sensitivity of this data and the importance of security measures to secure compliance are taken seriously at TEN DIGIT.

CONTACT US

Should you have any questions or concerns regarding HIPAA compliance, please contact us directly:

Gary Brandt, CEO
Text or Call (888) 512-8398