SmartHub Connect & Orbit Cybersecurity White Paper

Security / Data Protection Concept
Belimed AG, Zug, Switzerland
July 2022

Belimed
Infection Control

Engineers of Confidence.

Content

1. Introduction

1.1. Why address cybersecurity

The topic of cybersecurity is becoming increasingly important in today's connected world. Many companies from different industries focus on integrating field devices like equipment or IoT devices into organization-wide information systems or making their devices available in a network-based environment. This trend can also be observed in the medical technology sector. Especially in this context, where secure operation of medical devices is crucial for the patient's, operator's or environment's safety, cybersecurity becomes essential.

This white paper highlights the importance of cybersecurity measures in the medical environment. It demonstrates Belimed's approach in its role as a manufacturer of medical devices and serves as a guide to mitigate potential threat scenarios associated with increasing digitalization and related networking.

Based on past experiences, it has been shown that most vulnerabilities do not arise in the medical device itself, but in the associated infrastructure or at the interfaces between the medical device and the IT network. Accordingly, cooperation between all those responsible for the various system levels is essential. It is especially important to sensitize all stakeholders about the risks and raise the awareness of potential cyber threats. All stakeholders such as the manufacturer, integrator or operator must play their part and contribute to a secure environment as a whole.

1.2. Cybersecurity handling

With the increasing importance of cybersecurity in the medical environment, various standards and guidelines have been introduced to help manufacturers develop their products according to the state of the art in cybersecurity and to help operators build the necessary infrastructure and operational processes. Belimed develops their devices according to the state of the art for product and software design and follows a risk-based approach to mitigate security risks. Relevant standards such as the IEC 62443[1]/EN IEC 82304-1[2] series of standards or BSI and NEMA guidelines are considered in Belimed's development process to ensure secure operation of the devices and services.

[1] IEC 62443: Security for Industrial Automation and Control Systems
[2] EN IEC 82304-1: Health Software – Part 1: General requirements for product safety

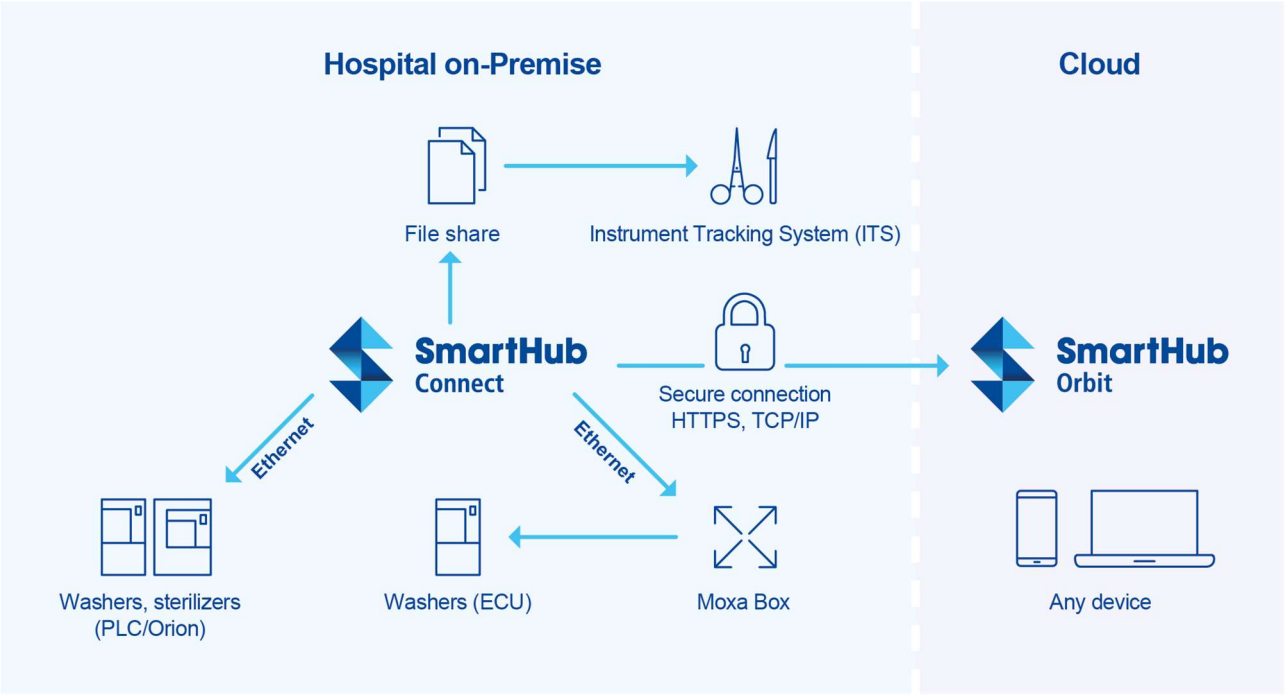
2. General information

This section provides information about the Belimed portfolio and its interfaces within the IT network. It also provides details on the threat analysis that was conducted to determine an appropriate security level and define measures to minimize cyber threats accordingly.

2.1. Elements of Belimed Connect

Belimed's digital portfolio consists of the following elements:

- **Belimed medical devices**
  - Medical device control system and user interface
    - ECU-based washer-disinfectors
    - PLC-based sterilizers and washer-disinfectors
    - ORION-based washer-disinfector WD 290 IQ
- **Belimed SmartHub Connect (on premise application)**
  - On-site server with SmartHub Connect software
  - Interface to the medical devices
    - ECU-based washer-disinfectors: serial device server (RS485/ethernet converter box)
    - PLC- and ORION-based washer-disinfectors and sterilizers: ethernet connection
  - Interface to the healthcare provider's IT network
- **Belimed SmartHub Orbit (cloud application)**
  - External cloud server platform
  - Data access for system diagnosis and predictive maintenance



2.1.1. Belimed washer-disinfectors and sterilizers

Intended use

Belimed washer-disinfectors and sterilizers are used to reprocess (washing, disinfecting and sterilizing) surgical instruments and accessories.

Security concept

A general disclosure for security measures applied to Belimed's medical devices incorporated in a medical IT network is stated in NEMA's MDS2 documents (Manufacturer Disclosure Statement for Medical Device Security).

Applicable standards

Belimed washer-disinfectors and sterilizers are considered as medical devices and fulfill the corresponding software requirements according to EN IEC 62304[3] for software as part of a medical device. In terms of cybersecurity, Belimed evaluates risks and measures based on a threat model and considers the IEC 62443[1] series of standards. A target security level SL-T 2 according to IEC 62443-4-2[4] and IEC 60601-4-5[5] is defined and measures are addressed to meet the requirements. For more details regarding the security level classification, refer to section 2.4.

2.1.2. SmartHub Connect

Intended use

SmartHub Connect is an on premise software application to gather machine data from the connected washer-disinfectors and sterilizers and to visualize the machine status on a dashboard. SmartHub Connect serves as an interface to the healthcare provider's instrument tracking system (ITS).

Security concept

The SmartHub Connect application is designed for secure and independent operation within the customer's IT network.

In terms of security and to minimize potential attack points, the following considerations were made:

- Network security: encrypted, unidirectional data flow from the customer's IT network to the external cloud.
- Privacy: only machine and batch data and no patient data is collected by SmartHub Connect (see also section 4).
- Data integrity: the data on the SmartHub Connect server reflects the machine data from the connected Belimed washer-disinfectors and sterilizers. The data cannot be altered on SmartHub Connect but is processed and distributed for further analysis and visualization.

[3] EN IEC 62304: Medical Device Software – Software Life Cycle Processes
[4] IEC 62443-4-2: Security for Industrial Automation and Control Systems – Part 4-2: Technical security requirements for IACS components
[5] IEC 60601-4-5: Medical electrical equipment – Part 4-5: Guidance and interpretation – Safety-related technical security specifications

- Access control: govern access to the various functions of the Belimed equipment with clear access control.
- Interfaces: SmartHub Connect offers safe and unambiguous interfaces to the healthcare provider's infrastructure

Applicable standards

The SmartHub Connect solution considers the respective legal and regulatory requirements. SmartHub is considered as software that is used in a healthcare environment and fulfills the corresponding software requirements in the style of EN IEC 82304-1[2] for standalone software or for software as part of a non-medical device in a healthcare environment. In terms of cybersecurity, Belimed evaluates risks and measures based on a threat model and considers the IEC 62443[1] series of standards. A target security level SL-T 2 according to IEC 62443-4-2[4] and IEC 60601-4-5[5] is defined and measures are implemented to meet the requirements. For more details regarding the security level classification, refer to section 2.4.

2.1.3. SmartHub Orbit

Intended use

SmartHub Orbit is a cloud application for advanced machine data analytics for remote diagnosis and predictive maintenance. Access to SmartHub Orbit is not limited to the healthcare provider's internal network, but is also external.

Security concept

The external cloud service is provided by Microsoft Azure. For this, the healthcare provider must allow the data transfer out of its internal network via an encrypted communication port.

In terms of security and to minimize potential attack points, the following considerations were made:

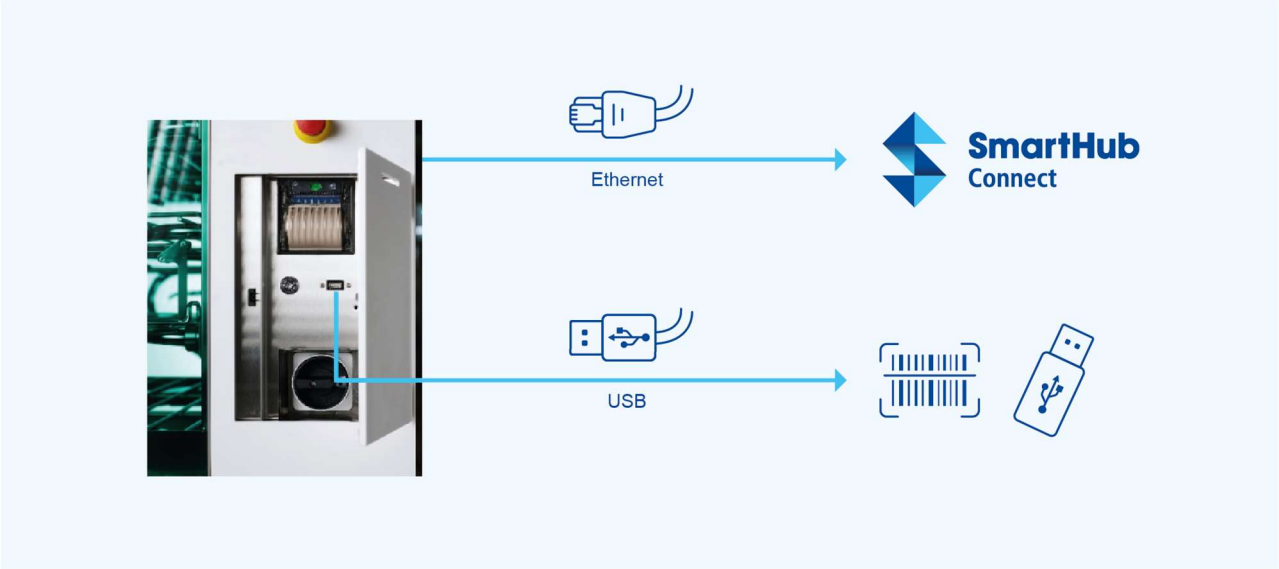
- Network security: encrypted, unidirectional data flow from the customer's IT network to the external cloud.
- Privacy: only machine and batch data and no patient data is sent to the cloud (see also section 4).
- Data integrity: the data in the cloud reflects the data that is handled on the main data processing center SmartHub Connect. The data is used for further analysis and visualization and cannot be altered in the local SmartHub Connect.
- Read only: data is only used for advanced analytics and visualization. No reversed remote access to the CSSD is possible to configure machine settings or change program parameters.
- Penetration tests: frequent tests are performed to identify new security vulnerabilities and to protect the application against intruders to the best of our knowledge and belief (see also section 3).

Applicable standards

The SmartHub Orbit solution considers the respective legal and regulatory requirements. SmartHub is considered as software that is used in a healthcare environment and fulfills corresponding software requirements in the style of EN IEC 82304-1[2] for standalone software or for software as part of a non-medical device in a healthcare environment.

2.2. Physical interfaces of Belimed devices

The following physical interfaces exist on Belimed devices. It must be noted that only devices (e.g. barcode readers) and auxiliaries that are sold by Belimed AG are allowed to be connected to the corresponding interfaces.



2.2.1. USB ports

The USB ports are for connecting printers or barcode scanners. They are also used to upload software updates or to export data by the healthcare provider or the service technician via a flash drive.

Protection of USB ports

- Access to the devices is spatially restricted and therefore only designated user groups (e.g. user, administrator, service technician) can access the USB ports.
- Every transaction is recorded.
- Software updates can be installed by personnel with administrator access rights only.

2.2.2. Interface to SmartHub Connect

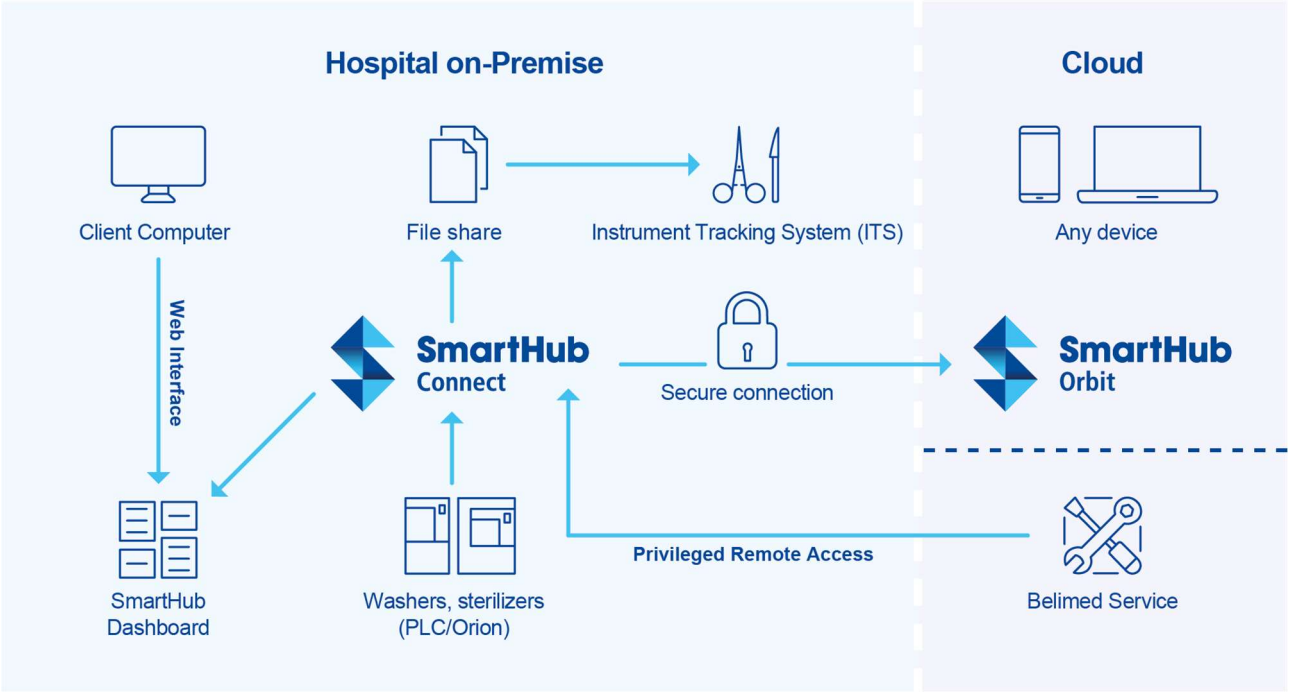
Belimed IQ devices, PLC-based medical sterilizers and washer-disinfectors can be connected directly to SmartHub Connect with a network cable. To connect washer-disinfectors with an ECU control system to SmartHub Connect, a serial device server must be interposed to convert the signal.

No wireless connection

The equipment intentionally does not offer a wireless interface (e.g. WI-FI) as wireless networks tend to be less stable in hospital environments than wired LAN. In addition, wireless networks are particularly unreliable in the subterranean floors, where Belimed equipment is frequently used.
Wireless interfaces also open up additional possible cyberattack vectors in a network environment.

2.3. Network interfaces of Belimed Connect & Orbit solutions

SmartHub Connect collects the machine data from the connected devices and acts as a gateway for further data distribution and processing. The SmartHub Connect and Orbit solutions are designed so that only a predefined subordinate system can be connected to it. The following interfaces are possible for further data analysis and visualization.



2.3.1. Client computers

Client computers can access the SmartHub Connect server via web interface to display the dashboard or to configure the SmartHub Connect settings. It is the responsibility of the healthcare provider to configure the internal network so that only the desired client computers have access to the server on which SmartHub Connect is installed and that the connection is encrypted.

2.3.2. Instrument tracking system

SmartHub Connect offers interfaces to various instrument tracking systems (ITS) in order to store CSV files with relevant batch data in the designated folder of the ITS. It is the healthcare provider's responsibility to ensure an encrypted connection.

2.3.3. Interface between SmartHub Connect and Orbit

The connection between SmartHub Connect and Orbit is encrypted and unidirectional from the customer's IT network to the external Microsoft Azure server. For this, the healthcare provider must allow the data transfer out of its network using the encrypted port 443.

2.3.4. Interface between SmartHub Orbit and Belimed Service

Belimed Service can access the machine and batch data on the SmartHub Orbit Cloud platform. It is important to note that the data available on SmartHub Orbit is a copy of the data collected on SmartHub Connect. Data transfer to the cloud is controlled exclusively by SmartHub Connect, and therefore no data transfer can be requested from outside without the healthcare provider's consent.

2.3.5. Privileged Remote Access

If Belimed Service requires external access to SmartHub Connect for troubleshooting or configuration, Belimed Service accesses the healthcare provider's network whenever possible via Privileged Remote Access (PRA) from *BeyondTrust*. This ensures that the user is authenticated before access, that the connection is approved by the healthcare provider and that the healthcare provider is notified when Belimed Service starts and stops access.

2.4. Threat analysis of the use environment of Belimed devices

In order to determine a reasonable set of security measures applicable to Belimed devices in a given use environment, an adequate target security level SL-T as specified in section 2.4.4 was assessed based on the following threat analysis.

2.4.1. Objects or processes that must be protected in the use environment

Object or process	Applicability	Comment
Patient data	No	Devices in the use environment do not generate any data that is linked to patient data, nor do they process such data.
Commercial data	No	The use environment does not have any connection to a hospital information system with commercially relevant data.
Operating data	Yes	Devices in the use environment generate data that is relevant for regulatory purposes or that provides information about the operation of the systems. This data might be transmitted to superordinate systems in real time or might be downloaded by division managers or service technicians with the appropriate access rights.
Integrity of the use environment	Yes	Integrity might be affected by DoS (denial of service) attacks, Trojans, other types of extortion.
Operation in the use environment	Yes	Operation might be affected by DoS (denial of service) attacks, Trojans, other types of extortion.

2.4.2. Possible attackers of the use environment

Attackers	Motivation	Likelihood	Comment
Activist	Ideological	Low	Not a controversial environment
Hacker	Amusement	Low	-
Hacker	Commercial	Low	Attacks on these networks do not have an immediate effect. Additionally, the core function of the devices is also possible completely separated from a network (offline).
Criminal	Commercial	Medium	Insertion of a Trojan is rather unlikely but may be interesting as a resource for further attacks
Competitors	Commercial	Low	-
Security researchers	Amusement/ commercial	Medium	Targeted test of the network. Motivated for official, professional or private reasons.
(Ex-) Employees	Malicious/ revenge	Low	-
System operators	Commercial	Low	Modification, use beyond the intended application
Foreign powers	Sabotage	Low	Malicious attacks

2.4.3. Possible risks for patients or users

Risk	Root cause	Evaluation
Reduced performance	Caused by corrupt software or data due to intentional manipulation of, for example, program parameters	Possible
Devices in the environment not functioning	Caused by corrupt software or data due to intentional manipulation of, for example, program parameters	Possible
Devices in the environment damaged	Caused by corrupt software or data due to intentional manipulation of, for example, program parameters	Unlikely
User injured	Caused by corrupt software or data due to intentional manipulation of, for example, program parameters Safety risks of the devices that can result in injury are mitigated with hardware control measures.	Unlikely

2.4.4. Definition of Security Levels according to IEC 62443-4-2[4]:

- SL 0: No specific requirements or security protection necessary
- SL 1: Protection against casual or coincidental violation
- SL 2: Protection against intentional violation using simple means with low resources, generic skills and low motivation
- SL 3: Protection against intentional violation using sophisticated means with moderate resources, medical IT-network specific skills and moderate motivation
- SL 4: Protection against intentional violation using sophisticated means with extended resources, medical IT-network specific skills and high motivation

2.4.5. Results

Potential attackers (activists, hackers, criminals, etc.) of the use environment where Belimed devices are installed and operated are in general assumed to be individuals with low resources, low motivation, generic skills and no particular knowledge of the infrastructure of the use environment. In view of the security levels defined in IEC 62443-4-2[4] and IEC 60601-4-5[5] and based on this threat analysis, a target security level SL-T of 2 is adequate for the present use environments.
In order to adequately protect the integrity and operation of the use environment, as well as the performance and function of devices in the use environment, Belimed determined appropriate measures in accordance with IEC 62443-4-2[4] to fulfill the requirements of a target security level SL-T of 2.

2.5. Delimitation of system and responsibility

Belimed assumes the following IT-infrastructure preconditions:

- Physical access to the equipment in a CSSD is restricted and governed by the strict access controls of the hospital.
- The IT network of the hospital is secure and the measures of the hospital IT department are effective and protect all devices connected to such network.
- Access to the SmartHub services within the IT network is clearly governed and only permitted for authorized personnel.
- Only dedicated communication ports are used to send machine and batch data from the healthcare provider's IT network to SmartHub Orbit.
- No personal or diagnosis data (especially patient data) is processed and stored within the SmartHub Connect and Orbit solution.

It must be noted that according to regulations (e.g. EN IEC 80001-1[6]), the operator of such equipment is responsible for safety and efficacy of the operation of such equipment. That includes data security, privacy and safety issues as well as privacy of user data.

[6] EN IEC 80001-1: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities

3. Penetration testing

By integrating SmartHub into the Cloud and making data available outside the healthcare provider's IT infrastructure, a secure application is essential to ensure secure operation of the service without adding vulnerabilities to the healthcare provider's IT network and data processing.
The functionality of SmartHub Orbit is constantly enhanced and new features are iteratively integrated. To identify possible vulnerabilities within the application at an early stage and to keep the application secure, penetration tests are performed by an external partner on a regular basis or when new features with a certain criticality level are implemented.

3.1. Scope of the penetration test

The scope of the penetration test includes the SmartHub Orbit web application and the network traffic from machines via SmartHub Connect to SmartHub Orbit.
The testing partner uses a standard user account and an administrator user account so that the test can be performed from the perspective of both an external attacker as well as an insider threat (e.g. hospital staff) that has been granted access to the web application.
The system is tested against various known attack vectors and general procedures for ethical hacking.

3.2. Results

The test results and potentially identified vulnerabilities are summarized in a Penetration Test Report by the testing partner and provided to Belimed. Each finding is classified based on its security impact and criticality and recommended mitigation actions are determined by the testing partner. Identified vulnerabilities are subsequently evaluated by Belimed and considered in the future development of the application.
Upon request, a certificate of the penetration tests can be provided to customers.

4. General Data Protection Regulation (GDPR)

The GDPR entered into force in May 2018 and has since become binding for all member states. The GDPR is only concerned with the processing of personally identifiable information (PII) and different measures are applicable based on the role of controller or processor.

4.1. Personally identifiable information (PII)

Patient data

No patient data is processed on Belimed devices and on SmartHub Connect & Orbit solutions.

Machine or batch data

Not considered as personally identifiable information.

Operator data

Generally, no operator data is sent from Belimed devices or rather the on-site gateway SmartHub Connect to SmartHub Orbit. If desired, the healthcare provider can make the operator's name visible in the batch reports. Although this type of data falls under personally identifiable information, operator data in this context is not considered critical or a special category of personal data.

4.2. Handling of personally identifiable information (PII)

Based on the assessment of personally identifiable information in section 4.1 and the present legislation, the only data relevant to Belimed and covered by the GDPR is operator data. Although the operator data is not considered a special category of personal data, Belimed acts as data processor in accordance with the GDPR. If such operator data is made accessible in SmartHub Orbit, Belimed fulfils its obligations as a data processor accordingly.

For scenarios such as service or maintenance activities where Belimed has access to the on-site Belimed devices or SmartHub Connect and eventually has insight into operator data, Belimed fulfils its obligations as medical device manufacturer in accordance with the MDR 2017/745/EU (Medical Device Regulation) and the GDPR is not applicable.

More details regarding data handling can be found in the data license agreement.

5. Security information & guidance

This section provides information about Belimed's security approach during the whole product life-cycle and indicates which security practices are targeted. Accordingly, it is stated which security principles are implemented by design (secure by design) and which responsibilities lie with the healthcare provider.

5.1. Defense in depth strategy

Belimed sustains a comprehensive defense-in-depth strategy in order to maintain a secure product life-cycle. The different segments are stated in the following section.

5.1.1. Specification of security requirements

Security capabilities required for appropriate protection of confidentiality, integrity and availability of data, function and services of the medical devices are identified based on security level SL-T 2 of IEC 62443-4-2[4].

5.1.2. Secure by design

Belimed ensures that its product portfolio is secure by design by following the regarding product life-cycle management standards. The embedded software for Belimed washer-disinfectors and sterilizers is developed according EN IEC 62304[3] and the standalone, non-medical software for Belimed SmartHub is developed inspired by EN IEC 82304-1[2]. Furthermore, Belimed aims to accomplish a security level SL-T 2 according to IEC 62443-4-2[4].

5.1.3. Secure implementation

Belimed aims to ensure secure implementation of product features according to the MDCG Guidance on Cybersecurity for medical devices and IEC 62443-4-2[4].

5.1.4. Security verification and validation testing

Security tests are scheduled for the system components and testing will be continuously improved. Identified gaps towards SL-T 2 according to IEC 62443-4-2[4] are included in a backlog list and addressed in the system development process.

5.1.5. Security guidelines

To keep up with the latest developments in cybersecurity, Belimed takes into account various guidelines, constantly reassesses potential cyber threats and adapts the necessary measures accordingly.

5.2. Management of security-related issues

Security-related issues occurring in the field are recorded in Belimed's CAPA tool and handled according to Belimed's corporate CAPA guidelines. Belimed maintains a quality management system (QMS) according to ISO 13485[7].

5.3. Security update management

Belimed ensures that security updates and security patches associated with the product are tested for regressions and made available to product users in a timely manner (service letters). For the IT infrastructure connected with the Belimed products, it is the operators' responsibility to keep the systems updated (e.g. Windows server for SmartHub).

5.4. Instructions for use

For instructions for use, please refer to the corresponding user manual of the specific device or software application.

[7] ISO 13485: Medical devices – Quality management systems – Requirements for regulatory purposes