SliceVault Security and Compliance Whitepaper

December 2022

How SliceVault Protects Data

Table of Contents

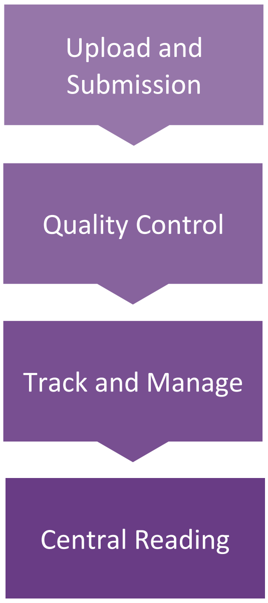
Introduction

The advancement of technology has transformed the way medical images are transferred, stored and shared in clinical trials. Imaging Data Management (IDM) platforms like SliceVault have become a key element in all imaging-based clinical trials. As the role of IDM platforms has evolved, the risk of security breaches has increased as well. Ensuring data confidentiality, allowing for system authentication and providing clear audit trails are necessities for every IDM platform provider.

The objective of this white paper is to outline the security features of SliceVault and describe how SliceVault helps clients meet their security and regulatory requirements, whether it is Good Clinical, Laboratory, and Manufacturing Practices (GxP) or other regulation enforced by competent bodies, such as the US Food and Drug Administration (FDA).

Product Overview

SliceVault is a cloud-based software that streamlines the transfer, management and analysis of medical images in clinical trials and related clinical research projects.



Sites submit medical images through a secure cloud portal. Personal health information is automatically removed in the process.

In the QC module qualified readers can perform manual quality control checks to ensure data quality and protocol compliance.

SliceVault tracks all enrolled patients and imaging data throughout the process. Queries can be issued, tracked and resolved within the same system.

Images can be analyzed by an Independent Review Board (IRP) using the optional Reader module or exported to external read environments.

To help organizations meet their security and compliance requirements, SliceVault is created and made available following strict Standard Operating Procedures designed to follow the requirements set forth in:

- FDA 21 CRF Part 11
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO9001:2015
- General Data Protection Regulation (GDPR)

Regulatory Compliance

FDA 21 CFR Part 11

FDA 21 CFR Part 11 provides guidance to suppliers who, in fulfilment of a requirement in a statute or another part of FDA's regulations, maintain records or submit information to FDA. The regulation sets out controls for closed systems like SliceVault. In particular, it specifies how to protect records, limit system access, use of secure and computer-generated audit trails, and how to perform authority checks to prevent unauthorized access.

There is no FDA 21 CFR Part 11 certification for providers of IDM platforms. SliceVault clients can access detailed computerized systems validation specifications and records that demonstrates SliceVault's compliance with FDA 21 CFR Part 11.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA sets the standard for sensitive patient data protection. Anyone who deal with Protected Health Information (PHI) must have documented security measures, including technical and physical security restrictions, in place to ensure HIPAA Compliance.

Complying with HIPAA is a shared responsibility between SliceVault and our clients. Specifically, HIPAA demands compliance with the Security Rule, the Privacy Rule, and the Breach Notification Rule. SliceVault is a HIPAA compliant IDM platform. See 'De-identification' section for more information about how SliceVault protects PHI as per HIPAA regulations.

SliceVault enters into Data Processing Agreements with all clients as necessary under HIPAA.

ISO9001:2015

SliceVault has dedicated significant resources to quality management and information security procedures. Our Quality Management System (QMS) is designed to meet the requirements set forth in ISO 9001:2015 and includes Standard Operating Procedures (SOP) and related records for software development, risk management, vendor assessment, CAPA, incident response, data recovery etc.

General Data Protection Regulation (GDPR)

The GDPR is a European privacy law that became effective in May 2018. It imposes rules on organizations that offer goods and services to people in the European Union (EU) or that collect and analyze data belonging to EU individuals. The GDPR requires that IDM platform providers like SliceVault provide sufficient guarantees to meet key requirements of the GDPR, including controlled procedures for: data subject requests, data protection impact assessments and data breach notification

SliceVault has necessary controls in place and provides clients, which are involved in the data processing of European citizens, with a contractual commitment regarding the GDPR in the form of a Data Processing Agreement.

Operational security

Malware protection

An effective malware attack can lead to account compromise and data theft. As a responsible IDM platform provider SliceVault takes these threats very seriously and uses a variety of methods to prevent, detect and eradicate malware. All our operational systems are protected by industry-leading commercial antimalware systems (Microsoft Antimalware for Azure) to provide real-time protection that helps identify and remove viruses, spyware and other malicious software.

Monitoring

All incoming traffic to SliceVault's operational systems is inspected for suspicious behavior, such as the presence of traffic that might indicate botnet connections. This analysis is performed using industry-leading commercial tools (Microsoft Defender for Cloud) for traffic monitoring and analysis.

SliceVault staff continuously monitors the health of all operating systems to remain vigilant to potential new threats and deliver a consistent service with a high degree of availability.

Incident Management

SliceVault leverage Microsoft's rigorous incident management process for security events that may affect the confidentiality, integrity, or availability of the IDM platform, any sub-systems or data. If there is a security incident, SliceVault strives to respond quickly and effectively to protect our services and clients' data. SliceVault employs an incident response strategy designed to investigate, contain, and remove security threats quickly and efficiently.

If an incident involves customer data, SliceVault will inform the customer and provide the necessary investigative efforts without undue delay.

Security Features

SliceVault provides a variety of security and compliance features that helps to protect data and maintain data integrity, including access controls, workflow limitations, image de-identification, Personal Health Information (PHI) redaction, audit logging and specialized processes to prevent untimely or illegal access.

Controlling Access

User Authentication and Authorization

In security-conscious environments with closed systems it becomes critical to limited access to valid users only. User authentication must be implemented to verify the identity of the person accessing the IDM platform. User authentication must be implemented to delegate access to data and functionality in the workflow of the IDM platform.

The SliceVault IDM platform offers a robust authentication option with user-session authorization to ensure that SliceVault workflows are run by valid and authorized users and that access to specific data and functions are properly restricted.

Authentication with Username and Password

Users can login to SliceVault using autogenerated login credentials and delivered by email. Once users have logged into SliceVault, new users are requested to change password, after which they have immediate access to their workflows and data.

The following restrictions apply to login credential:

- Users are requested to change password at least every 90 days
- Users are automatically blocked after five failed login attempts
- Users are automatically logged out if the user is inactive for 60 minutes
- New passwords cannot replicate the three last passwords
- Passwords must be at least 8 characters, contain at least one digit, at least one capital letter, special characters are allowed
- Username and password cannot be empty

Functionality to create new user accounts is restricted to a specific user role (Trial Administrator).

Limiting Workflow Access

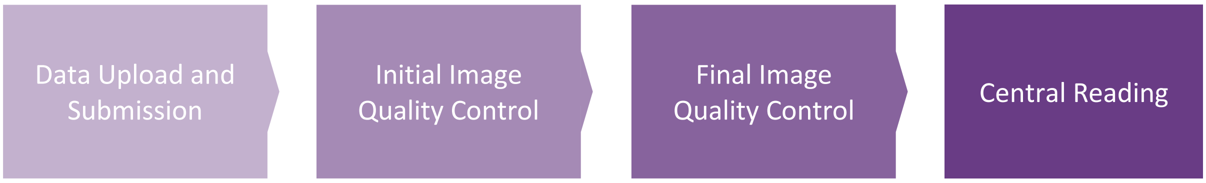
In addition to SliceVault's support for user authentication, Trial Administrators can grant workflow authorization and data access to specific users or user groups via a dedicated trial administrator web interface. This provides the fine-grain control Trial Administrators need to ensure that only authorized users have rights to particular data and workflows.

The SliceVault IDM platform has the following user roles with key restrictions as per the table below:

User role	Key restrictions
Investigator	Can upload, submit and edit all data from their user group
Investigator (locked)	Read only access to all data from their user group
Quality Control Manager 1	Access and edit submitted data from specified user groups
Quality Control Manager 2	Access and edit submitted data from specified user groups
Reader	Access and edit submitted data from specified user groups
Project Manager:	Read only access to submitted data from all user groups
Monitor	Read only access to submitted data from specified user groups
Trial Administrator	Manage users and user groups, no data access
API	Query (read-only) and retrieve data from specified user groups

Following the Windows principle of least privilege, SliceVault limits system vulnerability to security risks and exploits by ensuring that no users are granted more privileges than is actually required.

In addition to user role, access to data and functionality is further restricted by the data processing workflow, as depicted below:



Data Upload and Submission

Initial Image Quality Control

Final Image Quality Control

Central Reading

All imaging data is managed through the data processing workflow by permitted users. Permission, read-only and editor privileges are delegated to users depending on user roles and where data is located in the data processing workflow. For example, users with user-role Investigator enjoy editor privileges in the first step of the data processing workflow, but after submission to initial image quality control the user's privilege is changed to read-only.

DICOM De-identification

Following industry best-practices, the SliceVault IDM platform uses a standards-based approach to de-identification of DICOM images to ensure that images are free of PHI. The de-identification process is designed in accordance with the requirements set forth by the Federal Drug Administration (FDA) and the European Medicines Agency (EMA). The standard for de-identification of DICOM images (objects) is defined by the DICOM Standard: Digital Imaging and Communications in Medicine (DICOM), Part 15: Security and System Management Profiles.

PHI is defined as information that can be used to directly or indirectly identify an individual in relation to the individual's past, present or future health condition and the provision of health care to the individual. Common types of PHI include: patient name, address, birth date, social security number, medical and laboratory reports, physician name, hospital name and date of examination. PHI can be embedded in both DICOM tags and pixel data.

The process of de-identification, by which PHI is redacted or removed from the health information in the data uploaded to SliceVault, mitigates privacy risks to individuals and supports the use of data for scientific research. The de-identification process in SliceVault is an automated 3-step process, in which two de-identification methods are deployed sequentially: First redaction of individual PHI identifiers in DICOM tags and secondly redaction of PHI identifiers burned into the images by a qualified imaging expert. Both methods are executed locally prior to data transmission via secure communication to SliceVault's IDM platform.

Step 1: Automated redaction of individual PHI identifiers stored in DICOM tags is the first step in the de-identification process. The de-identification algorithm conforms to the current DICOM standard to ensure that data uploaded to and processed in SliceVault's IDM platform is transformed using approved redaction techniques such as data generalization by grouping of values into categories and data suppression/masking where specific values, or whole records are removed from the dataset.

Step 2: With SliceVault build in redaction technology, sensitive information burned into the medical images can be permanently removed from the data. Users can rely on the build-in optical character recognition algorithm to identify sensitive information or manually mask areas containing sensitive information.

Step 3: Images containing burned in annotations requires manual review and approval to be uploaded to SliceVault.

Audit Trails

Audit log files are recorded each day for all users, all user roles and for every step of the data processing workflow. Audit logs can be viewed by permitted users and the log viewer allows users to easily navigate through the history of change events

All audit log entries are assigned unique IDs, are locked for editing and are assigned the following attributes:

- Date and time for event
- User ID for the user authorizing the change event
- User group name
- Patient ID (when applicable)

- Visit ID (when applicable)
- Type of target ID
- Target ID
- Type of action
- Details describing the change event

The audit log includes the following change events:

- User authentication (successful login, failed login attempt, logout, session timeout)
- Change in user authorization (change in user role)
- Change in user credentials
- Data import (image ID, folder ID, visit ID, patient ID)
- DICOM de-identification and image redaction
- Change in image status and trial enrollment status
- Data download (image ID, folder ID, visit ID, patient ID)
- Data removal (image ID, folder ID, visit ID, patient ID, reason for removal)
- New queries, new query replies and change in query status
- Values in form fields, changes to values in form fields, change to form status and changes to form permission

The list is not exhaustive. Please contact SliceVault support at support@slicevault.com for more information about change events and audit logging.

Audit log files are securely stored as per FDA 21 CFR Part 11 requirements.

Service Delivery

State of the Art Data Centres

SliceVault has partnered with Microsoft to provide high availability, low latency, scalability, and the latest advancements in cloud infrastructure through the global Azure network. Certifications include ISO 9001, ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2 and physical security features includes a layered security model, including safeguards like electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, biometrics and 24/7 monitoring.

Encrypting Data in Transit, at Rest and on Backup Media

Data in transit requires constant protection to keep data secure, verify ownership and prevent attacks. SliceVault clients' data is encrypted when it is on a disk, stored on backup media, moving over the internet or traveling between data centers.

Low Latency and Highly Available Solution

Microsoft's highly redundant infrastructure also helps protect SliceVault's clients from data loss. Our recovery point objective (RPO) target is 24 hours and our recovery time objective (RTO) design target is also 24 hours. Incident response includes moving services to other Azure regions (in case of outage) and rapid DNS management (in case of denial-of-service attacks).

Our highly redundant design has allowed SliceVault to achieve an uptime of >99 % over the last year.

Web Application Firewall

All incoming traffic to SliceVault's IDM platform is routed through a Microsoft Azure Web Application Firewall to protect our SliceVault's web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.

Data Recovery

Standard Operating Procedures for Disaster Recovery details the policies and procedures of SliceVault in the event of a disruption to critical IT services or damage to IT equipment or data. These processes will ensure that those assets are recoverable to the right level and within the right timeframe to deliver a return to normal operations, with minimal impact on the business.

All data uploaded to the SliceVault IDM platform is backed up daily and stored on both primary and secondary backup locations.