1 Cyber security at seca

Safety and security are top priority in the development of medical devices - safety for patients, operators and third parties and security for the systems and the processed information, especially personal data. Medical devices are subjected to a legally required **risk analysis** in order to weigh up the benefits and harms of an application and to minimize risks as far as possible.

Nowadays, medical devices are increasingly used in a **networked IT infrastructure**. Patient data, control commands, warning messages and many other data are exchanged between devices and systems. This integration offers considerable added value for the use of medical devices. Data is available quickly, accurately and extensively where it is needed to help patients.

However, networking also has its downsides. The medical sector is now a **prime target for cyber criminals**. Data is stolen and sold on the black market, databases are encrypted for the purpose of blackmail. Far too often, medical providers have to limit their operations due to a cyber attack or close entire departments on short notice because the IT infrastructure has collapsed. This situation can jeopardize patient health due to delayed treatment, and likewise, targeted manipulation of individual patient data can pose a risk to health.

Therefore, the risk analysis for medical IT systems and integrated medical devices mentioned at the beginning must be extended to **cyber security**. This will highlight potential hazards with regard to the loss of data, its manipulation or unauthorized disclosure. In addition, compliance with **data protection** must be examined, i.e. the rights of a data owner to the integrity of his data and his right to information about the use of his personal data. A person's health data are generally considered to be particularly sensitive data.

2 Creating a security concept

The respective medical service provider is responsible for compliance with the legal and normative requirements regarding cyber security and data protection. The manufacturer of medical devices is obliged to design the medical devices in such a way that the operator can perform safe operation.

Safe operation includes the creation of a **security concept**. The following topics should be regulated in this:

- Threat analysis
- Risk-based approach to assessing the existing infrastructure (hardware, software, networks, personnel, organizational structure, processes)
- Sensitization of personnel to the topic of cyber security and implementation of appropriate training courses
- Learning from training and emergency situations
- Continuous improvement measures

The security concept should define cycles for the implementation of **regular measures**, such as:

- Installing the latest security updates on all devices and systems
- Checking log files for suspicious activities
- Operator retraining
- Emergency simulations

A security concept should also include **guidelines** that describe specific measures or behaviors, such as these:

- Password policy: What password requirements are used in the organization?
- Backup strategy
- Documentation of device and system configurations (for recovery in the case of an incident).
- Creation of an "emergency handbook", see section 5.

3 Integration into an IT network

Please note that the integration of medical devices that includes other equipment could result in previously unidentified risks to patients, operators or third parties. It is the responsibility of the network operator to assess these risks and to define and implement risk control measures. The standard IEC 80001-1:2010 provides guidance for the responsible organization to address these risks.

Please note in particular that subsequent changes to the IT network may introduce new risks and require a corresponding additional analysis is required. Changes to the IT network include:

- changes to the IT network configuration,
- connecting additional devices to the IT network
- disconnecting devices from the IT network
- upgrading devices connected to the IT network,
- upgrading devices connected to the IT network.

Details on the required IT network requirements and configuration instructions for the seca products can be found in the individual Product Cyber Security Sheets.

If applicable, the individual Product Cyber Security Sheets include a list of hazardous situations that arise when the IT network does not have the characteristics required to fulfill the purpose of connecting the medical device to the IT network. This can include aspects of effectiveness and data and system security as related to basic safety and essential performance.

4 Security recommendations for safe operation

In the case of cyber attacks, it is generally not a single device that is attacked, but a system. A single medical device can be the target of an attack, or it can be misused as a gateway, but in principle the entire system, a network or the entire IT infrastructure must always be examined for potential vulnerabilities when defending against cyber threats. In any case, the **device's own configuration options** should be examined first, along with the device functions that have an influence on the cyber security of the device.

In addition, particular consideration should be given to the **configuration of the integration** into a system. The first thing to determine here is which interfaces the device has and which are actively used. Interfaces that are not in use should be actively switched off or deactivated, if this is provided for in the respective device.

In addition to the configuration, the **daily operation** of the device also plays a decisive role. Employees who operate the medical device should be made aware of potential hazards. Behavior that contributes to the improvement of cyber security should be trained regularly. Here, the specific characteristics of each device should be addressed.

The functions that influence cyber security and the special features of each individual seca product are summarized in the respective "**Product Cyber Security Sheet**", which can be found in the appendix of this white paper.

5 Security recommendations for service operation

In addition to the normal operating mode, the service mode in particular should be subjected to more intensive consideration on the subject of cyber security. **Additional functions** of the device or system can often be used in service mode, and **access to sensitive data** is suddenly possible with special administrator or service rights.

After authentication as an administrator or service employee, special care should be taken to ensure the security of the system and the data stored in it.

seca devices and systems are configured in such a way that administrators and service staff have access to privileged functions, but no access to personal data of end users, patients or examinees.

After configuration or service work has been completed, logout should be performed as soon as possible. Under no circumstances should a device or system be left unattended when a person with extended rights is logged in.

Often, service mode also provides opportunities to test or improve the cyber security of the device. For example, reading log files on a regular basis can help detect irregularities or identify areas for improvement.

If remote maintenance of the device or system can be performed, i.e., access from another location, it must be ensured that the remote maintenance session may only be started after an explicit declaration of consent has been made on the device or system. This can be the clicking of a button, for example. Care must be taken to ensure that the remote maintenance session is ended as soon as possible after the work has been completed.

To ensure the confidentiality and integrity of the user data, seca uses only encrypted and secured remote maintenance connections.

If maintenance or remote maintenance is carried out, it must be ensured that the actual operation is not impaired in any way. For this purpose, it may be necessary to explicitly block the device or system in question from normal operation and, for example, to provide a replacement device.

If seca or third parties are commissioned to service the devices or system or have access to the data stored in the device or system, an operator contract must always be concluded which regulates exactly which activities may be carried out as part of the service and which data may be accessed and in what form.

6 Incident management

According to the *NIST Cybersecurity Framework* five basic cybersecurity activities exist: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**.

The **identification** of threats is usually performed during development of the devices and systems. The **protection** of these means implementation of appropriate safeguards in order to prohibit cyber security events.

Still, cyber security incidents can occur. It is crucial to implement methods and to establish processes that enable possibilities to **detect** ongoing cybersecurity incidents. Methods for detection can be either automatic, like generation of warning messages, or manually performed, like regular audit trail checks.

In an incident is detected, it is important to **respond** as soon as possible. Ideally, a response plan is in place that describes the exact actions to be taken to prevent or at least minimize the damage.

If damage has occurred, measures should be available to restore the device or system to its normal operating state as quickly as possible. Classic **recovery** measures include importing a backup or restoring a previously documented device configuration.

Damage events occur unplanned and usually lead to hectic operations. It is not uncommon for the damage to be exacerbated by hasty measures.

Therefore, when creating a cyber security concept, it is essential not only to plan how to avoid incidents of damage, but also which "detect, respond and recover" measures make sense. Responsibilities should be named and reporting chains defined in advance. The documentation of these measures, the "**emergency handbook**", should be quickly accessible to all relevant employees - not only stored electronically on a potentially vulnerable IT network, but also in printed form.

7 End-of-life management

When a product or system is decommissioned, it is particularly important to check what happens to the data on it. Personal data in particular must be handled sensitively for data protection reasons.

If there are retention obligations for the data stored on the device, it must be copied and backed up on a suitable medium.

If there is an obligation to delete the data, it must be deleted professionally. The seca devices and system offer corresponding functions for deleting the data.

Special attention must be paid to data stored on mobile data media (e.g. USB sticks). The data media can, for example, be professionally deleted and disposed of by specialized disposal service providers.

Proper deletion of devices and data media should also be carried out if they are passed on to third parties, for example for repair.

8 Further reading

Organization / Publisher	Publication
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Grundschutz-Kompendium (Edition 2022, German)

Organization / Publisher	Publication
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Cyber Security Requirements for Network-Connected Medical Devices
Bundesamt für Sicherheit in der Informationstechnik (BSI)	KRITIS-Sektor Gesundheit: Informationssicherheit in der stationären medizinischen Versorgung – Rahmenbedingungen, Status Quo, Handlungsfelder (German)
Deutsche Krankenhausgesellschaft e.V.	Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B2S, German)
U.S. National Institute of Standards and Technology (NIST)	Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1
European Union	General Data Protection Regulation (GDPR)
U.S. Department of Health & Human Services	Health Insurance Portability and Accountability Act

9 Contact

For further questions on cyber security or in a case of an incident please contact our regional subsidiary or service partner or the seca information security officer directly:

seca gmbh & co. kg
Information Security Officer
Medical Measuring Systems and Scales since 1840
Hammer Steindamm 3-25
22089 Hamburg
Germany
T +49 40 20 00 00 0
F +49 40 20 00 00 50
E information.security@seca.com
seca.com

10 Product Cyber Security Sheet for seca analytics 125

10.1 Product specific security recommendations for safe operation

10.1.1 Interfaces and connections

The seca analytics 125 support the following interfaces:

Interface	Communication partner	Relevant for cyber security	Possible threats	Recommended security measures
Encrypted WAN connection	▪ seca measuring devices	yes	Disclosure or manipulation of measurement data	Check configuration; check if the correct measurement devices are connected; The connection is secured by default; misconfiguration would be obvious.
Web interface	▪ Devices with web browser	yes	Disclosure or manipulation of measurement data	Check configuration; check if the correct user is logged in; the connection is secured by default; Misconfiguration would be obvious.
Integration interface (optional)	• EMR system	yes	Disclosure or manipulation of measurement data	Check configuration; set the security settings recommended by the EMR vendor.
Configuration and monitoring web interface	• Devices with web browser	yes	(internal use only)	(internal use only)

10.1.2 User accounts and authentication

User groups

The seca analytics 125 support two user groups and the corresponding rights:

User group	Authentication mechanism	Managed by	Rights	Functions relevant for cyber security
User	user name and password	Customer	Daily operation, perform measurements, analyse measurement results	• data communication with seca measuring devices
Administrator	user name and password	Customer	Administration of system settings and user accounts	• administration of user accounts • administration of system and interface settings

10.1.3 Authentication

In a typical use case, there are only two user accounts: The "user" supports a test person during the measurement on a device by and evaluates the measurement results. The 'Administrator' configures the connection to the seca measuring devices and manages user accounts.

Passwords of administrators and as well as users should comply with the password policy of their organization.

10.2 Device specific security recommendations for service operation

Since seca analytics 125 is a cloud solution, no service operation is available for the customer.

An additional administrator app enables the configuration of e.g. tenants and integrations. This is only accessible to seca employees.

Two-factor authentication is optionally available.

10.3 Relevant sections in the instructions for use

Several sections of the Instructions for Use of seca analytics 125 discuss topics that are relevant to cyber security. The following table provides a list of the relevant chapters with respective advice for secure use of the seca analytics 125:

Section	
6.3 Email receipt	It is important to configure the e-mail reception correctly. During operation of seca analytics 125 e-mails are sent that are relevant for information security.
6.4 Browser settings	Correct configuration of the browser can ensure proper operation of the seca analytics 125.
7. Using basic functions - Password	The section "Using basic functions" contains the following notes relevant to information security: • 7.1.1 Creating a password • 7.1.3 Changing a password • 7.1.4 Resetting a password Using a strong password is essential to avoid unauthorizes access.

Section	
7.1.9 Updating the software	It is highly recommended to always use the latest software. The corresponding section describes how the user learns that new software is available and how to update.
10. Troubleshooting	The "Troubleshooting" section contains important information on how to proceed if you suspect that information security has been compromised.
12. Compatible seca products	Safe operation can only be guaranteed if compatible seca products are connected to the seca analaytics 125.

11 Product Cyber Security Sheet for seca connect 103

11.1 Product specific security recommendations for safe operation

11.1.1 Interfaces and connections

The seca connect 103 supports the following interfaces:

Interface	Communication partner	Relevant for cyber security	Possible threats	Recommended security measures
Encrypted WAN connection	▪ seca measuring devices	yes	Disclosure or manipulation of measurement data	Check configuration; check if the correct measurement devices are connected; The connection is secured by default; misconfiguration would be obvious.
Web interface	▪ Devices with web browser	yes	Disclosure or manipulation of measurement data	Check configuration; check if the correct user is logged in; the connection is secured by default; Misconfiguration would be obvious.
Integration interface	• EMR system	yes	Disclosure or manipulation of measurement data	Check configuration; set the security settings recommended by the EMR vendor.

11.1.2 User accounts and authentication

User groups

The seca connect 103 supports three user groups and the corresponding rights:

User group	Authentication mechanism	Managed by	Rights	Functions relevant for cyber security

Admins	user name and password	Customer	• Create and delete users
			• Change user data:
			  • First name and last name
			  • Password
				• User management

User group	Authentication mechanism	Managed by	Rights	Functions relevant for cyber security
			• Tenants • Roles	

Tenants	user name and password	Customer	• Create and delete tenants
			• Edit tenants
			  • Change the name of the tenant
			  • Add or remove users
				• Administration of system and interface settings

Device	user name and password	Customer	• Change tenant to which a seca measuring device is assigned	• Administration of devices

11.1.3 Authentication

Typically, there is only one user account having all rights. The 'Administrator' configures the connection to the seca measuring devices and interfaces initially. Then, the software does not need ongoing maintzenance but runs as middleware in the backgroud.

Passwords of administrators and as well as users should comply with the password policy of their organization.

11.2 Device specific security recommendations for service operation

Since seca connect 103 is a middleware solution, no service operation is available for the end-user.

11.3 Relevant sections in the instructions for use

Several sections of the Instructions for Use of seca connect 103 discuss topics that are relevant to cyber security. The following table provides a list of the relevant chapters with respective advice for secure use of the seca connect 103:

Section	
5.4 Installing and configuring seca connect 103	It is important to configure the firewall and security settings of the operating system correctly
7.1 Primary functions	The section "Primary functions" contains the following notes relevant to information security: • Changing a password • Login and Logout

Section	
	Using a strong password is essential to avoid unauthorizes access.
7.3 Administering users	The section describes the creation of users and user role management. Using a strong password is essential to avoid unauthorizes access. Setting the correct roles is essential for authorized use of the software
7.6 Interface module: Updating the firmware	The section describes the update of measuring devices. It is important to keep firmware up-to-date to aplly latest security patches.
14. Troubleshooting	The "Troubleshooting" section contains important information on how to proceed if you suspect that information security has been compromised.
16. Compatible seca products	Safe operation can only be guaranteed if compatible seca products are connected to the seca conenct 103.