TeleMessage

HIPAA COMPLIANCE STATEMENT

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

Texting in Healthcare

HIPAA is the Health Insurance Portability and Accountability Act of 1996, which amends the Internal Revenue The speed, convenience, and reliability of text messaging has become the #1 form of communication in the United States however, the standard text messaging using the common Short Message Service (SMS) available on most phones is not secure and does not comply with HIPAA Requirements. In 2011, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) issued a directive effectively banning the use of SMS for physician's orders. With over 80% of physicians now using smartphones, the limitations placed on text messaging has posed a serious problem for organizations as physicians demand a communication solution that offers the speed and simplicity as SMS text-messaging.

What is the Impact of HIPAA on TeleMessage (for "Covered Entities?" or "Business Associates?")

TeleMessage is neither a Covered Entity nor a Business Associate. Specifically, as stated in the Federal Register, Vol. 75, No. 134, p. 40873, "…entities that act as mere conduits for the transportation of protected health information but do not access the information other than on a random or infrequent basis are not business associates" (also see: **http://www.hhs.gov/ocr/privacy/hipaa/faq/smaller_providers_and_ businesses/245.html**). TeleMessage provides a secure and private conduit and does not routinely access protected health information (PHI), therefore, the HIPAA security and privacy requirements do not apply to TeleMessage directly.

Having stated that, TeleMessage is dedicated to the privacy and security of its customer's information and facilitates compliance with the overall spirit and intent of the HIPAA requirements. Should any future updates take place in the laws concerning "Covered Entities" and "Business Associates" for HIPAA, TeleMessage will be well-positioned to map every compliance requirement. This level of due diligence provides health care customers the confidence to deploy their secure text messaging network without risking non-compliance.

Does TeleMessage facilitate support for HIPAA requirements?

All businesses, regardless of their size, which engage in the handling, maintenance, storage or exchange of private health or patient-related information, are subject to HIPAA. Health care organizations and technology partners, such as TeleMessage are committed in their efforts to ensure the confidentiality, integrity and availability of all protected electronic information.

TeleMessage provides the health care 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.

TeleMessage 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 TeleMessage 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 AND IMPLEMENTATION SPECIFICATIONS | Abbreviated

Technical Safeguards

Note: (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 ePHI (A)

Transmission Security (R)

- Encryption (A)

Physical Safeguards

Note: (R) Required (A) Addressable

Facility Security Plan (R)

Access Controls and Validation Procedures (R)

Administrative Safeguards

Note: (R) Required (A) Addressable

Security Management Process (R)

- Risk Management (R)

Information Access Management (R)

- Access Authorization (A)

Contingency Plan (R)

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

Although TeleMessage 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 workstations users? [No sharing of accounts.]	Each TeleMessage System ID can be associated with either a user's unique email address or phone number. TeleMessage'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.

TeleMessage

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, TeleMessage 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

a PC/Workstation with an internet connection. Via a web browser, users can login to a secure portal using their existing credentials so to retrieve message data and/or send out any new messages.

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 (R)

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

With TeleMessage, 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.

TeleMessage can configure logging and auditing on our SaaS-70 Type II platform. In additional, TeleMessage can also provide a direct feed from our servers to our clients of all message activity.

TeleMessage provides message delivery status and audit controls. In order to provide traceable, detailed delivery and receipt information. The TeleMessage 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. TeleMessage 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 have 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 TeleMessage 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 SSL encryption (128/256-bit). Data-at-rest on the mobile devices is also AES encrypted.

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?

TeleMessage uses a combination of Secure Sockets Layer (SSL) protocol to create a uniquely encrypted channel for private communication of health care data in motion. This is followed by Advance Encryption Standard (AES) encryption for data–at–rest. TeleMessage thus provides total coverage for moving any type of sensitive data to/from mobile devices through its secure messaging platform.

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.

Yes, both internal and external risk assessments are regularly performed to identify risks and vulnerabilities that may impact the client's PHI/ePHI data. Both our application and hosting environments have been assessed for risk and vulnerabilities.

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?

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?

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

Yes, TeleMessage is a fast maturing startup but our mission is to provide controls and security the enterprise demands. Our policies and procedures limit or, in almost every case, restrict any access internally to ePHI data, because we are only a "pass through" for that data. We don't process or analyze the data, just route it from source to destination.

We do have an information security policy for the organization and are quickly maturing to meet our future goal of becoming ISO compliant. In turn, this will allow us as an organization to not only meet ISO requirements for security but CoBit, NIST and HIPAA as well.

However, we have to balance this effort along with allocating resources to continue to build and mature our product offering. Through the steps we have taken to ensure strong access authorization controls, we feel we are progressive in terms of security posture given the size and scope of our company.

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. But again, any data's lifespan (TTL) on our infrastructure is on a restricted time frame. Data is flushed regularly based on the lifespan setting. Once deleted, data is permanently removed. We are not a data storage company so we do not retain or keep data beyond the lifespan setting.
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, TeleMessage 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.
Disaster Recovery Plan (R) 164.308(a)(7)(ii)(b) Implement policies and procedures to support execution of proper data recovery plans.	
Specific Question | Has your organization developed procedures for restoring data in the event of a disaster or widespread emergency?	Yes, based 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. TeleMessage's high availability infrastructure provides fault tolerance and redundancy.
HIPAA Security Rule Evaluation (R) 164.308(a)(8) Implement policies and procedures to support execution of proper data recovery plans.	
Specific Question | Has your organization performed a self or external evaluation of your operations, in accordance with the HIPAA Security Rule?	Yes, as part of our policy to promote security and compliance to regulations to ISO, NIST and HIPAA, we conduct self-evaluations yearly to measure progress and maturity in this area. We continue to improve both direct IT controls and any compensating control as needed to make sure we are always driving to compliancy with these regulations.

PHYSICAL SAFEGUARDS

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

Facility Security Plan (R) 164.310(a)(2)(ii) Implement policies and procedures to support strong controls for physical access controls.	
Specific Question | Have procedures and controls been implemented to safeguard your facility(s) and equipment from unauthorized physical access or theft?	Yes, TeleMessage has a physical security policy that outlines procedures and controls to support unauthorized physical access or theft of any data in our office and data center locations. In fact, customer data is neither kept nor stored in our office environment. All message data securely routes directly through our Tier-IV SaaS-70 Type II hosted infrastructure.
Access Controls and Validation Procedures (R) 164.310(a)(2)(iii) Implement policies and procedures to support strong controls for physical access controls.	
Specific Question | Have procedures been implemented to control and validate a person's access to your facilities, especially data centers?	Yes, pin code is required for building access and office access keys are only provided to key personal for tight access controls. All sensitive data contracts, HR documents etc. are in locked file cabinets. Important to note is that NO client message data (PHI or other) actually resides at our office location (internal workstations, servers or laptops.) Data Center access controls follow SaaS-70 Type II standards and procedures as well as industry best practices.

ORGANIZATIONAL REQUIREMENTS

This category focuses on overall organizational requirements in order to understand general practices effecting Business Associate obligations and patterns.

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, TeleMessage has not had any violation of HIPAA Security Rules
Business Associate Contracts (R) 164.314 (a)(1)(i) 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 that it receives or transmits on SJHS' behalf? 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? Will client be authorized to terminate contract if SJHS determines that the BA has violated a material term?	Yes, we are prepared to satisfy all requirements related to Business Associate. Even though we act only as a messaging channel, our SaaS-70 supported infrastructure is designed to facilitate secure and private message 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

TeleMessage took the initiative to enhance existing SMS and created a purpose–built solution for the health care sector that provides an easy-to-use, cost–effective, extremely secure and bi–directional mobile platform. The scarcity of primary care doctors is also forcing health care providers to look for ways to utilize mobile technol-ogy to increase efficiency, improve patient care and drive new businesses to their practice, without compromis-ing on compliance with HIPAA standards.

With TeleMessage for Business, it is now so much easier to communicate to emergency departments for procuring information and scheduling logistics. Even medical transcription companies are utilizing text messaging to expedite the process and route information effortlessly to the concerned physician at a moment's notice. As an organization, TeleMessage values all aspects of security including its development of secure products, its people and the supporting technology infrastructure. TeleMessage has recently started the process of establishing a security roadmap that leads to future ISO 27002 certification, on-going external 3rd party risk assessments and testing and as well as planning for execution on a formal HIPAA Compliancy Program Development, Risk Assessment and Audits. These programs have been initiated by the CEO and the executive team as part of TeleMessage's commitment to overall security best practices and making sure it's customers can be confident in their ability to remain compliant to HIPAA and other regulations while deploying the TeleMessage Secure Mobile Messaging solution in their organizations.

Secure Data Centers

Data centers should be secure and regularly assessed for security controls through on-going risk assessments.

- TeleMessage has partnered with industry leaders for data center services. Data Centers are Tier–IV, SaaS–70 Type II Certified and as well ISO 27001 compliant, providing SLAs at 99.95% for availability. Through this partnership, TeleMessage reinforces its core commitment to customers in regards to HIPAA Compliance through support for security, privacy, scalability and redundancy.

Text Messages Must be delivered only to the Requesting Recipient

- TeleMessage or Business provides message delivery status and audit controls. In order to provide traceable, detailed delivery and receipt information, the TeleMessage for Business application clearly indicates when the message was received on the device and when it was acknowledged by the recipient.

Encryption

Encrypted to protect electronic health information from unauthorized access while being transmitted over electronic networks.

- TeleMessage uses a combination of "Secure Sockets Layer" (SSL) protocol to create a uniquely encrypted channel for private communication of health care data in motion. This is followed by "Advance Encryption Standard" (AES) encryption for data at rest. TeleMessage for Business thus provides total coverage for moving any type of sensitive data to and from mobile devices through its secure messaging platform.

Archival, Retrieval, and Monitoring Requirements for Electronic Messaging

It is evident that data archiving, retrieval and monitoring will be a key element in any customer-centric SMS, text messaging solution for the health care industry. This is relevant for both security and regulatory purposes.

- TeleMessage or Business solution allows full flexibility to leverage existing deployed solutions for archival, retrieval and monitoring. There is also the option to deploy with TeleMessage for Business and leverage its own capabilities for the required functions. TeleMessage for Business has robust archiving, retrieval and monitoring capabilities that support not just the present–day compliance requirements for SMS, text messaging but future concerns as well. Layered on top of TeleMessage's rich core architecture is an extensible framework that allows seamless integration into other solution providers for enhanced compliance capabilities.

COMPANY PROFILE | TeleMessage

TeleMessage delivers intelligent and secure messaging seamlessly over any communication device.
TeleMessage helps operators retain their subscriber base by enhancing the user experience and assists enterprises achieve greater efficiency by optimizing their communication capabilities, TeleMessage seamlessly handles text, voice, data, multimedia and IP messages over mobiles, tablets, the web, Office, APIs and IT infrastructure.
Successfully deployed with over forty operators and thousands of enterprises worldwide, TeleMessage's software reaches hundreds of millions of users and powers billions of messages through customers networks.

TO LEARN MORE | Contact TeleMessage for Healthcare

Sales Team | ph: 978.263.1015 **| email:** sales@TeleMessage.com