| | | | |
|---|---|---|---|
| **Title** | V1.1 Aidoc Solution Security Overview | | |
| **Document number** | ID_V1.1 | **Document status** | Final |

| | |
|---|---|
| **Owner** | VP R&D |
| **Approver(s)** | CTO |

## Preface and document control

This document is intended to describe privacy and security principles and measures as implemented in the Aidoc Solution.



| **Revision History:** | | | |
|---|---|---|---|
| **Rev. #** | **Written by:** | **Description of Change** | **Date Signed** |
| 01 | Michael Braginsky | First issue. | 12-Jan-2019 |
| 1.1 | Mattan Shpaier | Revised Version | 01-Jun-2020 |

## 1 Table of Contents

## 2 Purpose

The purpose of this document is to describe Privacy and Security principals and measures implemented in the Aidoc Solution.

## 3 Scope

The measures described in this document are applicable for all versions of the Aidoc software from 2.0 and above.

## 4 System Architecture Overview

The Aidoc solution architecture contains three main components: Aidoc AI Orchestrator, Aidoc Analysis Service and the Aidoc Desktop Widget (“the client”).

**Aidoc AI Orchestrator**

The Aidoc AI Orchestrator is the central server of the system. It manages all integrations with customer systems and the workflow of AI analysis of cases. It is typically installed on a Virtual Machine in the customer’s environment. The Orchestrator is responsible for:

- Receiving DICOM files and HL7 messages from the different sources in the institution;
- Identifying the relevant data for each AI module out of the received information;
- De-identifying the data, uploading it and triggering the Aidoc Analysis Service to use the appropriate algorithm;
- Downloading AI analysis results from the Aidoc Analysis Service and re-identifying them;
- Distribution of AI analysis results to the Aidoc Widget and other pre-defined systems;

**Aidoc Analysis Service**

The Aidoc Analysis Service is a distributed, scalable cloud environment which includes all AI modules. The cloud machines which analyze the exams have designated hardware that allows minimal analysis turnaround times.

**Aidoc Desktop Widget**

The Aidoc Desktop Widget is a client that is installed on the workstations. It allows pushing notifications of urgent cases and presenting the key image of the finding in context with the opened exam. The Aidoc Desktop Widget is a lightweight software that is provided as an MSI, and can be pushed either manually using a local admin, or through the network. It communicates only with the Aidoc AI Orchestrator.

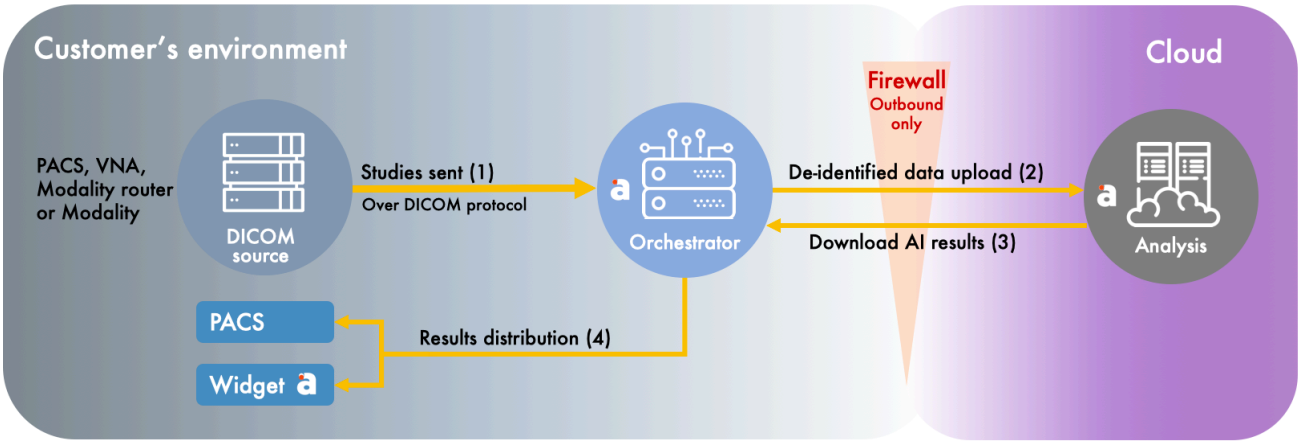


*Figure 1 - Architecture of the solution: relevant studies are routed or queried from the appropriate DICOM entity, sent to the Aidoc AI Orchestrator. The studies are de-identified and uploaded to the Aidoc Analysis server in the cloud, where the analysis is performed. Results are downloaded back to the Orchestrator, re-identified, and pushed to the widget, native worklist, reporting system, or PACS (as a separate new series in the study).*

## 5 Information Flow Overview

The high-level data flow is as follows:

- Studies are forwarded and/or queried from the PACS/VNA or sent directly from the modalities to the Aidoc AI Orchestrator.
- The Aidoc AI Orchestrator selects which exam to route to which AI modules, on an instance level, basing the decision on DICOM metadata and pixel data.
- The Aidoc AI Orchestrator  the data and sends it for analysis by the Aidoc Analysis Service.
- Every few seconds, the Aidoc AI Orchestrator polls the Aidoc Analysis Service for results, and when those are available, it downloads them.
- The Orchestrator re-identifies the results and distributes them to the different pre-defined destinations.

## 6 Security Features

The Aidoc solution is designed with built-in security and privacy features from the ground up, in order to comply with HIPAA and HITECH standards and with industry best practices, and provide maximal security to processed data.

Listed below are Aidoc's Privacy and Security principals:

**Physical Security**

Aidoc does not store or process any personal information on its premise. All information is stored and processed using Amazon Web Services / Google Cloud Platform / Microsoft Azure services. All 3 cloud providers are SOC 2 Type 2 and ISO27001 certified. These certificates cover physical security as well, ensuring the physical security of all data stored and processed by Aidoc

**Audit**

Audit logs on data access are maintained for 3 years. Aidoc cloud server audit logs are regularly reviewed by an authorized administrator and are maintained for analysis purposes should such need arise.

**Handling PHI**

Aidoc's main principal in treating with Protected Health Information (PHI) is that PHI never leaves the customer's environment.

Before DICOMs are being uploaded and sent for analysis, a new DICOM object is created and only non-PHI data is copied to it together with a new generated unique identifier. The identifier is used along the analysis process. Once the analysis result is fetched back to the customer's environment, the PHI is re-attached using this unique identifier, re-identifying the analysis results.

Other data types such as logging and analytics data are also de-identified before being sent to the cloud.

As part of the de-identification mechanism, PHI is encrypted at-rest while saved in the Aidoc AI Orchestrator's database.

**Encrypted Intercommunication**

All intercommunication between Aidoc system's components, such as communication between the Widget and Orchestrator, as well as Orchestrator and Aidoc Analysis Cloud, are encrypted using state-of-the-art transport layer encryption (TLS 1.2).

The degree of encryption is not configurable. All symmetric encryption is with AES-256 and all a-symmetric encryption is with RSA-2048 + SHA2.

**Outbound communication Only**

All communication between the Aidoc Orchestrator to the Aidoc Analysis Services is outbound-only and is always initiated from within the internal network outward.
In addition, there's two-way authentication between the Analysis Service and the Orchestrator.
Last, the firewall outbound rules are limited to allow communication to Aidoc Services only.

**User Authorization and Authentication**

The Aidoc AI solution comes with a built-in role-based access control mechanism. The Widget enforces this mechanism and requires authentication for all user functions.
Authentication can be done using Active Directory, 3rd party SSO (dedicated SSO solutions or through PACS, RIS or dictation software) or basic username-password credentials.
In addition, user connections have session timeouts and require re-authentication at the end of each session.

**Customer Data Separation**

Each customer is assigned a unique storage bucket, where only that specific customer data is stored. There is no sharing of production storage between Aidoc's customers.

**User Access Limitations**

Aidoc requests to allow its support team a remote access using a point-to-site / point-to-point VPN or any other equivalent software*. The remote access must be protected by Multi-Factor Authentication. For the cloud environment, Aidoc operation teams only access data through application interfaces and not directly, and VPCs of the environment are only accessible from Aidoc HQ.
* The installation process itself does not require a VPN access, and can be done by the customer or using a video call with a shared screen (the process takes 10-15 minutes).
All permission changes to Aidoc cloud are reviewed by a certified administrator and are properly audited.

**Cloud Protection**

Aidoc Analysis Service is a cloud service, deployed on a SOC2-compliant infrastructure and protected both by the cloud provider and Aidoc. The service is protected by Cloud built-in SIEM, Perimeter firewall and a Web Application Firewall.
In addition, mechanisms like Multi-Factor Authentication for all admin actions, WAF and anti-DDoS and Private access keys are deployed.
All uploaded (de-identified) data is encrypted at-rest immediately after it is uploaded.

**Vulnerability scans and penetration testing**

- Aidoc's cloud resources are scanned for vulnerabilities quarterly.

- Aidoc's solution is penetration-tested with consideration of OWASP principles quarterly.
- The application is penetration tested upon major changes.

**Business Continuity and Disaster Recovery**

In the cusomter's environment, Aidoc's solution relies on the customer's disaster recovery practices. In case of service outage for any reason, the Aidoc AI Orchestrator will process lost data by querying it from the PACS/VNA.

Aidoc cloud is hosted on AWS / Azure / GCP, all of which are SOC 2 Type 2 certified. Aidoc relies on said cloud providers with regards to power supply, property damage, water intrusion, and other types of potential physical disasters.

In general, the Aidoc solution does not provide any storage or data retention functions, so the business continuity of the cloud environment is expressed in a high availability cloud architecture.

In case of malfunction in the site hosting Aidoc cloud, a new cloud is instantiated in a different availability zone.

**Security Practices**

Aidoc maintains an Information Security Management System compliant with the ISO27001 standard, and is certified annually. The ISMS includes procedures and controls for:

- Management commitment.
- CISO organization
    - Requirement on training and qualification
    - Involvement in development processes
    - Resource planning and management to ensure sufficient security resources
- Identification of the needs and expectations of all stakeholders.
- Risk and Threat Analysis
    - At least annually for the entire organization.
    - As part of the development process, in every version.
- Development and Production environments separation
- Human Resources risk management and security.
    - Personnel training – initial and continuous.
    - Contractual secrecy obligation.
    - Management by the “least privileges” principle.
    - Disciplinary process.
- Secure programming.
- Change management.
- Patch and vulnerability management.
- Access Control including network access control.
    - Employing Firewalls and network access restrictions in conjunction with user access management.
    - Network resources are only available physically within Aidoc HQ or by secure connection using VPN.
- Compliance with relevant laws and regulations.
- Business continuity.
- Information Security Event Management.
- Encryption and key management.
- Individual accountability.
- Vendor and Supplier Risk Management and legal security and privacy agreements, including outsourcing of any IT work.
- Physical and Environmental Security.
- Data classification and handling.

- System Acquisition.
- Secure data disposal and media retirement