RV 700 1.60.00
Security White Paper

Baxter is committed to protecting the security of our products and the data privacy of our customers. We strive to maintain and improve the security of our devices throughout the product lifecycle, including:

- Security by Design
- Security risk management
- Secure coding
- Security scanning and testing
- Responsible vulnerability disclosure processes
- Vulnerability and threat monitoring
- Security patch management
- Incident response
- Information sharing

Baxter maintains continued vigilance for cybersecurity threats and vulnerabilities affecting our products and services. We are dedicated to ensuring that our customers receive information related to these threats, vulnerabilities, and actions to maintain the integrity of our products and the protection of patient data. In order to fulfill these commitments, Baxter maintains a global Product Security program focused on designing security best practices into our products and maintaining secure operations throughout our product's lifecycle.

Effective security management is a shared responsibility. Our product literature and support teams provide recommended network settings and configurations to enable proper and secure connectivity. We advise customers to conduct a hazards analysis pursuant to ISO/IEC 80001 Application of Risk Management for IT-networks Incorporating Medical Devices prior to deployment in order to identify and remedy any interoperability issues.

If you would like to report a potential product related privacy or security issue (incident, breach or vulnerability), please contact Baxter - 4321 State Street Rd, PO Box 220 Skaneateles Falls, NY 13153-0220 or visit https://www.hillrom.com/en/responsible-disclosures/

The purpose of this document is to detail how Baxter security and privacy practices have been applied to the RV700, what you should know about maintaining security of this product and how we can partner with you to ensure security throughout this product's lifecycle.

Table of Contents

1 Product Description

RV 700

The Welch Allyn RetinaVue 700 Imager (RV700) is a high-resolution ophthalmic camera used to acquire, save and transmit digital images of the human eye. Anterior and posterior ocular structures such as the surface of the eye, cornea, and fundus including retina, macula and optic disc can be imaged. It is a prescription use only medical device.

2 Hardware Specifications

- RV 700 Display: LCD Touch Screen Monitor – 4.3 inch
- Micro USB Port
- Speaker
- Standard Capacity Rechargeable Lithium-Ion Battery: 7.2V / 3200 mAh
- High-Capacity Rechargeable Lithium-Ion Battery: 7.2V / 6400 mAh
- Wireless Connectivity - 2.4GHz/5GHz, 802.11a/b/g/n Wi-Fi module
- Camera: 2592 x 1944 pixels (5MP)
- AC Power Supply

3 Operating Systems

Texas Instruments: Linux Kernel 4.9.41

4 Third-party Software

Third-party components are included in the SBOM. SBOM will be provided to the customers on request.

5 Network Ports and Services

- RV 700 does not run any network service.
- RV 700 uses TLS 1.2 while communicating with RVN
- RV 700 uses SSH and SFTP while communicating with Azure – Fleet Management Server and Azure – BLOB Server
- RV 700 uses UDP while communicating with NTP Server
- All Communication are initiated by RV 700

6 Sensitive Data Transmitted

- Sensitive Patient Data is Transferred only between RVN and RV 700
- Customizable Patient Orders (such as First name, Last name, Date of Birth, Gender).
- Patient's Retinal Images
- Patient Exam Data

7 Sensitive Data Stored

- Customizable Patient Orders (such as First name, Last name, Date of Birth, Gender).
- Patient Exam Data
- Patient Retinal Images
- RV 700 configuration settings (including device Access Code).
- RV 700 Wireless configuration settings (including Access Point Passwords, Certificates for Communication and Encryption).

8 Network and Data Flow Diagram

RV 700 supports Wireless based TLS 1.2 communication with RVN. RV 700 uses SSH and SFTP while communicating with Azure – Fleet Management Server and Azure – BLOB Server. RV 700 uses UDP while communicating with NTP Server. All Communication are initiated by RV 700. The data transmitted includes the PHI described in the *Sensitive Data Transmitted* section 6.

8.1 Network Data flow

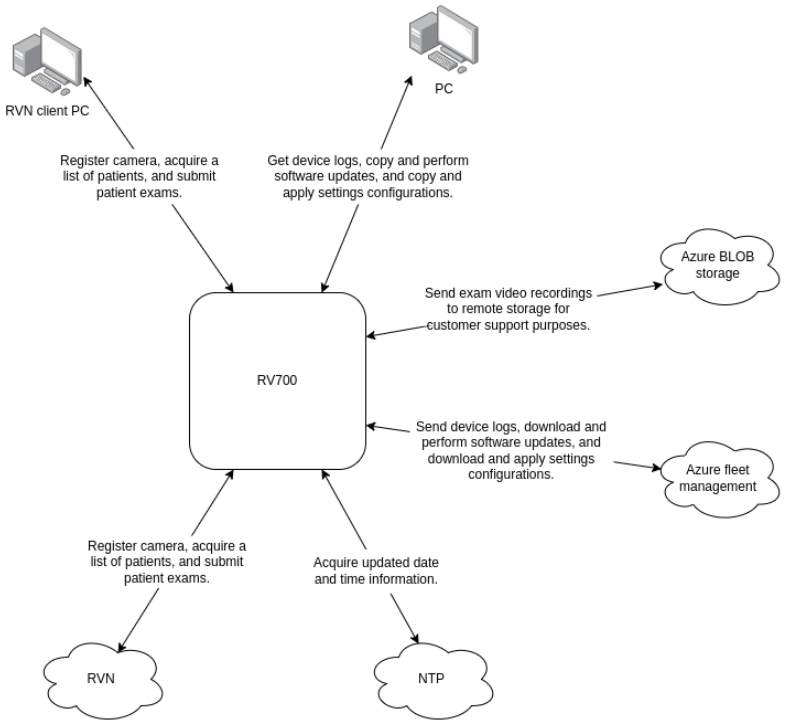

Figure 1- RV 700 Network and Data Flow diagram

8.2 Network Security

For Wireless Communication, RV 700 uses IEEE 802.11a/b/g/n, 2.4GHz/5GHz Wi-Fi compliant, provides the following authentication methods:

- IEEE 802.11 (WPA2 – Personal and Enterprise)

9 Malware Protection

RV 700 is an embedded device that does not allow user to install additional software.

10 Authentication Authorization

RV 700 does not support user-based access. Customer can set an Access Code to avoid unwanted access to the device.

11 Network Controls

Since RV 700 is an embedded device, user does not browse internet. RV 700 supports Wireless based TLS 1.2 communication with RVN. RV 700 uses SSH and SFTP while communicating with Azure – Fleet Management Server and Azure – BLOB Server. RV 700 uses UDP while communicating with NTP Server. All Communication are initiated by RV 700.

12 Encryption

12.1 File storage Encryption

RV 700 does not support Encryption at Rest. Device needs a proprietary cable and Password based login to access the data.

12.2 Communication Encryption

RVN: Patient Data is transferred in a TLS 1.2 tunnel with AES-256-CBC encryption and X.509 certificate-based mutual authentication of device (client) and server

RV 700 uses SSH and SFTP while communicating non patient data with Azure – Fleet Management Server and Azure – BLOB Server.

RV 700 uses UDP while communicating non patient data with NTP Server.

13 Audit Logging

RV 700 does not implement audit logs.

RV 700 provides basic logging mechanism intended for troubleshooting purposes. It shall log information about the following network communication in a log file:

- Configuration changes
- Connection success or failure
- Device Power ON
- Device Shut Down

14 Remote Connectivity

RV 700 does not support remote connectivity.

15 Service Handling

Service procedures are handled by the supplier. Please contact Baxter for more information.

16 End-of-Life and End-of-Support

RV 700 End-of-Life or End-of-Support dates are not established.

17 Secure Coding Standards

Baxter software development process incorporates secure development policies from IEC 62304.

18 System Hardening Standards

RV 700 does not use system hardening standards.

19 Risk Summary

A Software Risk Assessment was completed of the RV 700 product. Risks were assessed based on threat, impact and vulnerability. Vulnerability scanning were completed on the product; no critical vulnerabilities were identified. In addition, the RV 700 is enrolled in the Baxter's Security Vulnerability Management Process, which routinely monitors our applications for vulnerabilities.

Customer responsibilities were identified in the risk assessment, specifically:

- The device and IT Network the device is connected to should be securely configured and maintained per the IEC 80001 standard, or an equivalent network security standard or practice.
- Unauthorized connection to IT networks could result in previously unidentified risks to patients, operators, or third parties. The manufacturer is not liable for these additional risks, as the identification, analysis, evaluation, and control should be conducted by the responsible organization. Changes to the IT network could also introduce new risks that require additional analysis. This includes changes in network configuration, connection of additional items, disconnection of items, update of equipment, and upgrade of equipment.

20 Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and Baxter, or Baxter subsidiaries or affiliates (collectively, Baxter). Baxter does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.