GIVA HIPAA-COMPLIANT CLOUD HELP DESK SOFTWARE

All USA based hospitals, healthcare organizations, affiliated industries and foreign organizations doing business in the USA are required by law to meet the regulations of the Health Insurance Portability and Accountability Act (HIPAA). HIPAA compliance requires very strict security policies and data encryption with significant penalties for failing to protect personal health information (PHI) in electronic health and medical records. Giva makes HIPAA compliance very easy for our customers since the data center, hardware and software infrastructure of Giva's cloud help desk software meet the very strict HIPAA compliance regulations.

7 KEY ELEMENTS OF HIPAA-COMPLIANT MANAGED HOSTING

1) Business Associate Agreement (BAA)

2) Data Encryption

3) Onsite and Offsite Backup

4) Physical, Logical and Network Access Controls

5) Vulnerability Management and Logging

6) Security, Incident, and Training Policies

7) SSAE 18 SOC 2, Type 2 Certified Facilities-Controls-Process

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

GIVA'S HIPAA-COMPLIANT CLOUD HELP DESK SOFTWARE INCLUDES A BUSINESS ASSOCIATES AGREEMENT (BAA) TO PROTECT ELECTRONIC HEALTH & MEDICAL RECORDS

✓ A HIPAA business associate agreement (BAA) is a contract between a HIPAA-covered entity (Giva's customer) and a HIPAA business associate (Giva). The contract protects personal health information (PHI) in any electronic health or medical record of the HIPAA-covered entity in accordance with HIPAA regulations.

✓ The signed BAA contractually obligates Giva to protect our customer's PHI. This means that Giva shares liability with our customers in the very unlikely event of a data breach.

✓ A BAA clearly defines the roles and responsibilities of Giva in protecting PHI in hospital and healthcare electronic health or medical records.

✓ Cloud help desk software used by a hospital or healthcare organization without a BAA is not HIPAA complaint.

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

DATA ENCRYPTION FOR GIVA'S CLOUD HELP DESK SOFTWARE

Giva uses HIPAA-compliant data encryption to ensure that all PHI data in hospital and healthcare electronic health and medical records is secure.

SSL – Private Website Encryption

✓ Giva uses 256-bit secure sockets layer (SSL) certificates established on our cloud help desk software for any domains on which sensitive information is accessed or displayed.

✓ All access to our cloud help desk software requires secure login credentials.

✓ With our high availability data center infrastructure, SSL is also installed on the load balancers to ensure end-to-end privacy.

VPN – Secure Remote Access

✓ All remote access, system administration connections and data transfers to Giva's HIPAA-compliant cloud help desk software for electronic health & medical records are encrypted using an SSL VPN (virtual private network) with dual factor authentication.

✓ All data travels across an encrypted VPN using very strong encryption. Giva uses the strongest encryption available from leading security vendors to protect sensitive PHI in electronic health and medical records.

Data Encryption Required for HIPAA Compliance

✓ In Motion - All sensitive electronic health and medical records data with patient health information, such as SSNs, patient diagnosis, medical history, etc. is encrypted using 256-bit secure sockets layer (SSL).

✓ Backups - Giva encrypts all backups of customer data which may include PHI from electronic health and medical records. HIPAA-compliant security controls are in place to limit and log all access to any backups.

✓ At Rest – All customer data, which may include PHI from electronic health and medical records, is encrypted when at rest.

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

ONSITE AND OFFSITE ENCRYPTED BACKUPS FOR GIVA'S CLOUD HELP DESK SOFTWARE

Giva's HIPAA-compliant backup strategy creates regular backups on a daily and weekly basis to enable the ability to quickly restore data from encrypted backups, if needed.

Onsite Backups

✓ Data Backup Plan (R) - § 164.308(a)(7)(ii)(A) Giva's HIPAA-compliant backup procedures create and maintain retrievable exact copies of all data that contains protected health information (PHI) from electronic health and medical records.

✓ Giva performs daily incremental backups and weekly full backups. Weekly full backups are retained for 2 weeks and daily incremental backups are retained for 1 week to ensure that critical data remains safe, encrypted and always available.

✓ Primary Backups are stored locally for fast restores.

Offsite Backups – Data Center – Different Location

✓ Offsite backups are a key requirement of HIPAA's Disaster Recovery Plan (R) -§164.308(a)(7)(ii)(B) to ensure procedures are in place to prevent data loss.

✓ To mitigate the risk of a catastrophic data loss in our redundant data center facilities, Giva further replicates backups to another data center in a different location.

✓ Backups are replicated to our offsite data center facility in a different location
every 24 hours.

PHYSICAL, LOGICAL, AND NETWORK ACCESS CONTROLS FOR GIVA'S CLOUD HELP DESK SOFTWARE

Giva's HIPAA-compliant security approach uses a comprehensive multi-tiered security strategy to protect PHI in electronic health and medical records combined with a multi-tenant infrastructure to manage costs for our customers. Giva's cloud help desk software is compliant with security and privacy standards including HIPAA, PCI, SSAE 18, and Safe Harbor.

Physical Access Controls of Data Centers

PHYSICAL SECURITY

- ✓ Restricted Parking / Premises
- ✓ Restricted Access to the Facility
- ✓ No Signs Identifying the Data Center
- ✓ Security Guard 24x7
- ✓ Photo ID Required
- ✓ Sign-In / Sign-Out Process

DATA CENTER SECURITY AND FACILIITY

Access Rights

- ✓ Restricted Access to Facilities
- ✓ Biometric Access Required
- ✓ Signs Posted for Restricted Access
- ✓ Unique Access ID for Each Employee
- ✓ Process for Granting/Revoking Access
- ✓ Escort Required for Visitors/Vendors
- ✓ Reconciliation of Staff with Access

Access Tracking

- ✓ Live Monitoring of Accesses
- ✓ Digital Log of Door Accesses
- ✓ Written Visitor Log
- ✓ Camera Placement at All Door Access
- ✓ Points, Aisles/Cages

Data Protection

- ✓ Shredders to Destroy Sensitive Documents
- ✓ Server Cabinets Secured
- ✓ Network Cables and Sockets Secured

Logical Access Controls

- ✓ Separation between each customer's data
- ✓ Separate & Defined Server Roles
- ✓ Access control and logging for all access to servers with PHI
- ✓ Firewalls between Public/Private Server Zones

DOCUMENTED POLICES/CONTROLS

- ✓ Access Control
- ✓ Password Management
- ✓ Firewalls
- ✓ Virus Protection
- ✓ Data Classification
- ✓ Encryption
- ✓ Retention
- ✓ Destruction
- ✓ Production Change Management
- ✓ Incident/Problem Management Program
- ✓ Security Incident Response Plan
- ✓ Risk Management

Network Access Controls

FIREWALL

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

- ✓ Cisco Hardware ASA firewalls
- ✓ Firewall redundancy
- ✓ Point to Point VPN Tunnels
- ✓ SSL VPN Remote Access
- ✓ Dual Factor Authentication
- ✓ 3DES Encryption
- ✓ IPSEC Tunnels INGRESS and EGRESS Filters

NETWORK

- ✓ Private VLAN
- ✓ DMZ Zone for public services
- ✓ Internal Zone for private server

INTRUSION PREVENTION

- ✓ Intrusion Detection
- ✓ Intrusion Prevention
- ✓ Prevention of "Phone Home bots"
- ✓ DDOS Mitigation
- ✓ SSL Offload IDS/IPS of SSL traffic
- ✓ Web Application Firewalls for OWASP 10

ENTERPRISE – ANTI-VIRUS

- ✓ Enterprise Grade Anti-Virus
- ✓ Host-based intrusion prevention
- ✓ Centralized Reporting
- ✓ Abnormal Process Logging

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

VULNERABILITY MANAGEMENT AND LOGGING FOR GIVA'S CLOUD HELP DESK SOFTWARE

A security-first approach means that a regular assessment of application vulnerabilities is a key part of providing the highest levels of data security for PHI from electronic health and medical records. Proper log management is utilized for anomaly detection and forensic analysis.

Vulnerability Management

- ✓ Monthly third-party vulnerability and penetration scan
- ✓ Security team reviews scan results
- ✓ Remediation of all threats found
- ✓ Partner with Trustwave for extended validation
- ✓ Whitelists on IDS/IPS and Web Application Firewalls to ensure vulnerability scanners have enhanced view into infrastructure
- ✓ Timely infrastructure patching to ensure all security updates are applied
- ✓ Security research for proactive notification of potential threats

Comprehensive Logging

- ✓ Tripwire Enterprise security solutions
- ✓ File Integrity Monitoring to detect changes to system files preventing back doors and root kits
- ✓ Log offloading into external log servers to prevent attackers from "covering their tracks"
- ✓ Enhanced retention of firewall, web app firewall, and event logs
- ✓ Dual factor authentication with extended logging for remote users

DEFINED AND TESTED SECURITY POLICIES AND PROCEDURES FOR GIVA'S CLOUD HELP DESK SOFTWARE

Giva's HIPAA-compliant data centers have a comprehensive set of documented policies that have evolved in accordance with security standards and best practices. These security policies go beyond basic data center compliance and encompass how technology, people and process come together to drive outcomes to protect PHI in electronic health and medical records.

Giva Policy Documents Available for Review

- ✓ Annual SOC 2 Type 2 Auditors Report
- ✓ Backup Policy
- ✓ Disk Sanitization and Destruction Procedures
- ✓ Monitoring Incident Response Procedures
- ✓ Packet Inspection Exceptions Policy
- ✓ Patching and Maintenance Policy
- ✓ Infrastructure Change Management Policy
- ✓ Security Incident Response
- ✓ Service Level Agreement
- ✓ Security & Datacenter Audit Fact Sheet
- ✓ Business Continuity Plan
- ✓ Escalation Procedures
- ✓ Company Security Policy
- ✓ Data Classification Policy
- ✓ Problem Management Procedure
- ✓ Human Resources Procedure for new employee addition
- ✓ Provisioning Quality Assurance Policy and Procedures
- ✓ Customer Authentication Procedures
- ✓ Procedure for Reviewing Vulnerability Reports

SSAE 18 SOC 2 TYPE 2 CERTIFICATION FOR GIVA'S CLOUD HELP DESK SOFTWARE

SSAE 18, also called Statement on Standards for Attestation Engagements 18, is a regulation created by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA) for defining how data centers report on compliance controls.

Technology

Enterprise and service provider class technology from Dell, Cisco, F5, VMware, EMC, Netapp, Tripwire, Trustwave, Microsoft and Red Hat.

People

Skilled HIPAA-certified engineers available 24/7/365.

Process

All processes are validated against a rigorous set of controls by an independent team of CPA auditors. The annual SSAE 18 SOC 2 Type 2 compliance report is issued and shared with all Giva customers upon request.

The SOC 2 framework is a comprehensive set of criteria known as the Trust Services Principles that are composed of the following five sections:

- Security of a service organization's system.
- Availability of a service organization's system.
- Processing integrity of a service organization's system.

- Confidentiality of the information that the service organization's system processes or maintains for user entities.
- Privacy of personal information that the service organization collects, uses, retains, discloses, and disposes of for user entities.

The Type 1 SSAE certification performed for many data centers uses the following criteria:

1. The description of the service organization's system was designed and implemented as of only a _single specified report date which is typically 12/31/xx_.

2. The control objectives stated in the description were suitably designed to achieve compliance as of only a _single specified report date which is typically 12/31/xx_.

In other words, a Type 1 report is just a snapshot in time at a particular date which is typically 12/31/xx.

In sharp contrast, the Type 2 SSAE certification performed for Giva's data centers uses the following criteria which are more rigorous, difficult to pass and a higher overall standard:

1. The description of the service organization's system was designed and implemented _over the period of examination which is typically a one year period such as 1/1/xx – 12/31/xx._

2. The control objectives stated in the description were suitably designed to achieve compliance _over the period of examination which is typically a one year period such as 1/1/xx – 12/31/xx_.

Datacenter Specifications

POWER

✓ Direct connection to power grid at 13.2 kV

- ✓ 2N electrical design
- ✓ Dual Redundant UPS / Battery Strings
- ✓ Automatic Transfer Switch
- ✓ 750 kW back-up generator
- ✓ 2300 Gallons of fuel onsite
- ✓ Enough capacity for up to 7 days

COOLING

- ✓ n+1 Design
- ✓ Redundant CRAC Cooling
- ✓ Temperature of 70 degrees F / 50% Hum
- ✓ Hot Aisle/Cold Aisle Design
- ✓ Redundant Glycol Pumps

FIRE

- ✓ Dry-piped pre-action fire protection system
- ✓ FM200 Gas Fire Suppression System

CONNECTIVITY

- ✓ 3 Tier 1 Network Carriers
- ✓ 30 Gbps Bandwidth
- ✓ 4 Fiber Paths
- ✓ 2N Network Design

Giva™

+ DEPLOY IN DAYS / TRAIN IN 1 HOUR
+ HIGHLY CUSTOMIZABLE WITHOUT PROGRAMMING OR CONSULTANTS
+ ROBUST, FAST & PAINLESS REPORTING FOR HIGHER QUALITY DECISION-MAKING

ABOUT GIVA

Founded in 1999, Giva was among the first to provide a suite of help desk and customer service/call center applications architected for the cloud.

Now, with hundreds of customer driven releases, the Giva Service Management™ Suite delivers an intuitive, easy-to-use design that can be deployed in just days and requires only one hour of training. Giva's robust, fast and painless reporting/analytics/KPIs quickly measure team productivity, responsiveness and customer satisfaction resulting in faster and higher quality decision-making. Customization and configuration are all point and click with no programming or consultants required to deliver a substantially lower total cost of ownership.

Giva is a private company headquartered in Santa Clara, California serving delighted customers worldwide.

robust, fast & painless
reporting for higher quality
decision-making

deploy in days,
train in 1 hour

highly customizable without
programming or consultants

the **Giva**difference