Frequently Asked Questions

Alcon

ORA SYSTEM™

with VerifEye™ + Technology

Customer Product Security Guide

Windows 10 (64-bit)

April 2022

Table of Contents

System Information

FAQ Overview

This document provides answers to common security questions related to the ORA SYSTEM™, AnalyzOR™ Technology app, and the cloud server. For general information, refer to the ORA SYSTEM user manual.

Terms

The following terms are used in this user guide or in the system:

- **App** – The online AnalyzOR Technology interface that facilitates communication between the cart and cloud
- **Cart** – The physical ORA SYSTEM device
- **Cloud** – The AnalyzOR Technology cloud server
- **System** – The app, cart, and cloud components working together to produce results as intended

Abbreviations and Acronyms

The following abbreviations and acronyms appear in this guide or in the application:

Term	Description
DNS	Domain name system
FAQ	Frequently asked questions
HIPAA	Health Insurance Portability and Accountability Act
HSDP	HealthSuite[1] Digital Platform
ID	Identification
ISO	International Organization for Standardization
IT	Information technology
SHA 2	Secure has algorithm 2
SQL	Structured query language
USB	Universal serial bus
XTEA	extended tiny encryption algorithm

[1] HealthSuite is a registered trademark of Koninklijke Philips N.V.

System Requirements

Local Network Requirements

The local network used to connect the cart or app requires the following features:

- DNS: home.wavetecvision.com (54.162.49.196 and 54.162.161.99)
- Protocol: HTTPS
- Ports: 53 (DNS) and 443 (HTTPS)

Cart Requirements

The cart requires Windows 10 or newer and an active connection to the app.

App Requirements

Operating System	Browser
Windows[1] 10 (or above)	*Google Chrome*[2] (version 67 or above) *Firefox*[3] (version 60 or above) *Microsoft Edge*[2] (version 17 or above)
macOS[4] (version 10 or above)	*Safari*[4] (version 11 or above)
iOS (version 12 or above)	*Safari* (version 11 or above)

[1] Microsoft Edge and Windows are trademarks of the Microsoft group of companies
[2] Trademarks are property of their respective owners.
[3] Firefox is a trademark of Mozilla Foundation.
[4] macOS and Safari are trademarks of Apple Inc.

Frequently Asked Questions

Confidentiality

Data Privacy

Does the system contain electronic protected health information (PHI)?

Yes. The cart and cloud contain patient first name, last name, date of birth, surgery date, gender, and surgical parameters.

Does the system contain electronic financial data or payment card industry (PCI) data?

No. The system does not contain financial data or statements or payment information.

Does the system print confidential data?

No. The app does not allow printing.

Does the app expose sensitive information in error messages?

No. If an invalid login information is provided, the resulting error message is written so that it cannot be determined which credential was incorrect.

Can support and maintenance personnel access patient data from the app?

No. Only authorized individuals may access patient data. Administrative users can be assigned different privilege levels, but they must go through access control procedures to obtain access.

System Access

Does the cart support remote access?

Yes. Authorized Alcon representatives may access the cart remotely with LogMeIn[1] Central for software updates, diagnostics, and troubleshooting. Access can be restricted upon request.

What network services are required for the device functionality?

TCP 443, TCP 80, and UDP 67 (DHCP)

Are there USB or other ports? Can they be disabled?

Yes. The cart includes USB, Ethernet, and HDMI ports. Access to USB ports is restricted to admin accounts and logically protected.

Encryption

Is data encrypted in transit?

Yes. Files are encrypted by XTEA. Communication with the system uses TLS 1.1 and TLS 1.2 over HTTPS, 128-bit SSL using Microsoft WCF Basic256 Algorithm suite with the following parameters:

- AES-256 for encryption
- SHA-256 for message digest
- RSA-OAEP-mgf1p for key wrapping

Is data encrypted at-rest?

Both. At-rest on the cart, data is encrypted using AES-256 encryption. In the cloud, data is stored in an MS SQL Server[2] database and password-protected.

Are user IDs stored in the cloud? Are passwords encrypted?

User IDs are stored in an encrypted database. Passwords are stored with a one-way hash (SHA-2).

[1] Trademarks are property of their respective owners.
[2] MS SQL Server is a trademark of the Microsoft group of companies.

Authentication and Authorization

Does the app require authentication?

Yes. The app requires a password.

Can user IDs be used to represent a group of people?

User IDs are intended to be used by a single person. Alcon strongly discourages sharing user IDs.

What are the user password conventions?

Passwords must adhere to the following conventions:

- Between 10 and 128 characters
- At least 3 out of the following 4 complexity rules:
  - At least 1 lowercase character (a to z)
  - At least 1 uppercase character (A to Z)
  - At least 1 digit (0 to 9)
  - At least 1 special character: `@ # $ % ^ & * ( ) _ + , . | ~ - = \ ` { } [ ] / “ : ; ‘ < > ! ?`
- No more than 2 identical characters in a row (for example, 111 is not permitted)

Are passwords entered in a non-displayed field?

Yes. Passwords characters are disguised by default. However, users can manually or temporarily view the characters.

Does the app maintain a history of used passwords?

Yes. The last 10 passwords cannot be reused.

Does the app support additional user authentication devices?

Two-factor authentication is available for the app. The cart only supports a username and password.

Is there a limit to invalid access attempts?

Yes. The maximum number of attempts is configurable from 5 to 10 by an administrator. After the limit is met, the user must wait 5 minutes before contacting an administrator to reset the password.

How often are users required to change their passwords?

App users must change their password every 30, 60, 90, or 120 days (defined by an administrator).

Does the app use security questions for identity verification?

Yes. The questions are chosen by the user for password resets and other account maintenance. All answers are stored in a hashed format in the cloud.

Does the app support Active Directory[1] integration?

No. There are no configurable local users on the system.

Are concurrent sessions allowed?

Only one session is allowed at a time for the same user.

How are user accounts managed?

Either Alcon-certified personnel or local Alcon-trained users manage other users through the app, including enabling or disabling accounts.

Are users logged off after a period of inactivity (timed out)?

The cart logs users out at the daily verification check unless it is not in surgery mode. The app logs users off after 1 hour of inactivity.

Does the cart use independent local user accounts?

No. All accounts are managed through the app.

[1] Active Directory is a trademark of the Microsoft group of companies.

Integrity

Monitoring

Are the security administration functions separate from other functions?

Yes. User access determines function availability and separate login credentials are required.

Can security administrators disable a user ID in real-time without deleting it from the system?

Yes. App users may be temporarily locked, deactivated, or removed from the system. In all cases, an audit trail is maintained.

Can security administrators define when to automatically disable inactive user accounts?

App administrators can define a password expiration period after which a user is no longer able to access the system. Alcon recommends practices review their user list periodically for inactive users.

Can system administrators monitor devices and account access by function?

Yes.

Can security administrators change access permission levels of specific users?

Yes. App administrators can elevate another user up to the administrator level.

Safeguards

Can users change data on the cart?

No. Users must make changes through the app.

Is access to functions without authorization or authentication allowed?

No. A valid user ID and password are required to access functions defined by the user account role.

Does the cart prevent a default user from modifying trusted certificates?

Yes. Certificates are protected through role-based access controls.

Does the app provide safeguards against a Trojan or spyware?

The app uses a browser on a local machine. Therefore, any safeguards against malicious programs must be installed and managed by the customer IT department.

What anti-virus or anti-malware products and vendors are supported?

F-Secure server security on cloud servers

Does the cart protect against unexpected network traffic (such as a firewall)?

The cart enables Windows firewall and supports the default rules. It also supports additional enhancement to the inbound rules to further secure the system from unauthorized access.

Event Log Management

Does the system provide logs for audit trails?

Yes. The app provides logs for successful and failed access attempts as well as user creation and maintenance activities.

What audit or logging capabilities are available for review?

The cart logs critical security events in audit logs. The logs include the following data:

- User activities or events
- Date stamp and access details of sensitive data (for example, PHI) and system resources
- Access to admin or privileged accounts
- Operating system security events

Are SAS70, SSAE 16, or SOC reports available?

Yes. SOC 2 Type II reports are available upon request with a non-disclosure agreement.

Does the cloud provider comply with ISO/IEC 27002?

Yes. The Philips[1] HSDP platform adheres to ISO 27002 guidance and is ISO 27001-certified (available upon request).

Does the cloud provider have periodic external vulnerability scans?

Yes. The cloud provider performs regular scans per its information security policies and procedures.

Does the cloud provider have independent security audits?

Yes. Audits are conducted annually. HSDP is compliant with HIPAA and SOC 2[2] Type II.

Availability

Data Availability and Storage

When is patient data available?

Patient data is available when user with an appropriate permission level selects a patient from the cart software.

How is data stored?

The cloud provider stores customer data on a central server but limits access to applicable practice and permission levels. There is also an SQL database locally on the cart.

Who is the cloud provider?

Philips HDSP

Where is the data center?

USA with geographic redundancy in encrypted form

[1] PHILIPS is a registered trademark of Koninklijke Philips N.V.
[2] SOC 2 is a trademark of the American Institute of Certified Public Accountants (AICPA).

Recovery

Is stored data backed up? If so, how often?

Cart data is backed up locally every time the user logs off. It also synchronizes with the cloud every 15 minutes (excluding surgery mode).

App data is backed up daily and the transaction log is backed up hourly.

Is backed up data encrypted?

Yes. AES-128 encryption is used.

How long are backups retained?

The cart retains backed up data for a minimum of 120 days. Customer data backups are retained for a minimum of 12 months.

Is backup media stored off-site?

Yes. It is stored in the cloud.

Can data be restored after a backup?

Yes. Data is restored through database synchronization.