HIPAA COMPLIANCE STATEMENT

tigerconnect

HIPAA COMPLIANCE STATEMENT

TigerConnect provides customers with the tools, services and products to facilitate compliance with HIPAA regulations.

WHAT IS HIPAA?

HIPAA is the Health Insurance Portability and Accountability Act of 1996, which amends the Internal Revenue Service Code of 1986. This law impacts all areas of the healthcare industry and is designed to improve the portability and continuity of healthcare. It calls for greater accountability in the area of health care, simplification of the administration of health insurance, and use of administrative, technical and physical safeguards to protect confidential health information of patients. More specifically, HIPAA requires healthcare providers to adopt sound practices for protecting the confidentiality of all patient information in any form.

HOW DOES TIGERCONNECT FACILITATE HIPAA COMPLIANCE?

Healthcare organizations that engage in the handling, maintenance, storage or exchange of protected health information (PHI) are subject to HIPAA and must ensure the confidentiality, integrity and availability of PHI.

TigerConnect provides the healthcare enterprise a suite of security mechanisms to ensure the highest standards of patient confidentiality and overall data protection with regards to PHI and in accordance with HIPAA.

HIPAA SECURITY STANDARDS

Security standards are divided into the following categories: administrative, physical and technical safeguards.

ADMINISTRATIVE SAFEGUARDS

Documented, formal practices to manage the selection and implementation of security measures that protect information and guide the conduct of personnel in relation to the protection of information.

PHYSICAL SAFEGUARDS

Practices to manage the protection of physical computer systems and related buildings and equipment from fire and other natural and environmental hazards, as well as from intrusion.

TECHNICAL SAFEGUARDS

Processes that are put in place to protect and to control information access and data that is stored and transmitted over a communications network.

TigerConnect assists organizations, not only with the technical safeguards, but also with their administrative and physical safeguard responsibilities under the HIPAA regulations. The following chart summarizes the HIPAA specifications that can be supported by TigerConnect to compliment a full security environment. Each set of safeguards is comprised of a number of standards, which generally consist of several implementation specifications that are either required (R) or addressable (A). An “implementation specification” is a detailed instruction for implementing a particular HIPAA Security Rule standard.

While required specifications are mandatory as the name suggests, addressable specifications must also be implemented if reasonable and appropriate under the circumstances. Addressable specifications are not optional. If the entity chooses not to implement an addressable specification based on its risk assessment, it must document the rationale supporting that determination and, if reasonable and appropriate, implement an equivalent alternative measure.

HIPAA SECURITY STANDARDS & IMPLEMENTATION SPECIFICATIONS: ABBREVIATED

TECHNICAL SAFEGUARDS | (R) REQUIRED :: (A) ADDRESSABLE

Access Controls (R)

- Unique User Identification (R)
- Emergency Access Procedure (R)
- Encryption & Decryption (A)

Audit Controls (R)

- Notification and Archiving (R)

Integrity (R)

- Mechanism to Authenticate PHI (A)

PHYSICAL SAFEGUARDS | (R) REQUIRED :: (A) ADDRESSABLE

Facility Security Plan (R)

Access Controls & Validation Procedures

ADMINISTRATIVE SAFEGUARDS | (R) REQUIRED :: (A) ADDRESSABLE

Security Management Process (R)

- Risk Management (R)

Information Access Management (R)

- Access Authorization (R)

Contingency Plan (R)

- Data Backup Plan (R)
- Disaster Recovery Plan (R)
- HIPAA Security Rule Evaluation (R)

Although TigerConnect may be viewed as having the capabilities to assist only with the technical safeguards established by the HIPAA Security Rule, the technology and tools can also assist with both the administrative and physical safeguards, as outlined in the following pages.

HIPAA security compliance is not achieved with a single piece of hardware, software, or process. All IT technologies and processes must be working in accordance to create an absolute and complete secure environment. Each security practice must be considered within an entity's own technological environment once completing a full-risk assessment. The following is a summary list of the HIPAA Security Rule standards and implementation specifications.

TECHNICAL SAFEGUARDS

The following outlines the general processes used to protect data and to control access to ePHI. They include authentication controls to verify sign-ons and transmission security (such as data encryption) to protect integrity and confidentiality of data.
Note: (R) Required, (A) Addressable

ACCESS CONTROL (R) 164.312(a)(1)

Implement policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights

UNIQUE USER IDENTIFICATION (R)

Requirement: Assign a unique name and/or number for identifying and tracking user identity entity

Specific Question: Does your organization require the use of unique user names for all workstation users?
[No sharing of accounts]

Each TigerConnect System ID can be associated with either a user's unique email address or phone number.

TigerConnect's Information Security policy does not allow the sharing of accounts. Also, based on your role either as system admin or end-user, a specific user name is assigned to each individual provisioned on our mobile messaging platform. Again, any system ID [admin or user] is also paired and matched with an email address, phone number, or device ID of their phone.

EMERGENCY ACCESS PROCEDURE (R)

Requirement: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.

Specific Question: In the event normal communication methods are unavailable, such as during an emergency, will the client be able to obtain necessary ePHI information as needed?

Emergency access procedures are necessary when normal procedures for messaging access, mobile device in particular, may not be feasible due to data connection availability from the mobile carrier. In that case, TigerConnect clients can use the Web Client to send and receive messages.

If "normal communication" (via user's personal mobile device) is either inaccessible or unavailable, ePHI information can still be obtained. Each user will have access to the Web Client given the availability of web-enabled desktop. Via a web browser, users can log into a secure portal using their existing credentials to retrieve message data and/or send out any new messages. TigerConnect uses a cloud hosted infrastructure to minimize the risk of data loss.

AUDIT CONTROL (R) 164.312(b)

Implement hardware, software, and/or procedural mechanisms that record and examine activity in any system that contains or uses ePHI.

NOTIFICATION AND ARCHIVING

Specific Question: Does your organization have procedures and/or mechanisms to track and record activity on systems containing ePHI and customer data?

With TigerConnect, notification indicators display when a message has been received and opened. Further message activity can be retrieved by implementing our open interface into most standard archiving solutions.

TigerConnect has configured logging and auditing on our AICPA AT-801 platform. Our cloud hosted servers have account monitoring in place and user activity is logged. In addition, TigerConnect can also provide a direct feed from our servers to our clients of all message activity.

TigerConnect provides message delivery status and audit controls. In order to provide traceable, detailed delivery and receipt information. The TigerConnect application clearly indicates when the message was received on the device and when the recipient opened it.

Additional tracking is also provided through archiving procedures. TigerConnect allows full flexibility to leverage existing deployed solutions for archival, retrieval and monitoring.

INTEGRITY (R) 164.312(c)(1)

Implement policies and procedures to protect ePHI from improper alternation and destruction.

MECHANISM TO AUTHENTICATE ePHI (A)

Requirement: Implement electronic mechanisms to corroborate that ePHI has not been altered.

Specific Question: Does your organization have procedures and tools to protect electronically transmitted ePHI from unauthorized access and/ or modification?

Messages sent via TigerConnect cannot be copied or forwarded thus protecting the integrity of the message and preventing harmful unnecessary data exposure.

All electronically transmitted data (ePHI and related) is encrypted using TLS encryption [128/256-bit]. Data-at-rest on the mobile devices is also AES encrypted. TigerConnect has user monitoring on cloud hosted servers and all users are authenticated and tracked.

Messages cannot be copied, pasted, or forwarded therefore enhancing standard security and privacy controls that support message data integrity. Messages are tightly encapsulated and can be configured to travel only within a defined private network

TRANSMISSION SECURITY 164.312(e)(1)

Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communication network

ENCRYPTION AND DECRYPTION (A)

Requirement: Implement protection of data-at-rest and data-in-motion

Specific Question: Are controls and procedures in place to encrypt and decrypt data at-rest, in transit and in storage?

TigerConnect uses a combination of Transport Layer Security (TLS) protocol to create a uniquely encrypted channel for private communication of healthcare data in motion. This is followed by Advanced Encryption Standard (AES) encryption for data-at-rest. TigerConnect thus provides total coverage for moving any type of sensitive data to/from mobile devices, through its secure messaging platform. Any data-at-rest in TigerConnect is encrypted.

ADMINISTRATIVE SAFEGUARDS

In general, this section of HIPAA Security Rule describes administrative procedures that include formal practices governing the implementation of security measures and the conduct of personnel.

SECURITY MANAGEMENT PROCESS (R) 164.308(a)(1)(i)

Implement policies and procedures to prevent, detect, contain, and correct security violations.

RISK MANAGEMENT ANALYSIS (A)

Requirement: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

Specific Question: Are risk assessments regularly performed?

All relevant information technology and computing resources are identified, diagramed and documented.

An annual risk assessment is conducted by a third party. All vulnerabilities detected have a remediation plan.

Important to note is that, based on our model of data retention as messages are processed through our secure mobile messaging platform, our client's PHI/ePHI data exposure is very limited or almost none. Based on the lifespan setting (TTL) of messages sent, once a message is deleted, the message is deleted from the sender's device, the recipient's device and all servers. Our controls are designed to support the value of sensitive data, in that, it should be removed when necessary versus managing message storage endlessly on mobile devices thus creating huge data exposure risk across every mobile phone device in your organization. This also has reduced eDiscovery efforts as well.

INFORMATION ACCESS MANAGEMENT (R) 164.308(a)(4)(i)

Implement policies and procedures for authorizing access to ePHI that are consistent with entity's determinations under the HIPAA Privacy Rule

ACCESS AUTHORIZATION (A)

Requirement: Implement policies and procedures for granting access to ePHI. Specific Question: Has your organization implemented policies for ensuring the confidentiality and privacy of customer data?

Specific Question: Has your organization implemented procedures for granting employees access to customer data, while ensuring the ongoing protection of the information from inappropriate or malicious activities?

TigerConnect's solution enforces restricted access to help safeguard the integrity and proper use of ePHI.

Yes, Our policies and procedures limit or, in almost every case, restrict any access internally to ePHI data.

We do have information security and HIPAA security policies for the organization that have been audited by a third party and are quickly maturing to ensure our ISO and HIPAA compliance.

Only approved users can retrieve client data in any sensitive area of our application, based on their role in the company. We regularly inspect access rights of our IT staff, as well as monitor their activity. Level of data access is granted solely on the basis of the internal employee's job function.

In addition, all of our employees, administration and development are local. We do not use offshore outsourcing for service creation or delivery, thereby limiting risk associated to access management. All user access is

DATA BACKUP PLAN (R) 164.308(a)(7)(ii)(A)

Implement policies and procedures to support execution of proper data backup plans.

Specific Question: Has your organization implemented procedures for ensuring the ongoing availability of customer information, while ensuring the integrity of the data?	Yes, TigerConnect believes that superior technology necessitates consciousness for security. With that, we strive to effectively promote and employ industry standards and best practices for our product's implementation, utilization and protocols so to ensure confidentiality, availability and integrity that client's data always remains secure. We do have operating procedures and processes to allow for specific clients' requirements for data backup. We can configure this capability specifically for the client or provide them a feed so that it can be performed, managed and stored by the client as part of their electronic communication data retention policies. Our cloud hosted servers are on a robust platform that provides us stability and emergency access to backup processes by our provider.

DISASTER RECOVERY PLAN (R) 164.308(A)(7)(ii)(B)

Implement policies and procedures to support execution of proper data backup plans.

Specific Question: Has your organization developed procedures for restoring data in the event of a disaster or widespread emergency?	Yes, based on our Business Continuity Plan [BCP] and Disaster Recovery [DR] procedures we can work with our clients to restore data based on each client's specific RTO [recovery time objective.] Depending on any specific needs, we can outline any additional processes to assure we can meet our client's backup and restoration requirements. TigerConnect's high availability infrastructure provides fault tolerance and redundancy. Our cloud hosted servers are on a robust platform that provides us stability and emergency access to backup processes by our provider.

PHYSICAL SAFEGUARDS

This category focuses on the mechanisms required for the protection of physical computer systems, equipment and the building in which ePHI is stored.

FACILITY SECURITY PLAN (R) 164.310(a)(2)(ii) Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	
Specific Question: Have procedures and controls been implemented to safeguard your facility(s) and equipement from unauthorized physical access or theft?	Yes, physical access is restricted by our hosting provider and access to our servers is logged and monitored regularly.

ACCESS CONTROL AND VALIDATION PROCEDURES (R) 164.310(a)(2)(iii) Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	
Specific Question: Have procedures and controls been implemented to control and validate a person's access to your facilities, especially data centers?	Data Center access controls follow AICPA AT-801 I standards and procedures as well as industry best practices. Every user accessing our servers by our hosting provider is logged and monitored.

ORGANIZATIONAL REQUIREMENTS

BUSINESS ASSOCIATE PATTERN OF ACTIVITY (R) 164.314(A)(1)(II)

Understanding of policy and regulatory violations.

Specific Question: Have any HIPAA Security Rule violations occurred during the last fiscal year?	No, TigerConnect has not had any violation of HIPAA Security Rules.

BUSINESS ASSOCIATE CONTRACTS (R) 164.314(A)(1)(II)

Understanding of BA Contracts.

Specific Question: Between client and your organization (aka: BA), will your organization satisfy the following Security Rule obligations: 1. The BA will implement safeguards to reasonably protect ePHI? 2. The BA will ensure that anyone who it provides ePHI to agrees to implement reasonable safeguards to protect client data? 3. The BA will report to client of any security incidents, of which it becomes aware?	Yes, we are prepared to satisfy all requirements related to Business Associates. Even though we act only as a messaging channel, our AICPA AT-801 supported infrastructure is designed to facilitate secure and private messaging from source to target users in your organization.

SUMMARY

Mobile messaging will continue to grow at a fast, consistent pace in the years to come and is primarily driven by two factors:

Consumer Demand

» Consumers' demand for enhanced data from businesses with whom they interact

Need for Mobilization of Workforce to:

» Reduce overall corporate costs

» Facilitate speed in decision making

» Improve employee efficiency

» Improve overall customer service

TigerConnect took the initiative to enhance existing text message communications and created a purpose-built solution for the healthcare sector that provides an easy-to-use, cost-effective, securely encrypted and bi-directional mobile platform. The rise of mobile devices in the workplace, specifically healthcare facilities, has forced providers to look for ways to utilize mobile technology to increase efficiency, improve patient care and drive new businesses to their practice, without compromising HIPAA compliance regulations.

As an organization, TigerConnect values all aspects of security including its development of secure products, its people, and the supporting technology infrastructure. TigerConnect is committed to enhancing their security best practices and making sure its customers can be confident in their ability to remain compliant to HIPAA and other regulations while deploying the TigerConnect secure text messaging solution in their organizations.

About TigerConnect

As healthcare's largest provider of clinical communication solutions, TigerConnect helps physicians, nurses, and other staff communicate and collaborate more effectively, accelerating productivity, reducing costs, and improving patient outcomes. With 6,000 facilities, 99.99% uptime, and over 10 million messages processed each day, TigerConnect continually delivers advanced product innovations and integrates with critical hospital systems such as the EHR, nurse call, and scheduling solutions.

The company's commitment to client success is reflected in its broad support organization that works directly with clients at every stage to streamline communication workflows and achieve the highest possible ROI.

Learn how clients like RWJBarnabas, Geisinger, and LifePoint are using TigerConnect to solve healthcare's biggest communication challenges.

Call Us:
310 401 1820

Email Us:
sales@tigerconnect.com

Visit Us on the Web:
www.tigerconnect.com

Follow us on Twitter:
www.twitter.com/TigerConnect

Connect with us on Linkedin:
www.linkedin.com/company/TigerConnect


tigertext
Work Securely