Frequently Asked Questions (FAQs) Pertaining to Glassbeam CLEAN™ Blueprint

Glassbeam Solutions for the Healthcare Market

Version 1.0, November 2018
# Table of Contents

1. How do you connect to my machines to get data? ................................................................. 1
2. How does the Gateway server collect data from the machines? ........................................... 1
3. Are you modifying or installing any software on the medical machine in anyway? .............. 1
4. What type of data is pulled out? .............................................................................................. 1
5. Who will have access to the Gateway Server and our internal network? ............................ 2
6. Is the (medical) data protected during transmission from Device to Glassbeam? ................ 2
7. Where is my data stored? Will our data be protected in the cloud? .................................... 2
8. How do you ensure security while data is at rest? ............................................................... 2
9. Is my data shared with anyone? Who gets access to it? ....................................................... 3
11. How do users access the data securely? ................................................................................ 3
12. How do you backup and restore data in case of failures? .................................................... 3
13. How long do you keep my data? ............................................................................................ 3
14. When requested upon contract cancellation, how do you securely destroy my data? ........ 3
16. Are you HIPAA compliant? ................................................................................................... 4
17. How does Glassbeam ensure that cloud based applications are free from any virus attacks or software vulnerabilities? ............................................................................................. 5
Here is a sampling of key questions that prospects in healthcare provider market enquire in the context of Glassbeam Healthcare solution.

**How do you connect to my machines to get data?**

Glassbeam uses a Gateway server to collect data from the machines. The Gateway server is located inside the customer firewall, where it collects data from medical devices and the PACS (Picture Archiving and Communications System) server. Once the data is collected, processed, anonymized and desensitized, the Gateway Server will securely transmit data to the Glassbeam cloud.

The Gateway server has three main functions:

- Accept data from all data sources, such as Medical Devices and PACS servers.
- Desensitize of all procured data
- Securely Transmit data from the hospital/clinical network to the Glassbeam Cloud by using secure protocols or VPN (site-to-site or point-to-point) connections.

*For more information, please read our Blueprint document.*

**How does the Gateway server collect data from the machines?**

The PACS Server will transfer data to the Gateway Server, via the DICOM (Digital Imaging and Communications in Medicine) protocol. Medical Devices will transfer data to the Gateway Server via SSH or SFTP.

**Are you modifying or installing any software on the medical machine in anyway?**

No software is installed on any of the machines. The only modifications made by Glassbeam are located in the configuration settings for outbound traffic, which do not impact the operation or performance of the machines. These modifications are needed in order to push data from the machines to the Gateway server.

**What type of data is pulled out?**

Glassbeam captures data from three sources:

*Modalities – Medical Devices:* Glassbeam captures machine logs that contains information, such as Configurations, Alerts/Events, State Information, Statistical Information, and Error Logs

*CMMS (Computerized Maintenance Management System):* Glassbeam captures maintenance information from CMMS systems, such as Work Order History, Asset Information, and Asset Maintenance History.

*PACS (Picture Archiving and Communications System):* Glassbeam accesses the PACS server to and captures DICOM Header information (no PHI data).
Who will have access to the Gateway Server and our internal network?

Only authorized personnel are given access to the Gateway server. In addition, the access is provided over a secure channel. Here are the safeguards in place:

- Multi-factor authentication to jump host
- Hardened systems and firewall rules protecting jump host
- Encrypted tunnel between Glassbeam and client networks

Is the (medical) data protected during transmission from Device to Glassbeam?

Glassbeam ensures encrypted data transmission over public networks. Patient sensitive information is stripped out before any transmission is made to Glassbeam. Confidential and sensitive information which can be intercepted, modified or diverted is encrypted during transmission over networks. Some examples of strong encryption are:

- Secure Socket Layer (SSL)
- Internet Protocol Security (IPSEC)

Where is my data stored? Will our data be protected in the cloud?

Data is stored on the cloud such as AWS (Amazon Web Services). At no point is the customer’s data stored on any of Glassbeam’s servers or at any of its facilities. For the infrastructure, Glassbeam partners with several world class PaaS providers like AWS in the Enterprise Cloud and Managed Hosting industry. These services are fully SA60 (SAS 70) compliant.

For more information on data security with AWS, click here

Preventing unauthorized access to a customer’s data is a critical business imperative for Glassbeam. While Glassbeam is a multi-tenant hosted SaaS service, it fully secures your data and makes it accessible only to users with appropriate access rights. Glassbeam employs a comprehensive tagging algorithm which tags all data to a unique hierarchical combination of manufacturer, product and schema.

How do you ensure security while data is at rest?

Raw logs received from the devices are stored in a log vault. This vault resides on Amazon’s S3 service. S3 is accessible only through an API with a pre-shared secure access key.

Processed data is stored in a variety of databases like Cassandra, Vertica etc. All databases are stored behind Amazon’s Firewall, which do not allow outside access to the machine. The database servers do not have public IPs assigned to them and can only be accessed by applications running within the subnet.
Is my data shared with anyone? Who gets access to it?

Customer data is not shared with any un-authorized entity. All confidential or sensitive data is protected via access controls to ensure that data is not improperly disclosed, modified, deleted or rendered unavailable. Logs track all access to such data and identify how and when the data was accessed.

Employees who have been authorized to view information at a particular classification level are only permitted to access information at that level or at a lower level on a need to know basis. All access to systems is configured to deny all except what a particular user needs to access per their business role.

How do you prevent data bleed across customers?

One potential security concern for SaaS applications is multi-tenancy. Such applications are sharing infrastructure across customers, such as Sales Force, Glassbeam etc. Applications provide safeguards that data does not bleed across customers. Glassbeam does this by not even accepting data which is not properly tagged to a customer. In fact there are 4 levels of hierarchical tagging. A user accessing the data is also pinned to a customer, so there is no way data for one customer can be seen by a user of another customer. For more information on how Glassbeam provides additional application level security, click here.

How do users access the data securely?

Users access the data over a web based interface. This interface is served over a 128 bit encrypted SSL connection. All Glassbeam applications are already migrated to use TLS 1.2 which is a successor to SSL. TLS runs at the transport layer of the OSI model. When a server and client communicate, TLS protocol ensures that no third party may eavesdrop, tamper with any message, and message forgery.

How do you backup and restore data in case of failures?

Glassbeam application ensures that all persistent data is highly available. This is ensured through redundancy in storage. Raw logs are stored in a log vault on Amazon’s S3 service. Processed data is stored in databases which are clustered and have an inbuilt replication across nodes. We use a replication factor of 3 – which means that all data is replicated 3 times. Application performance is not impacted even if 2 nodes fail.

How long do you keep my data?

All confidential and sensitive data, regardless of storage location, is retained only as long as required for legal, regulatory and business requirements. The specific retention duration is pre-agreed with customers and written in the contract.

When requested upon contract cancellation, how do you securely destroy my data?

All confidential or sensitive electronic data, when no longer needed for legal, regulatory or business requirements
is removed from Glassbeam systems using an approved method documented in Glassbeam's Information Security Policy. This requirement includes all data stored in systems, temporary files or contained on storage media.

For more information on Glassbeam's Information Security Policy, contact sales.

Are you collecting and transmitting Patient data? How do you handle PHI in DICOM data? How do you desensitize patient data?

Glassbeam does not collect or transmit Patient data. While Glassbeam does collect DICOM data, it passes through a scrubber program which removes all patient data. Our security consultant compared incoming DICOM data against the output created by the scrubber. The results are outlined below (all identifiers shown below are fictitious).

The following identifiable information was identified:

(0010,0010) PN [DOE^JENNIFER^A] # 18, 1 PatientName
(0010,0020) LO [GB1286528] # 10, 1 PatientID
(0010,0030) DA [19611205] # 8, 1 PatientBirthDate
(0010,0040) CS [F] # 2, 1 PatientSex
(0010,0101) SQ (Sequence with undefined length #=1) # u/l, 1 PatientPrimaryLanguageCodeSequence
(0010,1010) AS [056Y] # 4, 1 PatientAge
(0010,1030) DS [99.88] # 6, 1 PatientWeight
(0010,1040) LO [62 DR #1016^PLANO^TX^11111] # 34, 1 PatientAddress
(0010,1060) PN (no value available) # 0, 0 PatientMotherBirthName
(0010,2150) LO [US] # 2, 1 CountryOfResidence
(0010,2154) SH [\^] # 2, 2 PatientTelephoneNumbers
(0010,2160) SH [UNK] # 4, 1 EthnicGroup
(0010,2180) CS [UNKNOWN] # 8, 1 SmokingStatus

They verified that none of these identifiers are present in the output.

Are you HIPAA compliant?

Yes, Glassbeam is HIPAA compliant. Glassbeam performed a risk assessment for HIPAA Security Rule (45 C.F.R. §§ 164.302 – 318), HIPAA Privacy Rule (45 C.F.R. §§ 160, 164.500-534), and Breach Notification Rule (45 CFR §§ 164.400-414) during the period of September 12 to 21, 2018. This assessment included a review of appropriate
administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (ePHI).

The assessor’s certified that Glassbeam is operating in a manner that complies with the standards and specifications detailed in the HIPAA Privacy Rule, HIPAA Security Rule, and HIPAA HITECH Act.

**How does Glassbeam ensure that cloud based applications are free from any virus attacks or software vulnerabilities?**

Glassbeam periodically performs penetration testing of all externally facing servers. In addition it also performs an application vulnerability scan which detects and reports on known vulnerabilities in the application. The scan specifically looks for:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging and Monitoring
Glassbeam is the premier machine data analytics company bringing structure and meaning to complex data generated from any connected machine in the Industrial IoT industry. Funded by several ultra-high net worth investors, Glassbeam’s next generation cloud-based platform is designed to transform and analyze multi-structured data, delivering powerful solutions on customer support and product intelligence for companies such as IBM, Dell EMC, Novant Health, PTC, Dimension Data, Kodak Alaris, UCSF, Brown’s Medical Imaging, and RES.

2350 Mission College Blvd., Suite 777, Santa Clara, California 95054
408-740-4600
www.glassbeam.com
www.glassbeam.com/resources
www.linkedin.com/company/glassbeam-inc
@Glassbeam