THE DENTAL SOLUTIONS COMPANY™

Sidexis 4

Data Protection and Product Security

White Paper

Contents

1 Introduction

This White Paper describes the technical aspects of Sidexis 4 with relevance for IT security, cybersecurity and data protection.

It is aimed primarily at those service and customer employees who are responsible for installation, configuration, maintenance and use. This document is also aimed at the IT personnel responsible for the installation, configuration, maintenance and use of the local computer networks (IT networks) for operating Sidexis 4. In addition, it applies to data protection officers as well as marketing and sales personnel involved in supporting the procurement process.

This White Paper on product security contains all required information on the following topics:

- Advisory notes as to how the requirements of the General Data Protection Regulation can be met.
- Information on the measures for IT security in Sidexis 4 and notes on integrating Sidexis 4 into secure IT networks.
- Support in the evaluation process for medical devices.
- Information for generic questionnaires.
- Forwarding of information to customer and service personnel.
- Secure installation, configuration, maintenance and operation of the medical device (this White Paper is not intended as a substitute for the installation manual or the instructions for use).

Purpose of the document

The IT security of medical devices is part of product security and an important aspect of functionality. It is absolutely necessary to ensure that medical devices are used securely and that the following requirements, among others, are met:

- Protection of personal data (confidentiality)
- Integrity of the medical device, in other words that it functions as intended
- Availability of the medical device
- Data and information security (cybersecurity) of the medical device, including the medical and clinical data, in a networked system environment
- Further IT security aspects over and above data security (non-repudiation)

To ensure product security, a medical device must be designed, tested and placed on the market in a precise manner. However, it must also be installed, configured, maintained and operated as intended. If only one of these aspects is not carried out correctly, this can impair product security and lead to potentially serious compliance consequences.

Data protection is closely related to product security. The “General Data Protection Regulation” of the European Union also lays down provisions for the protection of personal data for medical devices.

The purpose of this White Paper is to ensure that all persons and institutions responsible for installing, maintaining or operating a medical device as well as data protection officers and those responsible for operating the local computer networks (IT networks) have access to all the information they need to carry out their work properly:

- Additional information on the requirements of the “General Data Protection Regulation” and how the medical device helps operators to fulfill their obligations
- Additional information on the requirements of Regulation (EU) 2017/745 of April 5, 2017 on medical devices (MDR) with regard to IT security (cybersecurity) and important notes from the accompanying documentation to the MDR on IT security *Guidance on Cybersecurity for medical devices MDCG 2019-16*
- Information on all aspects with product security relevance in relation to customers and service employees
- Ensuring the availability of all required data and guidelines in preparation for secure installation, configuration, maintenance and use.

Please note that this White Paper is not intended as a substitute for the Sidexis 4 installation manual or the instructions for use. It merely serves to provide the necessary information in a consolidated and convenient format.

To avoid the need for individual customer consultation, the White Paper is designed to provide all information that may be required during the selection and procurement process for a medical device.

2 Data protection

ACCORDING TO THE "GENERAL DATA PROTECTION REGULATION" (GDPR) OF THE EUROPEAN UNION

The General Data Protection Regulation (GDPR) of the EU dated April 27, 2016, which entered into force on May 25, 2017, requires the person responsible for compliance with data protection law ("controller") to prevent unauthorized access to third-party personal data (such as patient data) that is transmitted to it or that it has itself created. The controller within the meaning of the GDPR may be either a natural or a legal person (for example a company).

This section gives a brief overview of certain key passages of the GDPR.

Cited passages of the GDPR are shown in "*italics*".

Data protection principles

The GDPR defines principles governing the extent to which personal data is to be collected or processed.

(Chapter II, Article 5)

1. Personal data shall be:

> *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*
>
> *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes … ('purpose limitation');*
>
> *c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');*
>
> *d) accurate and, where necessary, kept up to date … ('accuracy');*
>
> *(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed … ('storage limitation');*
>
> *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

Data protection for medical reasons

Medical data of any kind that relates to a natural person enjoys special protection under the GDPR. The following section describes the basis on which this type of data may be processed.

Chapter II, Article 9

1. *Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.*

2. *Paragraph 1 shall not apply if one of the following applies:*
   …
   (h) 'processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services …'

Duties of the controller in respect of data protection

In a dental practice, the data protection "controller" is often also the legal person that owns the practice. In a clinic, that can also be a group of persons. It is important to understand that the operator is fully responsible for implementing all measures to ensure compliance with the GDPR.

Chapter I, Article 4

> *'For the purposes of this Regulation:*
>
> *…*
>
> *7. 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data …'*

Chapter IV, Article 24

> *1. 'Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.'*

Note that the GDPR makes no distinction here between technical or organizational measures for data protection compliance. Indeed, technical measures will never be able to replace organizational measures in full.

Data protection officer

A dental practice or clinic always processes a large number of special categories of personal data for medical purposes. In this case, the processor and controller must nominate a dedicated data protection officer (Chapter IV, Article 37, 1.(c)).

Chapter IV, Article 37, 6.

The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

Tasks of the data protection officer (Chapter IV, Article 39)

1. The data protection officer shall have at least the following tasks:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation …;

(b) to monitor compliance with this Regulation … and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance …;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation … and to consult, where appropriate, with regard to any other matter.

3

Cybersecurity

Data and information security

ACCORDING TO REGULATION (EU) 2017/745 ON MEDICAL DEVICES (MDR) AND GUIDANCE ON CYBERSECURITY FOR MEDICAL DEVICES MDCG 2019-16 OF THE EUROPEAN UNION

Regulation (EU) 2017/745 on medical devices (MDR) dated April 5, 2017, which entered into force on May 25, 2017, requires manufacturers to set minimum requirements regarding the characteristics of IT networks and IT security measures, including protection against unauthorized access, necessary to run the software as intended.

This section gives a brief overview of certain key passages of the Guidance on Cybersecurity MDCG 2019-16 accompanying the MDR. For the German market, important definitions of the German Medical Devices Operator Ordinance (Medizinprodukte-Betreiberverordnung – MPBetreibV), such as the medical device safety officer, are explained.

Cited passages are shown in "*italics*".

Definitions according to Regulation (EU) 2017/745 (MDR)

Interoperability

(Chapter I, Article 2 Definitions, paragraph 26)
'interoperability' is the ability of two or more devices, including software, from the same manufacturer or from different manufacturers, to:
a) exchange information and use the information that has been exchanged for the correct execution of a specified function without changing the content of the data, and/or
b) communicate with each other, and/or
c) work together as intended.

Authorised representative

(Chapter I, Article 2 Definitions, paragraph 32)
'authorised representative' means any natural or legal person established within the Union who has received and accepted a written mandate from a manufacturer, located outside the Union, to act on the manufacturer's behalf in relation to specified tasks with regard to the latter's obligations under this Regulation

Importer

(Chapter I, Article 2 Definitions, paragraph 33)
'importer' means any natural or legal person established within the Union that places a device from a third country on the Union market

Distributor

(Chapter I, Article 2 Definitions, paragraph 34)
'distributor' means any natural or legal person in the supply chain, other than the manufacturer or the importer, that makes a device available on the market, up until the point of putting into service

Economic operator

(Chapter I, Article 2 Definitions, paragraph 35)
'economic operator' means a manufacturer, an authorised representative, an importer, a distributor or the person referred to in Article 22(1) and 22(3)

Post-market surveillance

(Chapter I, Article 2 Definitions, paragraph 60)
'post-market surveillance' means all activities carried out by manufacturers in cooperation with other economic operators to institute and keep up to date a

systematic procedure to proactively collect and review experience gained from devices they place on the market, make available on the market or put into service
for the purpose of identifying any need to immediately apply any necessary corrective or preventive actions

Incident

(Chapter I, Article 2 Definitions, paragraph 64)
'incident' means any malfunction or deterioration in the characteristics or performance of a device made available on the market, including use-error due to ergonomic features, as well as any inadequacy in the information supplied by the manufacturer and any undesirable side-effect

Field safety corrective action

(Chapter I, Article 2 Definitions, paragraph 68)
'field safety corrective action' means corrective action taken by a manufacturer for technical or medical reasons to prevent or reduce the risk of a serious incident in relation to a device made available on the market

Field safety notice

(Chapter I, Article 2 Definitions, paragraph 69)
'field safety notice' means a communication sent by a manufacturer to users or customers in relation to a field safety corrective action

Definitions according to MPBetriebV (only for Germany)

Activities in connection with the operation and use of medical devices

(Chapter 2 Definitions, paragraph 1)
Activities in connection with the operation and use of medical devices are in particular
1. installation,
2. provision,
3. maintenance,
4. refurbishment, and
5. safety-related and metrological checks.

Operator

(Chapter 2 Definitions, paragraph 2)
The operator of a medical device is any natural or legal person who is responsible for operating the healthcare facility in which the medical device is operated or used by the employees of that facility. By way of derogation from sentence 1, the operator of a medical product which is in the possession of a member of the medical and allied professions and which is brought into a healthcare facility for use by the latter is the respective member of the medical and allied professions. Any person who provides medical devices for use outside of healthcare facilities in his own business or his own facility or in the public realm is also deemed to be the operator of such medical devices.

User

(Chapter 2 Definitions, paragraph 3)
A user is any person who deploys a medical device within the scope of application of this Ordinance.

Healthcare facility

(Chapter 2 Definitions, paragraph 4)
A healthcare facility within the meaning of this Ordinance is any facility, body or institution, including rehabilitation and care facilities, in which medical devices are operated or used by medical staff, members of the care professions or other authorized persons within the scope of their profession.

Medical device safety officer

(Chapter 6 Medical device safety officer, paragraphs 1 to 4)
(1) Healthcare facilities regularly employing more than 20 people shall ensure that a competent and reliable person with medical, scientific, care, pharmaceutical or technical training is nominated as the medical device safety officer.
(2) The medical device safety officer, as the central point of reference in the healthcare facility, performs the following tasks for the operator:
1. acting as a contact person for authorities, manufacturers and sellers in connection with reports of risks associated with medical devices and during the implementation of field safety corrective actions and other requisite corrective measures,
2. coordinating internal processes of the healthcare facility in order to ensure compliance with the reporting and cooperation obligations of the users and operators, and
3. coordinating the implementation of the corrective measures and the field safety corrective actions at the healthcare facilities.

(3) The medical device safety officer shall not be hindered in fulfilling the assigned tasks according to paragraph 2 and shall not be disadvantaged as a result of fulfilling those tasks.
(4) The healthcare facility shall ensure that a functional e-mail address of the medical device safety officer is published on its website.

Definitions according to international standards

(ISO/TR 24971:2020-06 Medical devices - Guidance on the application of ISO 14971)

Security

"Security": a condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences, where hostile acts or influences could be intentional or unintentional.
Security as defined above includes cybersecurity and data and systems security.

Confidentiality of the data/of the system

"Confidentiality": property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
(Explanation from standard ISO/TR 24971:2020, Annex F)
In the instances, loss of confidentiality could be more important, because disclosure of personal health information can create a potential for blackmail.

Integrity of the data/of the system

"Integrity": property of accuracy and completeness.
(Explanation from standard ISO/TR 24971:2020, Annex F)
Loss of integrity could result in changes to a patient's medical record (e. g. changes in drug orders or medical data/images)

Availability of the data/of the system

"Availability": property of being accessible and usable upon demand by an authorized entity.
(Explanation from standard ISO/TR 24971:2020, Annex F)
Loss of availability of the medical device can result in delay of diagnosis or delay of treatment.

Principles of IT security (cybersecurity)

Regulation (EU) 2017/745 (MDR), including the accompanying documentation for cybersecurity MDCG 2019-16, defines principles governing the extent to which data and information security (cybersecurity) is to be considered for medical devices, including medical device software (MDSW).

Further supplementary principles are defined by national statutory requirements such as MPBetreibV (the German Medical Devices Operator Ordinance) but also by international standards such as ISO/TR 24971, among others.

What connection is there between a medical device and IT security measures?

It would be beyond the scope of this document to provide a full answer, but a brief summary is given here.

IT security measures are defined for a certain area of operation (*intended environment / intended operational environment of use*) of a medical device in order to mitigate and ideally eliminate the risks arising from data and information security for the medical device in a specific area of operation that could prevent the software from being used as intended and therefore also prevent the provision of key performance features of the medical device (intended use).

This is summarized in Regulation (EU) 2017/745 (MDR) as follows:

(Regulation (EU) 2017/745 (MDR), Annex I, Chapter II, paragraph 17.4)
Manufacturers shall set out minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

(Regulation (EU) 2017/745 (MDR), Annex I, Chapter III, paragraph 23.4, letter ab)
for devices that incorporate electronic programmable systems, including software, or software that are devices in themselves, minimum requirements concerning hardware, IT networks characteristics and IT security measures, including protection against unauthorised access, necessary to run the software as intended.

In addition, the accompanying documentation to the MDR, *MDCG 2019-16 Guidance on Cybersecurity for medical devices*, points out the need for cooperation between the various economic operators (see MDR definitions above) and technical operators (see accompanying documentation MDCG 2019-16, Chapter 2, paragraph 6 Joint Responsibility – Integrator-Operator-Users).

What specific security measures are to be expected for networked medical products?

The accompanying documentation to Regulation (EU) 2017/745 of the European Parliament and of the Council of April 5, 2017 *Guidance on Cybersecurity for medical devices MDCG 2019-16* issued by the Medical Device Coordination Group (MDCG) has been taken into consideration for the product security requirements relating to data and information security.

Sidexis 4 has already implemented risk measures for data and information security (cybersecurity), including certain measures for the secure use of Sidexis 4 in a networked operational environment (IT networks) as follows (list not exhaustive):

- Recommendations for a secure operational environment (Microsoft Windows): automatic logout, administration of user accounts, security updates, etc.
- Authentication and authorization of Sidexis 4 components
- System logs
- Management of security updates for Sidexis and operating system
- Anonymization of personal data
- Support for the encryption of patient data through third-party software (such as Microsoft Windows Bitlocker)
- Blocking (deactivation) of insecure system interfaces
- Verification of software integrity
- Authentication and authorization of system components and interfaces (nodes/adjacent systems)
- Monitoring of remote maintenance access
- Accompanying documentation for data protection and product security (this document)

(Guidance on Cybersecurity for medical devices MDCG 2019-16, Chapter 3, paragraph 3)
Security capabilities may be determined as suitable risk-control measures. The design and implementation of such capabilities need to comply with the state

of the art (see Annex I, sections 17.2 (MDR) or 1, 4, 16.2 (IVDR)) and cover a wide range of technical areas (see Table 3).

Table 3: Indicative list of security Capabilities for MD

Automatic Logoff
Audit Controls
Authorization
Configuration of Security Features
Cybersecurity Product Upgrades
Personal Data De-Identification
Data Backup and Disaster Recovery
Emergency Access
Personal Data Integrity and Authenticity
Malware Detection / Protection
Node Authentication
Person Authentication
Physical Locks
System and OS Hardening
Security and Privacy Guides
Personal Data Storage Confidentiality
Transmission Confidentiality
Transmission Integrity

For further information about the cybersecurity risk measures *by design* in Sidexis 4, please refer to *Strategies and proven methods* and *System information.*

Apart from the security measures *by design*, what other security measures need to be taken into consideration for cybersecurity?

In addition to the requirements for data and information security *by design,* which include for example the authentication of communication between the Sidexis client and the Sidexis server, there are further IT security requirements that fall outside the scope of the Sidexis 4 product and therefore outside the area of responsibility of Dentsply Sirona - SIRONA Dental Systems GmbH, referred to in the following as the manufacturer. These include for example the confidentiality and integrity of data transmission in the local computer networks of the establishment.

Requirements also arise in this regard for all economic operators (authorized representatives, importers, distributors) within the meaning of Regulation

(EU) 2017/745 but also within the framework of the German MPBetreibV (user, operator, healthcare facility, medical device safety officer) as set out in the following paragraph *Duties of those responsible*.

See examples for the configuration of a local computer network (IT network) in *Overview of the system environment: IT networks, network zones and secure communication links (conduits)*.

Alongside the technical measures, organizational measures for data and information security (cybersecurity) are also required. These include for example reciprocal communication between the operator and the manufacturer to clarify a cybersecurity incident and to jointly define a field safety corrective action (see definition in the paragraph *Definitions according to Regulation (EU) 2017/745 (MDR)* above).

To ensure the successful and secure integration of Sidexis 4 into the intended environment, all parties involved, as described in *Definitions according to Regulation (EU) 2017/745 (MDR) and MPBetreibV*, must work together in a coordinated manner.

Duties of those responsible for IT security (cybersecurity)

Responsibility for data and information security (cybersecurity) is divided between several operators and roles responsible for ensuring compliance with the cybersecurity requirements laid down by laws and standards (industry best practices).

I. Operators and duties from Regulation (EU) 2017/745 MDR:
   a. The **manufacturer** will consider the data and information security (cybersecurity) requirements from the development of the medical device and throughout the entire product lifecycle.
      The risk management process is applied to the risks pertaining to patient safety and privacy as well as to the risks pertaining to data and information security (cybersecurity), as recommended by the harmonized standard for risk management of medical devices (*ISO14971:2019 Medical devices — Application of risk management to medical devices*) and the accompanying documentation MDCG 2019-16 to *Regulation (EU) 2017/745 (MDR)* for cybersecurity.
   b. **Importers**

(Article 13 General obligations of importers, paragraph 8) Importers who have received complaints or reports from healthcare professionals, patients or users about suspected incidents related to a device which they have placed on the market shall immediately forward this information to the manufacturer and its authorised representative.

c. Distributors
(Article 14 General obligations of distributors, paragraph 5) Distributors that have received complaints or reports from healthcare professionals, patients or users about suspected incidents related to a device they have made available, shall immediately forward this information to the manufacturer and, where applicable, the manufacturer's authorised representative. They shall keep a register of complaints, of non-conforming devices and of recalls and withdrawals, and keep the manufacturer and, where available, the authorised representative and the importer informed of such monitoring and provide them with any information upon their request.

For importers and distributors, the provision of information about suspected incidents (patient safety including cybersecurity) relating to Sidexis 4 and its system environment (*intended environment*) to the manufacturer is mandatory in order to enable the manufacturer to fulfill its obligations to monitor and report incidents on the market for Sidexis 4.

II. Operators and duties from MPBetreibV:

a. All operators and roles (user, operator, healthcare facility, medical device safety officer) as defined by the Ordinance contribute to the fulfillment of the security requirements (measures for patient safety including cybersecurity). See the paragraph *Definitions according to MPBetreibV (only for Germany)* above for further information.

b. Monitoring of the operational environment for connected medical devices and reporting of incidents to the manufacturer
(Chapter 4 General requirements, paragraph 4) Interconnected medical devices and medical devices connected to accessories including software or to other objects may be operated and used only if they are suitable for use in this combination, taking into consideration the intended purpose and the safety of patients, users, employees or third

parties.

The operational environment includes the local computer networks (IT networks) and is referred to as the *intended operational environment of use* in the accompanying documentation MDCG 2019-16 to *Regulation 2017/745 (MDR)* for cybersecurity.

c. The proper use of Sidexis 4 as a medical device, including the secure and interoperable use of the operational IT networks (see definition of *interoperability* in the paragraph *Definitions according to Regulation (EU) 2017/745 (MDR)*), falls within the area of responsibility of the operator.

(Chapter 3 Obligations of the operator, paragraph 1)
The operator shall fulfill the obligations incumbent upon it according to this Ordinance in order to ensure the secure, proper use of the medical devices used to treat the patient in its healthcare facility.

d. The manufacturer always recommends that the operator nominate a medical device safety officer, although this role is not mandatory for healthcare facilities with fewer than 20 employees.
(Chapter 6, Medical device safety officer). See definitions and obligations in *Definitions according to MPBetreibV* above.

e. For Sidexis 4 and the connected systems for diagnostics using imaging methods, the operator must maintain a medical device log, in which details of incidents relating to patient safety, including cybersecurity, must be logged.

(Section 12 Medical device log, paragraph 1)
The operator shall maintain a medical device log in accordance with paragraph 2 for the medical devices listed in Annexes 1 and 2.

(Section 12 Medical device log, paragraph 2, item 6)
The following details pertaining to the respective medical device shall be entered in the medical device log, which may be maintained on all kinds of data media:
(6) Details of incident reports to authorities and manufacturer.

III. Operators and obligations from international standards and industry best practices for data and information security (cybersecurity):

As already indicated, the monitoring of the operational environment by the operator includes the local computer networks (IT networks). Even if the application of the international standard *IEC 80001-1:2021* is not mandatory, it is expedient for you as the operator to define risk management processes for data and information security risks arising from the integration of Sidexis 4 into your operational computer networks (IT networks).

It is recommended that the operator nominate an officer with responsibility for applying risk management to the operator’s IT networks. For this purpose the *IEC 80001-1:2021* standard defines the role of medical IT risk manager, who could assume responsibility for all tasks relating to data and information security compliance for connected medical devices such as Sidexis 4 in the operator's organization.

The *medical IT risk manager* must work with the medical device safety officer (see definition above in the paragraph *Definitions according to MPBetreibV)* to monitor potential cybersecurity risks in the operational environment, report incidents, and implement safety corrective actions.

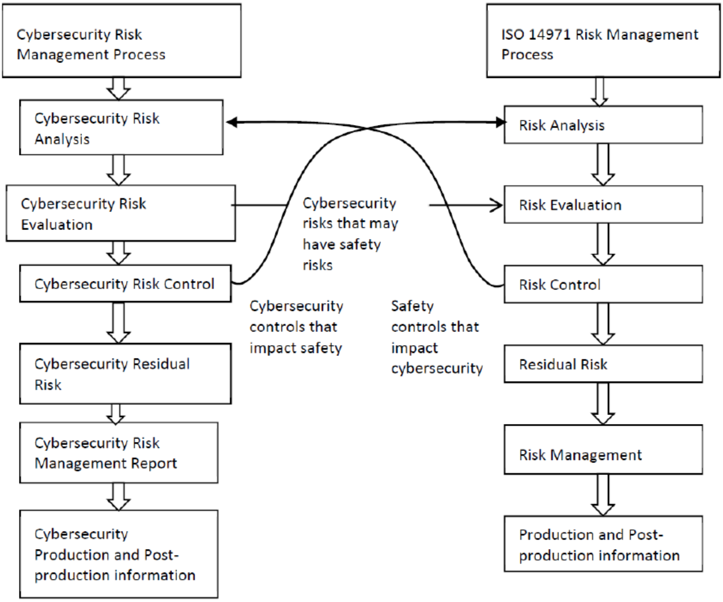
(*IEC 80001-1:2021 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management)*

Market monitoring of product security: reporting security incidents (post-market surveillance)

As already indicated, the risks arising from data and information security (cybersecurity) for medical devices, including software as a medical device, must be handled in the same way as patient safety risks in accordance with ISO 14971.

The cybersecurity risks for Sidexis 4 are monitored continuously by the risk management process for Sidexis 4 and are thus integrated into the risk management plan and the risk management file.

The monitoring of cybersecurity risks and the assessment of these risks with regard to their potential impact on patient safety takes place throughout the entire product lifecycle as recommended in MDCG 2019-16 issued by the Medical Device Coordination Group (MDCG) to accompany the MDR.


Cybersecurity Risk Management Process
Cybersecurity Risk Analysis
Cybersecurity Risk Evaluation
Cybersecurity Risk Control
Cybersecurity Residual Risk
Cybersecurity Risk Management Report
Cybersecurity Production and Post-production information
ISO 14971 Risk Management Process
Risk Analysis
Risk Evaluation
Risk Control
Residual Risk
Risk Management
Production and Post-production information
Cybersecurity risks that may have safety risks
Cybersecurity controls that impact safety
Safety controls that impact cybersecurity

Source: MDCG 2019-16 Guidance on Cybersecurity for medical devices, MDCG 2019-16, December 2019, Annex IV – Cybersecurity risk management process and safety risk management relationship.

Together with the manufacturer, all economic operators (operators, distributors and importers) also have an obligation to monitor cybersecurity incidents/vulnerabilities as part of their business processes for post-market surveillance and security incident management.

Alongside the sector-specific databases, other useful sources of information for security incidents are the national *Computer Emergency Response Teams (CERT)* such as CERT Germany https://www.cert-bund.de and CERT European Union https://cert.europa.eu.

Medical device safety officer

See definition in *Definitions according to MPBetreibV (only for Germany)*

Medical IT risk manager

See definition in *Duties of those responsible for IT security (cybersecurity)*

Contact details for queries regarding data protection and cybersecurity

In the first instance, contact

- the data protection officer or
- the medical device safety officer or
- the data and information security (cybersecurity) officer or medical IT risk manager

within your own organization to obtain as rapid a response as possible to your query.

Alternatively, you can also reach us online using our contact form: https://siroforcemobile.dentsplysirona.com

4 Strategies and proven methods

FOR DATA PROTECTION AND DATA/INFORMATION SECURITY (CYBERSECURITY)

This section contains information about proven methods for organizational and technical measures and shows how Sidexis 4 can support you in matters of data protection and IT security (cybersecurity).

Data protection: Patient consent

From a legal perspective, it is safest not to process personal data until patient consent has been granted. The GDPR defines certain rules governing how this consent is to be obtained.

(Chapter II, Articles 7 and 8)

- *Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.*
- *… the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form.*
- *The data subject shall have the right to withdraw his or her consent at any time. … It shall be as easy to withdraw as to give consent.*
- *Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

Data protection: Security of processing (Chapter IV, Article 32)

(Chapter IV, Article 32)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk …

Anonymization

- Anonymize the registered patient data in Sidexis 4 by setting the display so that only the patient’s card index number is shown on the upper left edge of the screen.
- Anonymize the patient data for DICOM exports (media without patient information) from Sidexis 4 in order to share it with other dentists from another legal unit (for example another practice) → For this purpose, it is preferable to use the DICOM export only on an encrypted data medium if it is neither possible nor desirable to anonymize the data.
- Sidexis 4 also allows you to print out the patient data without patient information using the *Ausdruck anonymisieren* (Anonymize printout) function.

Organizational measures

- Define conduct guidelines regarding data protection in the corresponding dental practice.
- Check your obligations with regard to data and information security (cybersecurity), particularly the potential need for a *medical device safety officer* and/or a *medical IT risk manager*. See *Duties of those responsible for IT security (cybersecurity)* above.
- Draw up an information security policy.
- Define access guidelines, including the logging of groups of persons and the associated roles for your own employees and, where applicable, the employees of your external IT business partner who are involved in defining and/or implementing the features of your IT networks and IT security measures, such as protection against unauthorized local or remote access.
- Train your practice staff to implement the conduct guidelines for data protection and cybersecurity.
  - Store a copy of each training course for your employees.
  - Select only properly trained staff to process personal data and IT infrastructure, including cybersecurity issues (based on their expertise and reliability).
  - Employees involved in processing personal data should have a permanent contract of employment

- Document the processing workflows in your practice.

(Chapter IV, Article 30)

> *1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:*
>
> > *a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;*
> >
> > *b) the purposes of the processing;*
> >
> > *c) a description of the categories of data subjects and of the categories of personal data;*
> >
> > *d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;*
> >
> > *e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;*
> >
> > *f) where possible, the envisaged time limits for erasure of the different categories of data;*
> >
> > *(g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).*
>
> *2. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:*
>
> > *a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where*

applicable, of the controller's or the processor's representative, and the data protection officer;

b) the categories of processing carried out on behalf of each controller;

c) where applicable, transfers of personal data to a third country or an international organisation …

d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

(3) The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.

(4) The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

(Accompanying documentation on cybersecurity to Regulation (EU) 2017/745 (MDR), MDCG 2019-16 Guidance on Cybersecurity for medical devices)

Important patient rights

Patients have a number of additional rights pertaining to the handling of their personal data:

- *Right to erasure ('right to be forgotten' (Chapter III, Article 17)*

  The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ...

  - Sidexis 4 supports the erasure of personal data as of Sidexis 4 V4.3.
  - Caution: The right to erasure does not overrule the national guidelines on the retention of X-ray images.

- *Right to data portability (Chapter III, Article 20)*

  The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided ...

  - Sidexis 4 enables personal data to be exported in standardized formats (e.g. DICOM).

- *Right to object (Chapter III, Article 21)*

  The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her ...

  - Caution: The right to object does not overrule the national guidelines on the retention of X-ray images.

Sensitive data

- Sidexis 4 processes personal data of patients in accordance with the (EU) General Data Protection Regulation. This includes:
  - Name
  - Date of birth
  - Card index no. For reasons of data protection, we recommend that you do not enter any sickness insurance or social insurance number here.
  - Photo of the patient
  - X-ray images and 3D volumes
  - Intraoral photos
  - Diagnostic findings and therapeutic information
  - (Social) insurance number
- Media can be anonymized for export.
- Sidexis 4 can be configured such that no personal patient data is displayed. The only exception is the card index number, which is essential in order to be able to identify the patient.

Adding information and comments to free text fields

Free text fields or comment fields are provided to allow users to describe things in their own words. Entries should be neutral and factual.

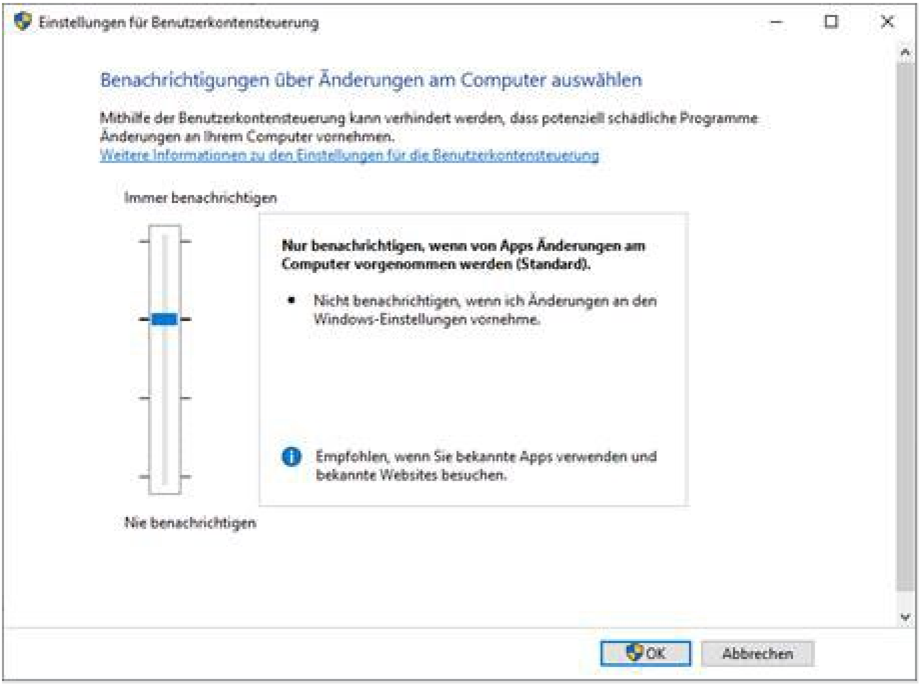
Please do not use these free text fields and comment fields to add personal, patient or health data such as the patient’s name.

Cybersecurity: User access controls. Authentication / user access authorization

Sidexis 4 uses security measures to protect against unauthorized access to the system and data. The existing user access control mechanism of your operating system (Microsoft Windows) enables privileges to be granted on a restricted basis for carrying out certain operations, such accessing the database.

Windows User Account Control (UAC) can be used to prevent potentially malicious programs from making changes to your computer.

Set User Account Control (UAC) to at least level 3 on each Windows workstation; this is the default setting in Windows: "Notify me only when apps try to make changes to my computer (default)".



Benachrichtigungen über Änderungen am Computer auswählen

Mithilfe der Benutzerkontensteuerung kann verhindert werden, dass potenziell schädliche Programme Änderungen an Ihrem Computer vornehmen.
Weitere Informationen zu den Einstellungen für die Benutzerkontensteuerung

Immer benachrichtigen

Nur benachrichtigen, wenn von Apps Änderungen am Computer vorgenommen werden (Standard).

- Nicht benachrichtigen, wenn ich Änderungen an den Windows-Einstellungen vornehme.

Empfohlen, wenn Sie bekannte Apps verwenden und bekannte Websites besuchen.

Nie benachrichtigen

Limit access to the Sidexis 4 server and to the workstations as far as possible:

- Only system administrators (Microsoft Windows) should have access to the server.
- Define strict password guidelines for defining secure passwords with regard to length, use of special characters, and the frequency with which passwords must be changed, and apply these to every user account set up on your operating system (Microsoft Windows) that is to use Sidexis 4. Multiple use of Sidexis 4 on a workstation by several logins to the same workstation is prohibited.
- Lock the workstation as soon as you no longer need to use it. To do so, use the functions provided by your operating system (Microsoft

Windows), such as automatic screen lock after a defined time. Instruct all users on how to leave their workstations in a secure state.

To install Sidexis 4, an administrator user account is required in your operating system (Microsoft Windows).

The Sidexis 4 installation program (setup) creates a user without administration rights for the Sidexis 4 server. This user (Sidexis4Service) is provided for starting the Sidexis 4 server service, for performing database backups, and for access (including by service engineers) to the protected data area SECURE MEDIA SHARE (PDATASEC).

Sidexis 4 requires authentication by password entry or certificate-based authentication for the following workflows:

- Access to critical functions or protected settings in the user interface
- Communication capability between Sidexis client and Sidexis server
- Performing operations on Sidexis databases

The following user-specific passwords must be assigned when Sidexis 4 is first installed or when it is updated:

- SQL SA password: Password for the service administrator of the Sidexis SQL database instance
- Sidexis 4 Service (Sidexis4Service) password: Password for the Windows user “Sidexis4Service” of the Sidexis 4 service (server) and MEDIA SHARES (PDATA and PDATASEC)
- Sidexis 4 Admin (S4Admin) password: Password for admin users in Sidexis 4 for accessing protected settings and sensitive functions (such as “Medien verschieben” (Move media) or “Patient löschen” (Delete patient)) of Sidexis 4

During operation, we recommend changing the passwords at regular intervals.

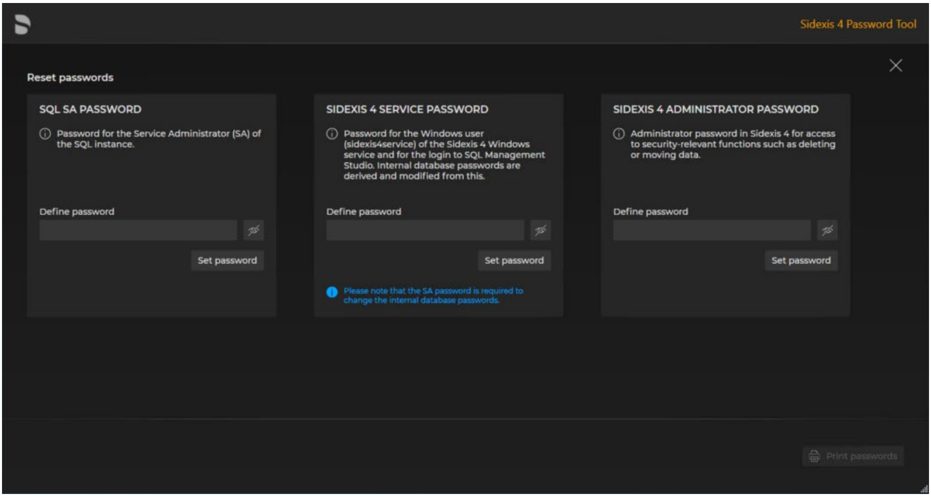
For this purpose, Sidexis 4 has a separate password tool that you can use to set and change secure passwords in accordance with the password security guidelines. Only Windows users with administrator rights can run the password tool, and the tool can only be used on computers on which the

Sidexis 4 server has been installed. The password tool ensures the integrity of the defined passwords with the aid of cryptographic functions.

The tool is available in German (DE), English (EN), Italian (IT), French (FR) and Spanish (ES). The tool uses the selected language on your Windows computer and English as the default setting.

You can find the password tool (file name: PasswordTool.exe) both in the installation directory of your Sidexis server installation and in the Windows Start menu in the SIRONA directory next to the Sidexis 4 software.

Further information on the password tool is provided in the Sidexis 4 installation manual.



Sidexis 4 Password Tool

Reset passwords

SQL SA PASSWORD

Password for the Service Administrator (SA) of the SQL instance.

Define password

Set password

SIDEXIS 4 SERVICE PASSWORD

Password for the Windows user (sidexis4service) of the Sidexis 4 Windows service and for the login to SQL Management Studio. Internal database passwords are derived and modified from this.

Define password

Set password

Please note that the SA password is required to change the internal database passwords.

SIDEXIS 4 ADMINISTRATOR PASSWORD

Administrator password in Sidexis 4 for access to security-relevant functions such as deleting or moving data.

Define password

Set password

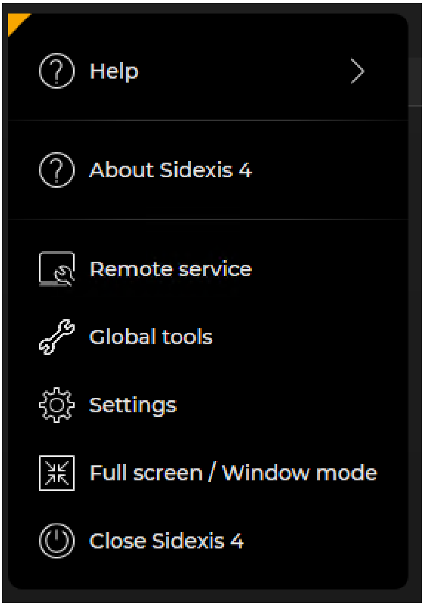
Cybersecurity: User access controls. Remote maintenance interface

The software product *Teamviewer* is used for customer service in the event of technical questions and for the remote maintenance of Sidexis 4. This product is not part of Sidexis 4.

You can access a remote support link for downloading the Teamviewer client via the main menu “Sidexis 4 Remote Service” of the Sidexis 4 user interface.

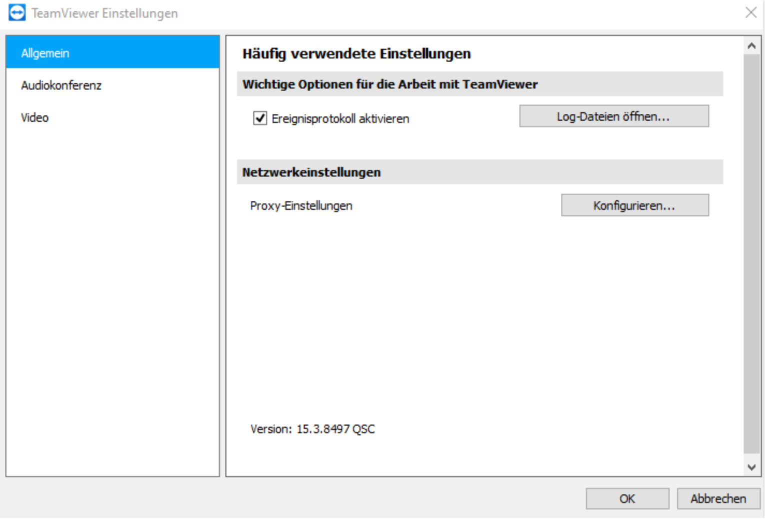
Following your local release, the weblink https://get.teamviewer.com/ds_imaging_support is opened and the Teamviewer software is downloaded onto your computer.

You can access the most important information about your Sidexis 4 installation via the "Anzeige Programminfo" (Show program info) menu of the user interface under submenu Remote Service.



Teamviewer records all activities during the session and the actions of the administration console in an integrated report log. Only authorized users can access the Teamviewer records and report logs (Audit Log) in accordance with a user guideline.

Check the remote maintenance log file (Teamviewer_Logfile) regularly in order to identify your releases on your workstation for remote access and potentially unauthorized remote accesses.



TeamViewer Einstellungen

Häufig verwendete Einstellungen

Wichtige Optionen für die Arbeit mit TeamViewer

☑ Ereignisprotokoll aktivieren

Netzwerkeinstellungen

Proxy-Einstellungen

Version: 15.3.8497 QSC

You will find more information on this in the Sidexis 4 service manual.

Cybersecurity: Logging user and system activities. System logs.

The Sidexis system log files containing sensitive data (DBMigration, delete, move) are stored in the protected SECURE MEDIA SHARE (PDATASEC) data area under the path <PDATASEC>\Log\Sidexis4. Regular Sidexis system log files without sensitive data are stored under the following path: %PROGRAMDATA%\Sirona\Log\Sidexis4.

The service manual glossary contains more detailed information about log files and their storage location and contents.

We also recommend that you regularly review the Sidexis **database log files** (SQL Server error log files) in order to identify potentially suspicious database accesses at an early stage.

You can find the **database log files** (SQL Server error log files) in the installation directory under:
“%ProgramFiles%/Microsoft SQL Server\MSSQL14.Sidexis_SQL\Log”

In addition, you should regularly check the Windows user log file in order to identify potentially suspicious accesses to your system.

Check the **remote access log file** (Teamviewer_Logfile) regularly in order to identify unauthorized remote accesses.

Cybersecurity: Security of data at rest. Data encryption.

The Sidexis 4 service is authorized to access the SQL database by means of authentication.

Security-relevant operations on patient and health data are protected and logged by means of authorization and authentication mechanisms. See Cybersecurity: Logging user and system activities. System log.

Sidexis 4 allows sensitive patient and health data to be stored in a separate, protected (and where appropriate encrypted) SECURE MEDIASHARE (PDATASEC) data area. The encryption functionality of your operating system (e.g. Microsoft Windows Bitlocker) is available to you for data encryption purposes. Bear in mind that encrypting large volumes of data may impair the performance of your system. Ensure that keys such as Bitlocker keys and restoration codes for the backup and restoration of your data are stored securely and redundantly (outside your system).

Check your security concept for the segmentation of your local computer networks (IT networks), the allocation of MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) data areas to your IT networks, and the definition of user access controls for the Sidexis 4 software, including authorized access to the databases.

Please refer to the Sidexis 4 service manual for further information on the provisioning of the Sidexis 4 databases, the configuration of data backups for the SQL database and the MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) databases, and possible data repair strategies.

Regular backup of patient and health data is recommended. See Cybersecurity: Data security. Availability of data and data backup

Cybersecurity: Security of data in transit. Data encryption. Authorization of adjacent systems.

Sidexis 4 requires secure data transmission (HTPPS data encryption) for the internal exchange of patient and health data between the components of Sidexis 4, such as intraoral/extraoral components, or with external communication nodes, such as the patient management system (PMS) of a clinic.

Communication with the Sidexis client and server via an interface can only take place after successful authorization and authentication of the interface and the communication nodes (adjacent systems) connected to it.

If you have created a network folder (network share) for SLIDA communication, SLIDA communication takes place via SMB (as of SMB 2.0 with encryption) on the network side in order to ensure the integrity of your patient and health data.

An authentication of the communication nodes (adjacent systems) takes place alongside the authorization of their components to perform certain operations in Sidexis 4. A specific application key and a security certificate are used for the authorization and authentication of the adjacent systems. Insecure adjacent systems are added to a blacklist by the Sidexis 4 configuration.

Unsecured communication interfaces to the adjacent systems can be deactivated at any time. See *Cybersecurity: Authentication of system components and deactivation of insecure interfaces*.

Communication between Sidexis client and server takes place via REST-based services using the HTTPS protocol with additional security measures for data integrity, such as data encryption and authentication of the communication nodes.

Access to the HTTPS web interfaces provided between the Sidexis 4 application services and the adjacent systems generally takes place via SSL/TLS secure links. Certificates are used for this purpose and are registered automatically on the Sidexis client PCs to be used.

Cybersecurity: Authentication of the Sidexis 4 components. Security certificates.

Sidexis 4 uses security certificates (X509) for the following purposes:

- to enable authentication of the Sidexis 4 components by means of a digital signature (certificate)
- to enable encrypted data communication between the Sidexis 4 components (certificate owners), for example between Sidexis 4 client and Sidexis 4 server

Cybersecurity: Protection against malware and manipulation. Authentication and integrity check for Sidexis 4.

Sidexis 4 has a tool (Integrity Checker) for checking the data integrity of the Sidexis 4 software distribution (*.dll and *.exe files).

The tool is available in German (DE), English (EN), Italian (IT), French (FR) and Spanish (ES). The tool uses the selected language on your Windows computer and English as the default setting.

You can find the Integrity Checker tool (file name: IntegrityChecker.exe) both in the installation directory of your Sidexis server and/or client installation and in the Windows Start menu under the SIRONA directory next to the Sidexis 4 software.

The Integrity Checker tool uses a *whitelist* (authorization register) to check:

- the data integrity of each DLL or individual EXE file with the aid of a cryptographic hash functionality (checksums) and a digital signature (certificate)
- the validity of each individual signature (certificate)

The integrity check always takes place when prompted by the user, either automatically via the Windows command line console or manually via the

Sidexis 4 user interface (see figures below). Any Windows user may run the tool.

The tool itself is protected against potential manipulation by third parties.

The integrity check does not require any parameters to be input. The tool uses the Sidexis 4 installation directory as the data path for the integrity check.

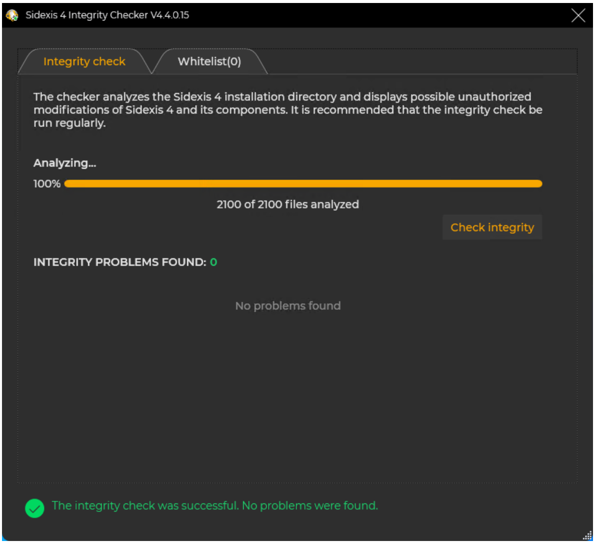
During the integrity check, the installation files are scanned and their integrity examined. Any identified integrity violations (*integrity issues)* are displayed on the user interface or, where appropriate, on the Windows command line console.

You also have the option of entering your assessment of the identified integrity violations (*integrity issues)* for certain unknown modules or tools as plausible (false positive) integrity violations (*accepted issues*) permanently in a whitelist (authorization register). Administrator rights are required for this purpose.

If implausible integrity violations are identified, we recommend that you perform an immediate repair installation of Sidexis 4 in order to prevent a potential compromise of the Sidexis 4 software.

The integrity check of the Sidexis 4 software should be carried out at regular intervals in order to provide efficient protection against malware. Perform the check from the installation directory, ideally before starting Sidexis 4 for the day.

Please refer to the installation manual for more information about the Integrity Checker tool.



Sidexis 4 Integrity Checker V4.4.0.15

The checker analyzes the Sidexis 4 installation directory and displays possible unauthorized modifications of Sidexis 4 and its components. It is recommended that the integrity check be run regularly.

Analyzing...

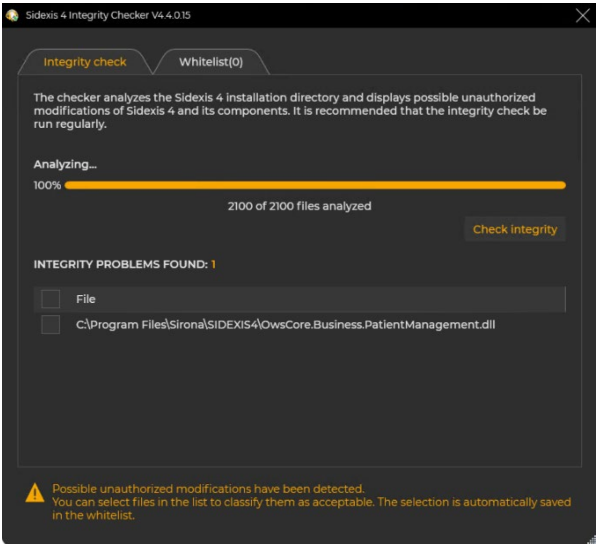
100%

2100 of 2100 files analyzed

INTEGRITY PROBLEMS FOUND: 0

No problems found

✓ The integrity check was successful. No problems were found.



Sidexis 4 Integrity Checker V4.4.0.15

The checker analyzes the Sidexis 4 installation directory and displays possible unauthorized modifications of Sidexis 4 and its components. It is recommended that the integrity check be run regularly.

Analyzing...

100%

2100 of 2100 files analyzed

INTEGRITY PROBLEMS FOUND: 1

□	File
□	C:\Program Files\Sirona\SIDEXIS4\OwsCore.Business.PatientManagement.dll

⚠ Possible unauthorized modifications have been detected.
You can select files in the list to classify them as acceptable. The selection is automatically saved in the whitelist.

Cybersecurity: Authentication of system components and deactivation of insecure interfaces

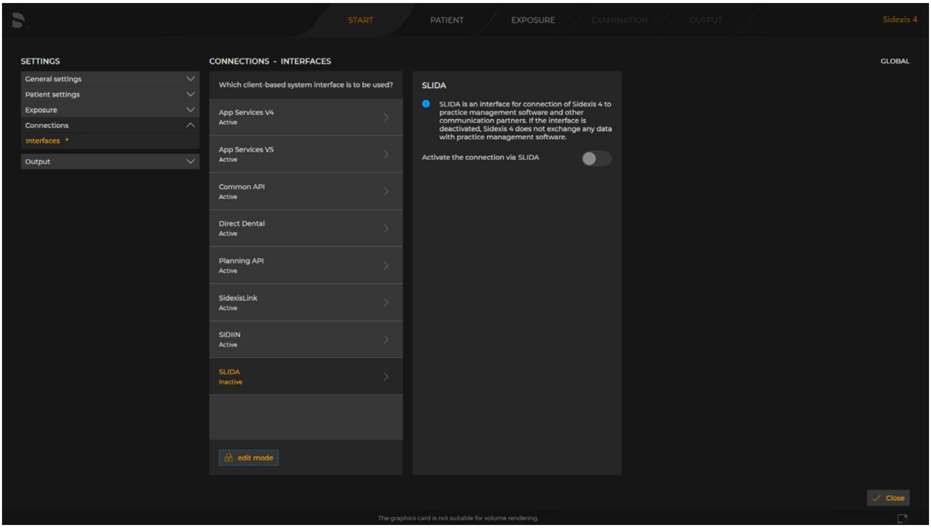
Sidexis 4 has security measures that enable a certificate-based authentication of the adjacent systems and Sidexis 4 system components and the deactivation of insecure interfaces.

If Sidexis 4 is executed abnormally, if the user suspects that malware has been loaded, or to remove unauthorized communication nodes (adjacent systems) from the Sidexis system configuration, the following communication interfaces (nodes/adjacent systems) to Sidexis 4 can be activated and deactivated individually subject to agreement with the DENTSPLYSIRONA service hotline:

- SLIDA
- Direct Dental
- Sidexislink
- SIDIIN
- AppService V4
- AppService V5
- Common API
- Planning API

You can administer the activation and deactivation of the communication interfaces to Sidexis 4 in the configuration menu “Settings – Connectivity – Interfaces”.

To complete the Sidexis 4 installation, the service engineer can carry out further security measures such as the deactivation of insecure interfaces for the additional hardening of the Sidexis 4 software.



CONNECTIONS - INTERFACES

Which client-based system interface is to be used?

App Services V4
Active

App Services V5
Active

Common API
Active

Direct Dental
Active

Planning API
Active

SidexisLink
Active

SIDIIN
Active

SLIDA
Inactive

SLIDA

SLIDA is an interface for connection of Sidexis 4 to practice management software and other communication partners. If the interface is deactivated, Sidexis 4 does not exchange any data with practice management software.

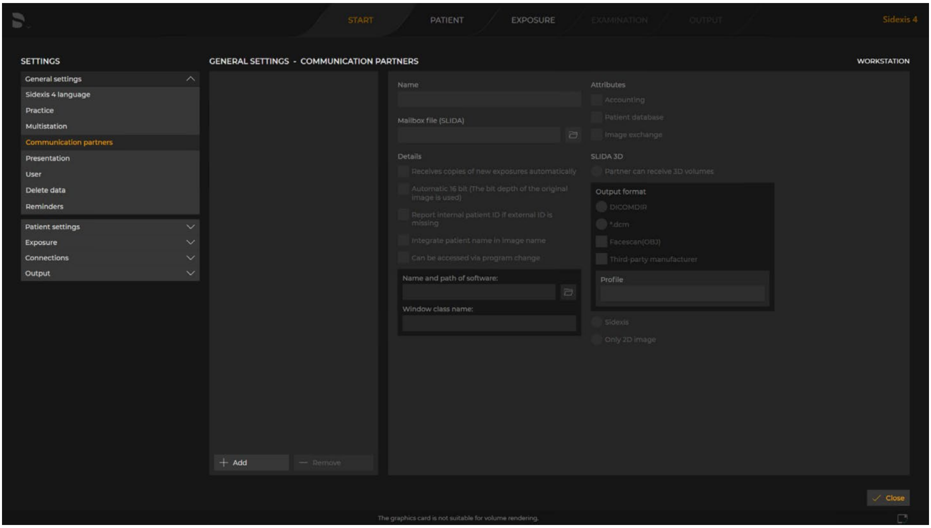
Activate the connection via SLIDA

The graphics card is not suitable for volume rendering.

To deactivate a potentially insecure interface, the Sidexis 4 administrator password must be entered.

Note: The deactivation of an interface will result in the functionality available via the interface being impaired or made unavailable.

You can define the settings for the communication interfaces (Communication Partners) to Sidexis 4 in the configuration menu “General Settings – Communication Partners”.



GENERAL SETTINGS - COMMUNICATION PARTNERS

WORKSTATION

Name

Mailbox file (SLIDA)

Details

□ Receives copies of new exposures automatically

□ Automatic 16 bit (The bit depth of the original image is used)

□ Report internal patient ID if external ID is missing

□ Integrate patient name in image name

□ Can be accessed via program change

Name and path of software:

Window class name:

Attributes

□ Accounting

□ Patient database

□ Image exchange

SLIDA 3D

○ Partner can receive 3D volumes

Output format

○ DICOMDIR

○ *.dcm

□ Facescan(OBJ)

□ Third-party manufacturer

Profile

○ Sidexis

○ Only 2D image

The graphics card is not suitable for volume rendering.

Cybersecurity: Data security. Availability of data and data backup

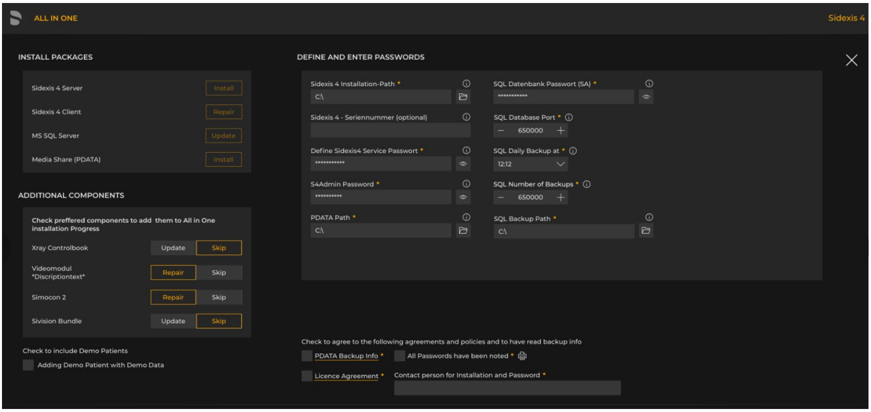
Ensure the availability and resilience of your IT systems, IT computer networks and MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) data at all times:

- Increase availability by using redundant systems such as RAID systems.
- Create MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) data backups at regular intervals. Perform both data backups at the same time to ensure the temporal data consistency of PDATA and PDATASEC.
  - The backup of the MS SQL database is set automatically during installation of the Sidexis 4 server and therefore takes place automatically.
  - It is possible to perform a file backup of locally stored patient and health data; this takes place in the protected data area SECURE MEDIA SHARE (PDATASEC) and the unprotected data area MEDIA SHARE (PDATA). This backup must be set by the operator and reviewed regularly by the responsible CERT (medical device safety officer, medical IT risk manager, etc.).

  - Configure the file backup with corresponding backup software, bearing in mind that all files and subfolders must be backed up.
  - Pay attention here to the temporal sequence so that you can also include the backup of the SQL database in your file backup.
  - Perform regular checks to determine whether you can restore an existing backup and to verify the plausibility of the backup data on a test server.
    - ➔ Tip: Monitor the ERRORLOG file, which can be found under “%ProgramFiles%/Microsoft SQL Server\MSSQL14.Sidexis_SQL\Log”, for (un)successful backup operations.
- Check your security concept for the segmentation of your local computer networks (IT networks), the allocation of MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) data areas to your IT networks, and the definition of user access controls for the Sidexis 4 software, including authorized access to the databases.

Please refer to the Sidexis 4 service manual for further information on the provisioning of the Sidexis 4 databases, the configuration of data backups for the SQL database and the MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) databases, and possible data repair strategies.

- Draw up an emergency concept, for example in the form of an emergency plan. Consider the following aspects for the emergency concept:
  - The most important risks for your business processes and resources, and your risk strategies in this regard
  - Consider the risks arising from data and information security in the emergency plan, such as data loss as a result of a damaged hard disk or unavailability due to failure of your IT networks.
  - Develop a continuity strategy that allows you to restart and restore your business processes within the required time.
  - Plan a training concept for your staff on the topic of emergency management and data security



INSTALL PACKAGES

Sidexis 4 Server — Install
Sidexis 4 Client — Repair
MS SQL Server — Update
Media Share (PDATA) — Install

ADDITIONAL COMPONENTS

Check preffered components to add them to All in One installation Progress

Xray Controlbook — Update [✓ Skip]
Videomodul *Discriptiontext* — [✓ Repair] Skip
Simocon 2 — [✓ Repair] Skip
Sivision Bundle — Update [✓ Skip]

Check to include Demo Patients

□ Adding Demo Patient with Demo Data

DEFINE AND ENTER PASSWORDS

Sidexis 4 Installation-Path * C:\
Sidexis 4 - Seriennummer (optional)
Define Sidexis4 Service Passwort * ***********
S4Admin Password * **********
PDATA Path * C:\

SQL Datenbank Passwort (SA) * ***********
SQL Database Port * 650000
SQL Daily Backup at * 12:12
SQL Number of Backups * 650000
SQL Backup Path * C:\

Check to agree to the following agreements and policies and to have read backup info

□ PDATA Backup Info * □ All Passwords have been noted *

□ Licence Agreement * Contact person for Installation and Password *

Source: Sidexis 4 Installation Manual

Cybersecurity: Maintenance of Sidexis 4

Remote maintenance

Insecure remote maintenance access can lead to authorized penetration into your IT systems and data. This can result in manipulation of your software and data losses. Define and use remote maintenance accesses with great care, as follows:

- Ideally, draw up a guideline defining how remote maintenance is to be carried out, including what activities are to be monitored, what target data is to be kept and how the communication links are to be protected.
- Check where and when remote maintenance is absolutely essential and permit access to the corresponding workstations only for the required period and for the system components to be maintained.
- Agree a legally binding contract on remote maintenance with your service provider and contact your IT security manager, medical device safety officer or your medical IT risk manager.
  Tip: Verify the service provider's authenticity. Ask for information that only your service provider can know, such as your customer number.
- Monitor remote maintenance accesses and document every operation.

Tip: Make a video recording of the remote maintenance (you may need your service provider's consent for this).

- Following remote maintenance, check the audit log file for each remote maintenance access.
  See *Cybersecurity: User access controls. Maintaining an audit log*

Provision and installation of software and security updates

Dentsply Sirona | SIRONA Dental Systems GmbH, as the manufacturer, will ensure the maintenance of the Sidexis 4 software throughout the entire product lifecycle within the framework of your development, market surveillance and reporting processes.

The maintenance measures will be made available to the customer in the form of software updates. The maintenance measures encompass all kinds of adaptive, perfective, corrective or preventive software changes, both for product functionality (update) and for product security (security update).

Dentsply Sirona | SIRONA Dental Systems GmbH, as the manufacturer, will inform your customer via its own sales network and its distributors worldwide about available software updates, including installation instructions, and will make these available for download in a protected area with limited access (distributor area) on the official online portal.

Potential IT security (cybersecurity) incidents will be regularly monitored and evaluated and security updates provided as necessary as part of the activities for market surveillance and security management for the Sidexis 4 software in collaboration with relevant economic operators (operators, distributors, importers and users).

Together with the manufacturer, all economic operators (operators, distributors and importers) also have an obligation to monitor cybersecurity incidents/vulnerabilities as part of their business processes for post-market surveillance and security incident management.

You need administrator access rights to install software updates in Sidexis 4. Please refer to the installation manual for further information about installing the Sidexis 4 software.

Cybersecurity: Security management. General.

Regularly review your security concept and your security management strategy with your risk management and IT security (cybersecurity) officers to confirm the suitability and effectiveness of the security measures.

You will find a few useful tips below (list not exhaustive):

IT infrastructure

- Protection against malware: anti-virus program
  Use professional anti-virus software on all computers (workstations) within your local computer network (IT network) and scan all information from all data sources (USB stick, CD-ROM/DVD, web pages, e-mails including attachments, etc.).
  Ensure that the anti-virus program is updated regularly and configured correctly for the Sidexis 4 operational environment with regard to data integrity, data protection and the performance design of your IT systems. Only users with administrator access rights must be permitted to make security-related changes to the program settings.
- Operating systems (OS)
  Use only tried-and-tested versions of operating systems on all computers (workstations) within your local computer network (IT network); these must have been released for secure, interoperable use with Sidexis 4 (see Sidexis 4 system requirements).
  We recommend that you avoid using older versions of the operating systems, despite their interoperability with Sidexis 4, on account of the risks associated with potentially missing security functions and settings.
  Likewise, additional security measures (*hardening*) are recommended for the operating systems as follows (list not exhaustive):
    - Deactivate or, where appropriate, remove unnecessary services, applications and network protocols.
    - Carefully configure the user authentication for your operating system with the aid of a security guideline.
    - Control resources restrictively (access to resources such as software and data).

Ensure that you install relevant security updates from the original vendor of the operating system for the versions (operating system) released for Sidexis 4 on all computers.

- Firewall:
  Use a firewall to protect your local computer network (IT network). Allow access to your local computer networks and your computers only in exceptional cases (*secure by default*) and draw up a firewall guideline to regulate how data flows into and out of your networks.

  Limit internet access to a minimum.

  Consider the technical security relationships between the firewall configuration and remote maintenance. Determine the group of authorized users for remote maintenance through the assignment of corresponding user rights and in the user access control and firewall security guidelines.

  Review the firewall rules for connections from and to printers, copiers and multifunctional devices from the internet in order to prevent your local computer networks (IT networks) from being compromised.

  Regularly update all network components (such as routers).

Third-party software

Only install and use third-party software if this is required for the work to be carried out in the dental practice.

Use only current versions, including all available security patches.

Check regularly whether vulnerabilities have been identified for the third-party software. See the next section.

Tip: Select a security software product that informs you actively when security updates are available for third-party software.

Management of vulnerabilities

As part of your security management strategy, we recommend that you draw up a specific guideline for IT security incident and vulnerability management.

Reference sources available to you containing an efficient description and categorization of vulnerabilities and software defects include for example ANSI/AAMI SW91:2018 *Classification Of Defects In Health Software* .

Regularly review the publicly available information on vulnerabilities. We recommend the following leading information sources:

- NIST Vulnerability Database (NVD):
  https://nvd.nist.gov
- The MITRE Corporation Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/cve/search_cve_list.html
  Site migration to https://www.cve.org/ currently ongoing
- BSI (Germany), CERT-Bund notifications:
  https://www.bsi.bund.de/DE/Service-Navi/Abonnements/Warnmeldungen/warnmeldungen_node.html

Literature and resources

We recommend that you consult globally available sources of useful information and recommendations on IT security (cybersecurity) for your security analyses and decisions, such as:

- The Computer Security Resource Center (CSRC) of the U.S. National Institute of Standards and Technology (NIST): https://csrc.nist.gov/publications/sp
- The IT Baseline Compendium and Standards of the German Federal Office for Information Security (BSI): BSI - IT-Grundschutz-Kompendium (bund.de)
- The European Union Agency for Cybersecurity (ENISA): ENISA (europa.eu)

5 System information

This section gives an overview of the Sidexis 4 system and provides all information that IT administrators need to set up Sidexis 4 securely in a local computer network.

Brief overview of Sidexis 4:

Purpose, indication and contraindication

This information is provided in the **Sidexis 4 user manual** (REF 6774579 for German and REF 6774587 for English).

Release

The product bears the CE mark in accordance with Regulation (EU) 2017/745 on medical devices (MDR).

Intended operational environment of use

The Sidexis 4 system consists of two system components: a server and a client as a client-server solution that can be operated as a single-station or multiple-station system.

The seamless, high-quality operation of a local computer network (local area network/LAN) requires unrestricted conformity with the prevailing electrical installation in the building in accordance with the internationally recognized ISO/IEC 11801 standards, European standards EN 50173 and EN 50174, German standards VDE 0800-173 and 0800-174 or the U.S. standard EIA/TIA 568 A/B, which are derived from the cited basic standard. At the same time, the network connections to X-ray components of the manufacturer must also be monitored.

The configuration of a local computer network (IT network) is of great importance to a secure operational environment, also referred to as the *intended operational environment of use* by the accompanying documentation MDCG 2019-16 on cybersecurity to Regulation (EU) 2017/745 (MDR), as is data and information security (cybersecurity), as explained briefly in *Overview of the system environment: IT networks, network zones and secure communication links (conduits)*.

Alongside the requirements governing cybersecurity for the operational environment, further requirements relating to the system operability for the operational environment must also be considered. See the definition of *interoperability* in *Definitions according to Regulation (EU) 2017/745 (MDR).*

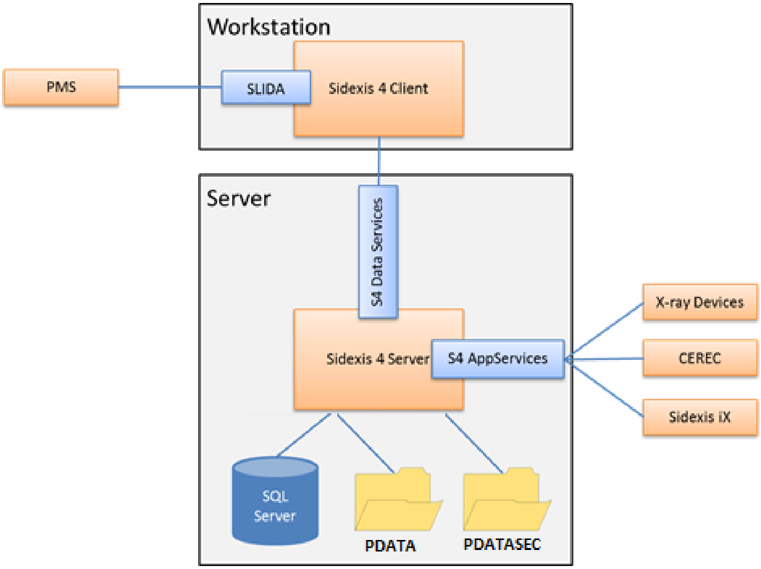
It is the responsibility of the operator, the healthcare facility and, where appropriate, the medical IT risk manager to implement a global target degree of interoperability (*interoperability level*) for all medical devices in an operational environment or IT network.

System requirements

Please regularly review the current system requirements at www.dentsplysirona.com/sidexis-4-system-requirements

Technical overview

The following diagram shows the components of the Sidexis 4 system – the client and server software components and the MEDIA SHARE (PDATA) and SQL Server database components – as well as the network interfaces provided for the integration of practice management systems (PMS), X-ray devices, CEREC software and Sidexis iX.



Sidexis 4 system components	
Software	
Sidexis 4 client *File name:* sidexis4.exe *Process name:* Sidexis4	The executable file with the name Sidexis4.exe represents the client component of the Sidexis 4 software, which can be found in the target folder of your software installation on the respective workstation(s) (PC). It is recommended that no administrator access rights be used for the normal use of the Sidexis 4 software on your computer. Standard user rights are sufficient.
Sidexis 4 server *File name:*	The executable file with the name SidexisRestService.exe represents the server component (Service) of the Sidexis 4 software, which can be

SidexisRestService.exe *Process name:* Sidexis4service	found in the target folder of your software installation on the respective workstation (PC). The Sidexis 4 server (Service) is configured during installation on your local computer with automatic system startup. It is recommended that no administrator access rights be used for the normal use of the Sidexis 4 software on your computer. Standard user rights are sufficient. *Recommendation:* Do not permit any remote access to the Sidexis 4 server (Service).
Databases	
Sidexis 4 SQL Server (instance) Microsoft SQL Server *Process name:* ▪ Sidexis_SQL ▪ PDATA_SQLEXPRESS Interfaces: ▪ Microsoft SQL Server 2017 Express ▪ Open Database Connectivity (ODBC)	Microsoft SQL Server is used to read out, write and search for patient and device data. This does not apply to media files (such as images, DVTs). During the use of Sidexis 4, all calls of the SQL Server instance from the Sidexis 4 server are executed by the NHibernate software component. Some older components, such as the SiConst consistency checker program, use the SQL Server instance via the ODBC connection. The Microsoft SQL Server instance "Sidexis_SQL" is installed and configured during installation of the Sidexis 4 server with the following settings: • Authentication: SQL Server and Windows authentication mode • Login audit: failed logins Tip: See *Cybersecurity: Logging user and system activities. System log*.

	• Network configuration: - Shared Memory: Enabled - Named Pipes: Disabled - TCP/IP: Enabled User accounts - User Access Management - SQL SA password: Password for the service administrator of the Sidexis SQL database instance - Sidexis 4 Service (Sidexis4Service) password: Password for the Windows user "Sidexis4Service" of the Sidexis 4 service (server) - Sidexis 4 Admin (S4Admin) password: Password for admin users in Sidexis 4 for accessing protected settings and sensitive functions (such as "Medien verschieben" (Move media) or "Patient löschen" (Delete patient)) of Sidexis 4 Data backup Use the options provided by Sidexis 4 to perform regular data backups of the SQL database. Note: The Sidexis 4 SQL Server uses commercial third-party software (off-the-shelf/OTS), namely SQL Server 2017 Express.
Sidexis 4 MEDIA SHARE (PDATA)	The file-based database MEDIA SHARE (PDATA) is used by the Sidexis 4 server to store general data

File folder or network share: PDATA	(not sensitive data!), data configurations and installation resources. *Recommendations:* ▪ Grant users access rights to the PDATA folder release (network share) only if this is essential for tasks related to the Sidexis 4 system. ▪ In particular, ensure that no access rights are granted to the MEDIA SHARE (PDATA) folder release (network share) for users via remote access or remote maintenance. ▪ Ensure that regular data backups are performed.
Sidexis 4 SECURE MEDIA SHARE (PDATASEC) *File folder or network share:* PDATASEC	The file-based database SECURE MEDIA SHARE (PDATASEC) is provided for the secure storage of sensitive data such as health and patient data, media data (such as recordings, DVTs and DICOMs), metadata and sessions via Sidexis 4. A secure data area must be set up for this purpose on your computer using the encryption software of your operating system (such as Microsoft Windows Bitlocker). Please ensure that the encryption keys (such as Bitlocker) and the restoration codes are stored securely and redundantly (if possible outside your computer on a separate storage medium). It is not possible to restore data without the Bitlocker keys and

	the restoration codes, even if backups have been made. *Recommendations:* The following points apply if you have released the file-based database SECURE MEDIA SHARE (PDATASEC) as a network folder (network share) on your IT network: ▪ Grant access rights to the network folder (network share) SECURE MEDIA SHARE (PDATASEC) only to the Sidexis 4 service (server). ▪ In particular, ensure that no access rights are granted to the network folder (network share) SECURE MEDIA SHARE (PDATASEC) for users via remote access or remote maintenance. ▪ Ensure that regular data backups are performed.
Interfaces	
SLIDA	SLIDA is an interface based on file-based communication (I/O operations, SLIDA input/output file) between the Sidexis 4 software and third-party software such as practice management systems. For each communication direction, a SLIDA input and output file is normally stored in a local folder on the computer that can be accessed by both communication partners. If you have created a network folder (network share) for SLIDA communication, SLIDA communication takes place via SMB with encryption on the network side.

	. *Recommendation:* For each SLIDA input and output file, use a folder that can be viewed and accessed only by certain users in order to carry out the corresponding Sidexis 4 activities.
Sidexis 4 Dataservices	This service endpoint is provided by the Sidexis 4 server to enable the Sidexis 4 client to access data. Transport Layer Security (TLS) is protected with the highest possible protocol determined between client and server. Depending on the combination of server and client operating system, this results in SSL 3.0, TLS 1.2 or TLS 1.3. The data endpoints access port 42928 and 42930 with a self-generated certificate.
Sidexis 4 AppServices V4 AppServices V5 AppServices V6	This service endpoint is provided by the Sidexis 4 server in order to enable X-ray devices and applications such as Sidexis iX and CEREC software to access high-level data (workflows, patients, media and configuration). *Note on AppServices versions:* Secure data transmission (Transport Layer Security/TLS) and component authentication is provided for Sidexis V4.4. The best possible SSL/TLS version (SSL 3.0, TLS 1.0 – TLS 1.3) will be negotiated. The service endpoints of these versions access ports 42929 (AppServices V4 and V5) and 42931 (AppServices V6) with a self-generated certificate.

Direct Dental	Client interface for integration of Sidexis XG devices/software plugins
SidexisLink	Interface for integration of Dentsply Sirona components such as Dentrix with the practice management system (PMS)
SIDIIN	Low-level interface to Dentsply Sirona X-ray devices. Generated data undergoes further processing in the PMS.
SiTwain	TWAIN 2.2 interface to Dentsply Sirona devices
Deactivation of insecure interfaces	See Cybersecurity: Security of data in transit. Data encryption. Authorization of adjacent systems.
Operational environment: adjacent systems	
Blacklist of insecure interfaces	Sidexis 4 has a preconfigured functionality for blocking (blacklisting) insecure interfaces. The blocking mechanism is updated systematically with the product updates. See Cybersecurity: Security of data in transit. Data encryption. Authorization of adjacent systems.

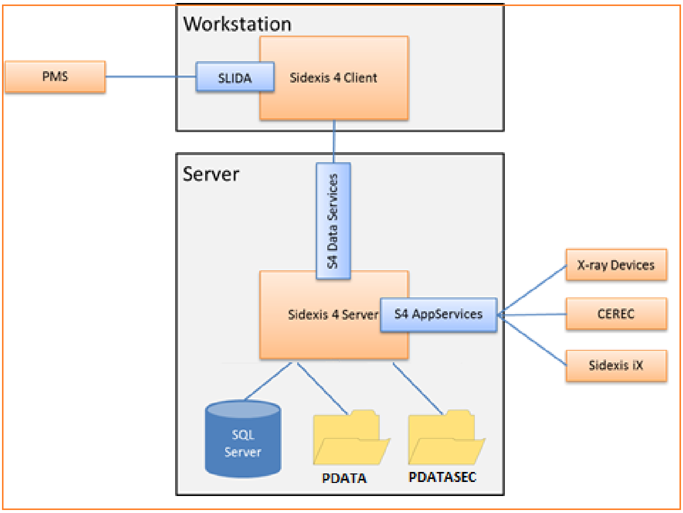
Overview of the system environment: IT networks, network zones and secure communication links (conduits)

The following diagrams (not exhaustive) show a few examples of possible configurations of your IT networks and the Sidexis 4 system. The IT networks are shown below with an orange frame.

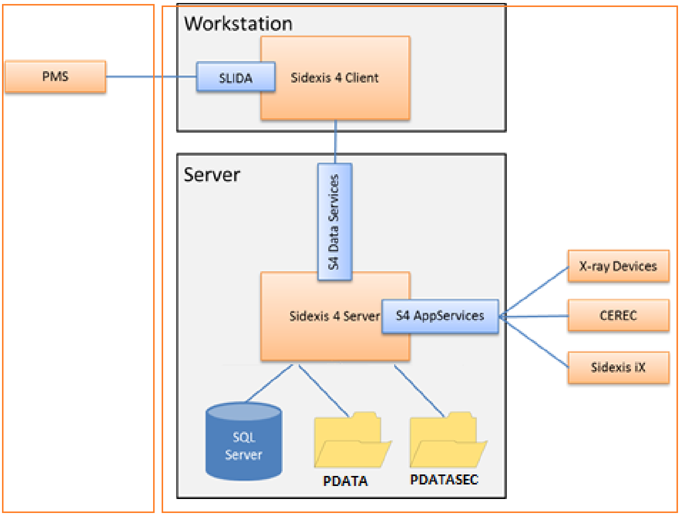
Please ensure that your IT networks are configured securely by your IT administrator in coordination with your medical device safety officer and, where appropriate, your medical IT risk manager. You can find useful information on the secure configuration of IT networks in the industry standard *DIN EN IEC 62443 Security for industrial automation and control systems*. The IEC 80001-1:2021 standard also helps you to apply risk management best practices for the IT networks in your organization.

The configuration of different security zones in an IT network (network segmentation) as well as the use of a DMZ for external interfaces, security routers and firewalls with secure communication links (conduits) combined with anti-virus software are recommended to ensure the secure use of the Sidexis system and to protect your patient data. This is only possible if the integrity of your local computer network is ensured by means of access controls for the different network segments.

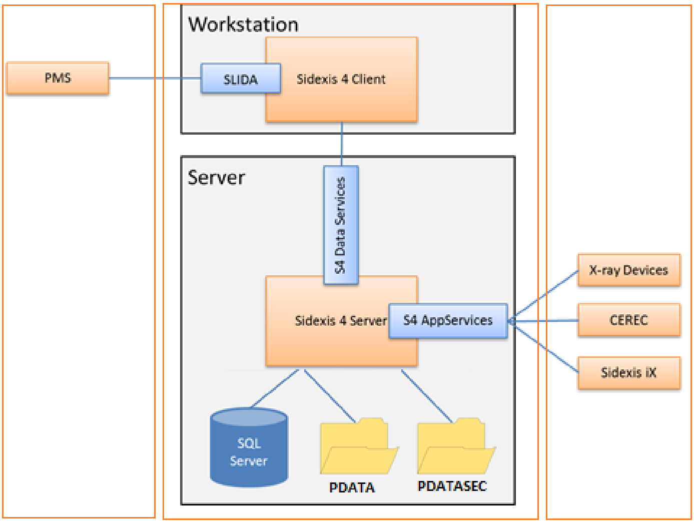
Example 1: only one IT network for all systems



Example 2: two IT networks – one for your PMS and one for all components of the Sidexis 4 system and the X-ray components



Example 3: multiple IT networks for separating PMS, Sidexis 4 client and server, and the X-ray components.



The secure segmentation and configuration of your IT networks is of great importance in protecting the Sidexis software and your health and patient data, including during data transmission between the IT networks (transmission confidentiality, transmission integrity).

6
Legal notice / disclaimer

Legal notice / disclaimer

Please note that this White Paper on “Data Protection and Product Security” is no substitute for legal advice regarding the manner in which the requirements of the European Regulations governing data protection and/or product security are to be met.

The author accepts no liability whatsoever for the up-to-dateness, correctness, completeness or quality of the information provided. Liability claims against the author in respect of material or immaterial damages caused by the use or non-use of the information provided or by the use of incorrect and incomplete information are generally excluded, save where willful misconduct or gross negligence on the part of the author can be proven.