Security White Paper

Overview

This White Paper presents the security details of the Trice Imaging service known as Tricefy. The paper explains how Tricefy meets security and privacy requirements associated with General Data Protection Regulation (GDPR) and other applicable laws and regulations.

Tricefy is a cloud-based system that receives and manages medical images (DICOM) from any imaging device (e.g. ultrasound), converts them to various consumer formats and makes them accessible to clinicians and patients. Figure 1 below shows the basic components of the system, followed by a description of each component:

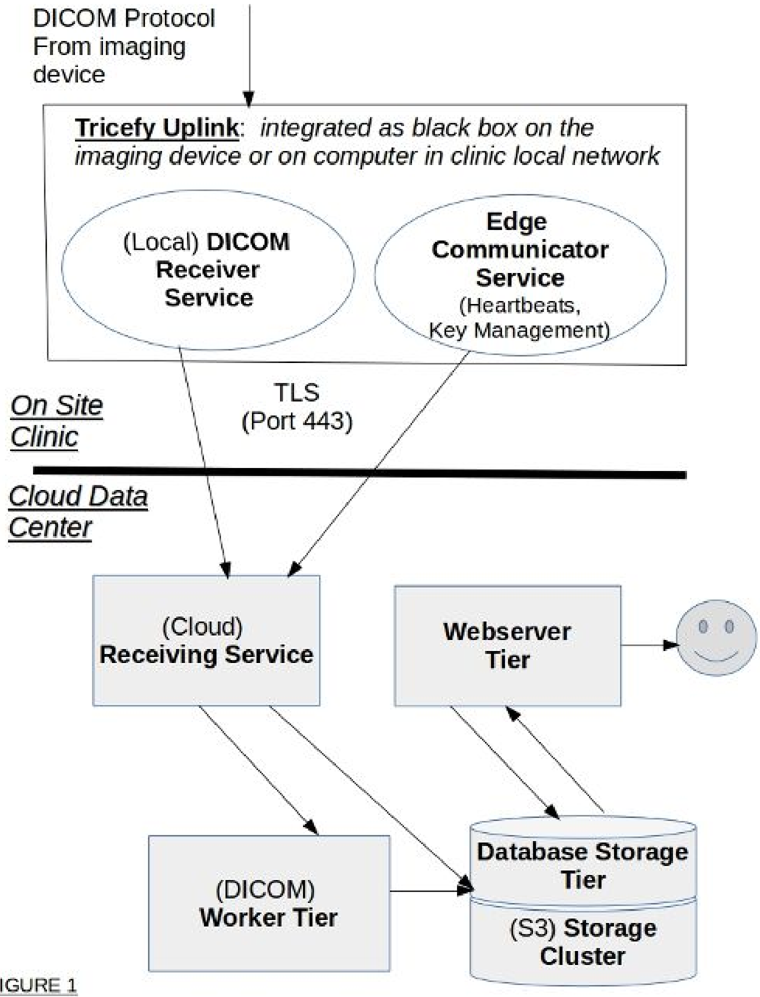
DICOM Protocol
From imaging
device
Tricefy Uplink: integrated as black box on the imaging device or on computer in clinic local network
(Local) DICOM Receiver Service
Edge Communicator Service (Heartbeats, Key Management)
TLS
(Port 443)
On Site Clinic
Cloud Data Center
(Cloud) Receiving Service
Webserver Tier
(DICOM) Worker Tier
Database Storage Tier
(S3) Storage Cluster

FIGURE 1

Tricefy components:

- Two small background services run (without admin or root privilege) on any computer or device in the customer's local network. These two services are hereby referred to as ***Tricefy Uplink***:
  - **DICOM Receiver Service**: A C-STORE, C-FIND and C-ECHO SCP DICOM receiver
  - **Edge Communicator Service**: Exchanges identification and configuration packets (eg., heartbeats) securely with the Cloud Receiving Service. It securely sends data files to the cloud and implements the DICOM C-MOVE service thereby acting as the SCU of the Storage Service Class.
- Tricefy Cloud platform (running on Amazon Web Services (AWS) infrastructure) with the following subnets:
  - **Receiving Service**: Endpoints for the two customer-local services described above (aka, Tricefy Uplink)

  - **Web Server Tier**: Runs the web application that provides the UI for workflow, image management and collaboration software
  - **Processing Tier**: Compute services that process DICOM files into consumer formats (e.g. .jpg, .mp4). Asynchronous processing, logging and outbound notifications occur within this tier.
  - **Database and Object Storage**: Securely persisting DICOM images, metadata, examination data, etc.

Physical Security

Tricefy Uplink

The two customer-local services comprising Tricefy Uplink can reside on any computer in the customer's local network or optionally can be installed directly on the imaging device itself. The physical security of this computer or device will be governed by the customer's active security policies. Tricefy Uplink does not need anything special. It can be provided as a service for Windows, OS X (Mac), Linux, or Android.

Tricefy Cloud Platform

The AWS infrastructure that hosts the Tricefy Cloud Platform includes the facilities, network, and hardware as well as some operational software (e.g., host OS, virtualization software, etc.). The AWS infrastructure is designed and managed according to security best practices, as well as a variety of security compliance standards. Trice Imaging has a BAA with Amazon Web Services.

A detailed description of the AWS infrastructure related security can be found in their security whitepaper: http://d0.awsstatic.com/whitepapers/Security/AWS%20Security%20Whitepaper.pdf. This includes detailed descriptions of Network Security, Access, Account Security, Data Security (Integrity, Availability and Redundancy), Change Management, and Service-specific Security (including instance, storage and database-related security).

Network Security

Tricefy Uplink

- Local DICOM Receiver Service gets DICOM Protocol Data Values (PDVs) locally in the customer's secure network using port 104 (or other configured port)
- These PDVs are sent to the Cloud Receiving Service securely using Transport Layer Security (TLS) on port 443 or port 4443
  - Private pre-shared keys are used (TLS-PSK)
    - With PSK protocol and Diffie-Hellman key exchange
  - AES-256 (256-bit AES) used for all Tricefy Uplink communications
- Edge Communicator Service sends periodic heartbeat packets to the Cloud Receiving Service (port 443 or port 4443)

- ○ X.509 certificate with TLS 1.3 used for all service-level communications

Tricefy Cloud Platform

Figure 2 below depicts the Tricefy Cloud Platform’s Network topology:

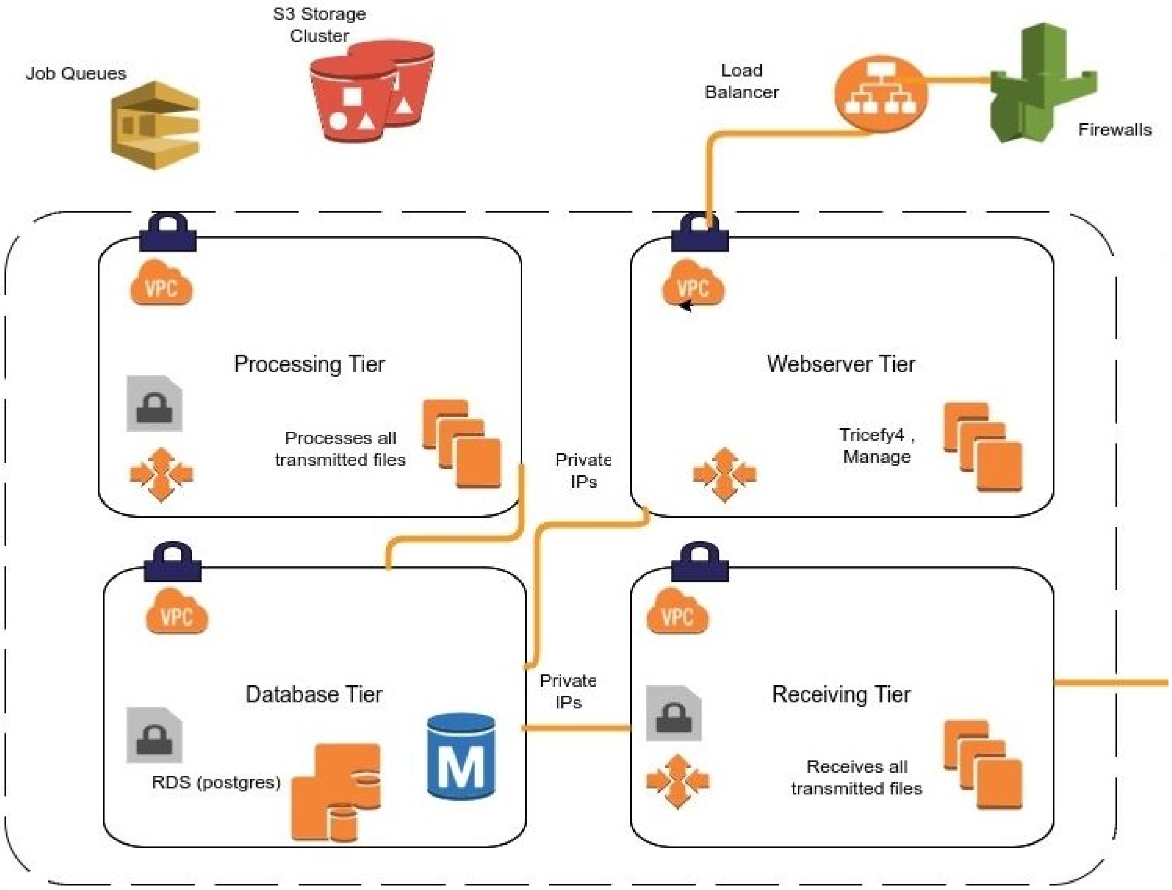

Figure 2

The Tricefy Cloud Platform is comprised of four functional tiers, each contained in a Virtual Private Cloud (abbreviated as VPC). A VPC is a cloud computing service in which AWS isolates a specific portion of their public cloud infrastructure for private use: the resources allocated to a Tricefy VPC are not shared with any other customer and include dedicated cloud servers, virtual networks, storage and private IP addresses.   Each Tricefy tier:

- Has redundant network locations (aka Availability Zones)
- Auto-scales to accommodate traffic fluctuation
- Has automatic termination and recreation of unhealthy hosts

The network security details of each tier are as follows:

- **Processing Tier**
  - ○ No synchronous communication with end users
  - ○ Object data transferred to and from the S3 Storage cluster using SSL/TLS and private IP addresses

    - Data transferred to and from the Database Tier using SSL/TLS and private IP addresses
    - 3d Party API calls made using SSL/TLS
- **Web Server Tier**
    - Port 80 is used only for HSTS redirection; port 443 is used to serve all application data
    - TLS with an AES-256 cipher is used for all browser access
    - Data transferred to and from the Database Tier using SSL/TLS and private IP addresses
- **Database Tier**
    - No network communication with end users, no external access is configured
    - Local access (private IP addresses) to other tiers in the Tricefy Cloud Platform
- **Receiving Tier:**
    - Direct TLS communication with Tricefy Uplink services (no intermediary load balancers used for most communications)
    - No outbound networked communication originates from this tier
    - Object data transferred to the S3 Storage cluster using SSL/TLS and private IP addresses
    - Data transferred to and from the Database Tier using SSL/TLS and private IP addresses
- **S3 Storage Cluster**
    - Local access (using private IP addresses) with the other tiers in the Tricefy Cloud Platform
    - Object data resides in the configured S3 region that satisfies all local and regional data privacy and protection laws.
    - Web Server tier uses secure URLs (SSL/TLS) to provide temporary user access to secure objects in the storage cluster. This is always done within the context of a secure session.

Cybersecurity

Extra technologies used to protect from attack, damage or unauthorized access are described below.

Penetration Testing

- Web Penetration Testing (or pen-testing) is a technique to evaluate cloud security by safely trying to exploit vulnerabilities. The output is a certified report of any exploitable security threats, vulnerabilities and risks allowing security staff to remediate as appropriate.
- Trice Imaging has pen tests performed regularly by a certified 3d party vendor (Provensec).

Web Application Firewall (WAF)

- The Tricefy WAF looks at every web (HTTPS) request sent to Tricefy; each web request is compared to a set of configurable rules to decide to either drop the request or allow it to continue. WAF rules include matching on the URL, HTTP header values or the request body so that web exploits including XSS (cross-site scripting), SQLi (SQL injection) and others that could compromise security are blocked.

Packet Level Filtering

Listening to packet level network traffic is not straight-forward within a third-party cloud environment like AWS since it is not possible to place a network appliance anywhere on the network perimeter.

Typical data center packet-level solutions include IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems). These solutions operate by listening passively (intrusion detection) or inline (intrusion prevention) to network traffic and matching this traffic to a rule set covering suspicious and malicious traffic signatures.

AWS Shield is a service that offers some IDS/IPS functionality as follows:

- Traffic filtering based on a combination of traffic signatures, anomaly algorithms and other analysis techniques to detect malicious traffic in real time
- Attack detection and mitigation for network and transport layers
- Metrics and reporting

Trice Imaging has enabled AWS Shield for all incoming traffic.

Continuous Monitoring and Associated Alerting

Trice Imaging uses 3d party services to provide both host and service based monitoring and alerting that includes metric collection, anomaly detection and analysis reports.

The alerts are integrated directly with a real-time communication platform allowing subscription based notifications and the ability to configure workflows in response to the alerts.

Data Security

All patient-related data is encrypted both in transit (as described in the Network Security section) and at rest. When data is persisted to any disk, it is guaranteed to be encrypted. The encryption occurs on the servers that host the instances, providing encryption as data moves between the instances and the storage. Encryption is based on the industry standard AES-256 cryptographic algorithm.

Data security for each part of the Tricefy system is described below:

Tricefy Uplink

- Tricefy Uplink: No patient data is persisted as part of any customer-local Tricefy Uplink service

Tricefy Cloud Platform

- **Processing Tier:**
    - Temporary storage is used by the Processing tier when DICOM is converted to consumer formats. All disks used for temporary storage are encrypted.
- **Web Server and Receiving Tiers:**
    - No patient data is ever persisted locally by the these two tiers.
- **Database Tier:**
    - The disks used by the database tier are all encrypted as described above.
- **S3 Storage Tier:**
    - All data in the S3 Storage tier is encrypted using strong multi-factor encryption. Each object is encrypted with a unique key; additionally the key itself is encrypted with a rotating master key. AES-256 (256 bit Advanced Encryption Standard) is used to encrypt the data.

Access Control

Server Access

- All access is controlled by SSH certificates
- Only technology staff responsible for server maintenance and production deployment are added as approved client certificate holders

Account Access

- In addition to authenticated clinic users, Customer Support Representatives and Software Developers may access a specific account in response to a support request or a system alert using this Break Glass Procedure
    - An administrative user can be tagged as a “super user” in the Tricefy database
    - A “super user” has the ability to login to all accounts
    - There is a detailed log showing who logged in and when; additionally, all accesses that occurred during the session are logged in detail

User Authentication: ID and Password

- Email address acts as the user id; users can create and change their own passwords
- Minimum password length required
- Password complexity rules enforced
- Multi-factor authentication via key-generating tokens (Yubikeys) and one-time codes (OATH-OTP) add additional security

Account Creation and Termination

- Clinics are set up and terminated by Trice Imaging Application Specialists or through an API that can be called by partners
  - Cinic termination invalidates Tricefy Uplink keys so that data is no longer received
- Clinics are created with one or more Administrative users
- Administrative users can invite colleagues to join their clinic

Auto Logoff

- Users are automatically logged off after configured time period expires

Access to Personal Information and Protected Health Information (PHI)

- Access to any data exposing personal data or PHI is always done in the context of a secure session with account level access
- Image and report data is always fully anonymized when sending links to patients

Software Process Security

- ISO 13485 certified processes for all product-related design, development and maintenance
- Data protection and security is integrated into the planning and design process for all active projects
- Distributed revision control and source code management
- Code coverage and code quality tools
- Continuous Integration
- Separate staging area matching production environment (all tiers)
- Automated testing (including security verification)
- Reproducible, fast, zero downtime deployment process with easy rollback

Disaster Recovery and Prevention

Database

- Replicas
- Scheduled data backups (with restore capability)

Storage Cluster

Figure 3 below shows how incoming radiology data is protected from unforeseen events:

- Incoming data is processed by the Receiving Service (1)
- As part of the transaction, the data is pushed to the primary storage cluster. This cluster is both distributed and replicated (2)
- The final step of the transaction is to copy the data to a bucket that exists in a completely separate account with access limited only to the Receiving Service. This backup bucket is also distributed and replicated (3)
- After a configurable number of days, the data is moved to cold storage, distributed and replicated as well (4)

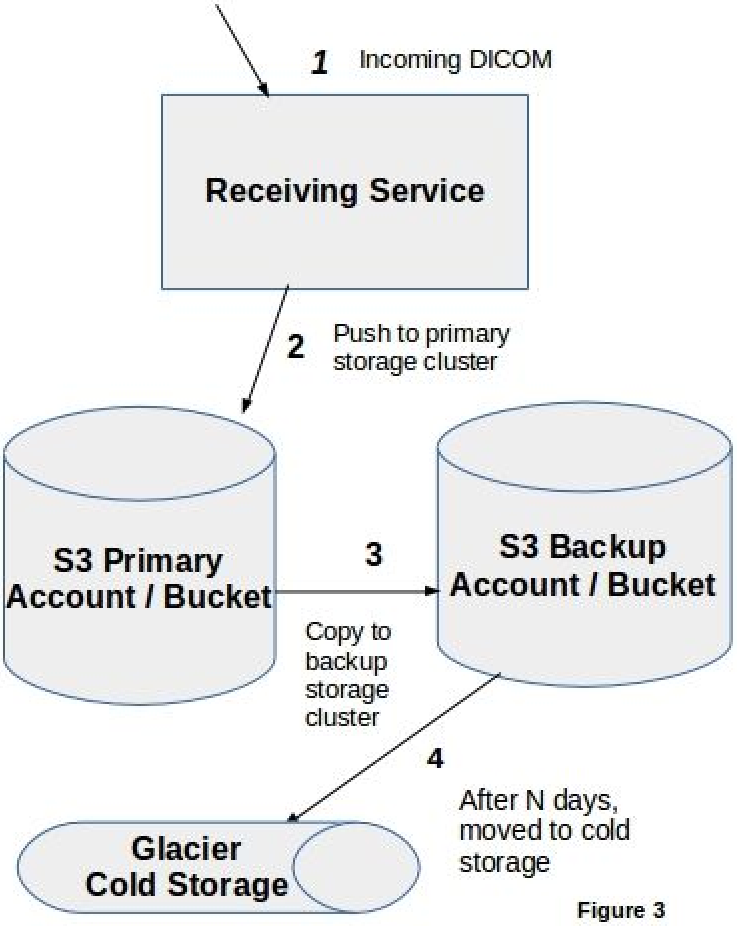
1
Incoming DICOM
Receiving Service
2
Push to primary storage cluster
S3 Primary Account / Bucket
3
S3 Backup Account / Bucket
Copy to backup storage cluster
4
After N days, moved to cold storage
Glacier Cold Storage

Figure 3