Dentsply Sirona THE DENTAL SOLUTIONS COMPANY™

Sidexis 4

Data Protection and Product Security

White Paper

Dentsply Sirona

Contents

1 INTRODUCTION 5

PURPOSE OF THE DOCUMENT 6

2 DATA PROTECTION 7

AND DATA PRIVACY 7

INTERNATIONAL REFERENCE WORKS FOR DATA PROTECTION 8
DATA PROTECTION PRINCIPLES 9

3 CYBERSECURITY 11

DATA AND INFORMATION SECURITY 11

INTERNATIONAL REFERENCE WORKS FOR CYBERSECURITY 12
DEFINITIONS ACCORDING TO INTERNATIONAL STANDARDS 13
PRINCIPLES OF IT SECURITY (CYBERSECURITY) 14
DUTIES OF THOSE RESPONSIBLE FOR IT SECURITY (CYBERSECURITY) 17
MARKET MONITORING OF PRODUCT SECURITY: REPORTING SECURITY INCIDENTS (POST-MARKET SURVEILLANCE) 19
MEDICAL IT RISK MANAGER 20
CONTACT DETAILS FOR QUERIES REGARDING DATA PROTECTION (DATA PROTECTION AND DATA PRIVACY) AND CYBERSECURITY 20

4 STRATEGIES AND PROVEN METHODS 21

DATA PROTECTION: GENERAL PRECAUTIONARY MEASURES FOR PROTECTING YOUR DATA (DATA PROTECTION AND DATA PRIVACY) 22
Anonymization *22*
Organizational measures *22*
Sensitive data *23*
Adding information and comments to free text fields *23*
CYBERSECURITY: USER ACCESS CONTROLS. AUTHENTICATION / USER ACCESS AUTHORIZATION 24
CYBERSECURITY: USER ACCESS CONTROLS. REMOTE MAINTENANCE INTERFACE 28

Cybersecurity: Logging user and system activities. System logs..... 29
Cybersecurity: Security of data at rest. Data encryption. 30
Cybersecurity: Security of data in transit. Data encryption. Authorization of adjacent systems. 31
Cybersecurity: Authentication of the Sidexis 4 components. Security certificates. 32
Cybersecurity: Protection against malware and manipulation. Authentication and integrity check for Sidexis 4. 32
Cybersecurity: Authentication of system components and deactivation of insecure interfaces 35
Cybersecurity: Data security. Availability of data and data backup 37
Cybersecurity: Maintenance of Sidexis 4 39
Cybersecurity: Security management. General. 41

5 SYSTEM INFORMATION 44

Brief overview of Sidexis 4: 45
Purpose, indication and contraindication 45
Release 45
Intended environment of use 45
Overview of the system environment: IT networks, network zones and secure communication links (conduits) 55

6 LEGAL NOTICE / DISCLAIMER 59

Legal notice / disclaimer 60

1 Introduction

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

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 staff in the organizational areas of cybersecurity, data protection, marketing and sales who are involved in supporting the procurement process.

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

-
- Information on the measures to ensure the secure handling of important data in Sidexis 4 and general notes on best practices from international regulations for data protection in your organization.
- 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.
- 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 security measures aimed at ensuring the secure handling of important data in IT security (security for data privacy) and adequate software design (data privacy by design) ensure compliance with key technical requirements and standards governing data protection (data protection and data privacy).

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 those responsible for cybersecurity and for operating the local computer networks (IT networks) have access to all the information they need to carry out their work properly.

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 and data privacy

This section gives a brief overview of certain key aspects for ensuring the secure handling of important data in your organization. Purely informative, non-binding references to international technical regulations and standards on data protection are provided to help you better understand the specific data protection requirements that apply to you under international, national or local legislation and to fulfill these requirements in your organization and your systems.

The security measures aimed at ensuring the secure handling of important data in IT security (security for data privacy) and adequate software design (data privacy by design) ensure compliance with key technical requirements and standards governing data protection (data protection and data privacy).

Certain key aspects for ensuring the secure handling of important data in your organization and your systems, including for example Sidexis 4, are described below.

International reference works for data protection

Notwithstanding the references to leading international technical regulations and standards on the topic of data protection provided for your information in this document, we recommend that you carefully check the individual data protection requirements that apply to your organization and your systems in your market, your country and your region.

- U.S.A: FDA Privacy Act
- U.S.A.: HIPAA Security Rule, Administrative Safeguards of the Security Standards for the protection of Electronic Protected Health Information (45 CFR § 164.308)
- Canada: Health Canada Personal Information Protection and Electronic Documents Act (PIPEDA)
- EU / EEA: Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)
- Asia-Pacific: Asia-Pacific Economic Cooperation (APEC), Privacy Framework
- U.S.A: National Institute of Standards and Technology (NIST), NIST Privacy Framework: A tool for improving privacy through enterprise risk management V1.0 (January 16, 2020)
- U.S.A: National Institute of Standards and Technology (NIST), Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy (NIST SP 800-37 Rev.2, December 2018)
- International: ISO13485:2016, “Methods for protecting confidential health information”

- International: ISO/IEC 27701:2019-08, Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
- International: ISO/IEC 29101:2018, Information technology — Security techniques — Privacy architecture framework

Your organization and your systems must fulfill the specific data protection requirements applicable under international, national or local legislation.

Data protection principles

Some data protection principles, regulations and requirements are universal, irrespective of the specific international, national or local legislation applicable to your organization (processes, systems and products).

Below you will find some useful points of reference to help you design a data protection strategy for your organization:

- Draw up a guideline defining roles and responsibilities for enforcing data protection and privacy in your organizational processes and systems
- Keep a record of the groups of people with access to sensitive data
- Ensure compliance with the applicable data protection provisions under international, national or local legislation Certain key regulations and standards are listed in the previous paragraph *International reference works for data protection*
- Define a guideline to ensure data protection across your supply and sales chains (supply chain data custody), setting out the duties of your contractors and suppliers
- Always plan the delimitation of business data and sensitive personal data into your processes (process delimitation) and your systems (technical delimitation)
- Define strategies to deal with the loss, theft or unauthorized disclosure of sensitive data (data breach)

- Restrict the volume of data and establish transparent rules for the use of sensitive data, such as patient and health data, for the intended purpose
- Design process-related and technical procedures for accessing and correcting sensitive data, including consent
- Implement data and information security (IT security) measures to ensure the secure handling of sensitive data (data protection and privacy by design), including for example storage and electronic communication
- Apply general security techniques, such as encryption, for protecting important data

3 Cybersecurity

Data and information security

ACCORDING TO INTERNATIONAL RECOMMENDATIONS, STANDARDS AND BEST PRACTICES

This section provides a brief overview of certain key international recommendations, standards, and best practices for data and information security (cybersecurity).

Cited passages are shown in "*italics*".

International reference works for cybersecurity

Notwithstanding the references to leading international technical regulations and standards on the topic of IT security (cybersecurity) provided for your information in this document, we recommend that you carefully check the individual requirements governing information security and cybersecurity that apply to your organization and your systems in your market, your country and your region.

Below you will find some useful international technical reference works and standards (list not exhaustive) to help you design an IT security (cybersecurity) strategy for your organization:

- International: Principles and Practices for Medical Device Cybersecurity, International Medical Device Regulators Forum (IMDRF), 18 March 2020
- International: AAMI TIR57:2016 Principles for Medical Device Security – Risk Management, Association for the Advancement of Medical Instrumentation (AAMI)
- EU and EEA: Accompanying documentation to Regulation (EU) 2017/745 on medical devices (MDR), Guidance on Cybersecurity for medical devices MDCG 2019-16 Rev. 1, July 2020
- Canada: Guidance Pre-market Requirements for Medical Device Cybersecurity, Health Canada, 2019/06/26
- U.S.A: FDA Guidance (Draft) Content of Premarket Submissions for Management of Cybersecurity in Medical Devices, 18 October 2018
- U.S.A: FDA Guidance (Final) Postmarket Management of Cybersecurity in Medical Devices, 27 December 2016
- U.S.A: FDA Guidance Strengthening Cybersecurity Practices Associated with Servicing of Medical Devices: Challenges and Opportunities, 17 June 2021
- U.S.A: NIST Cybersecurity Framework, National Institute of Standards and Technology (NIST)
- U.S.A: FDA Guidance (Draft) Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, 8 April 2022
- U.S.A: FDA Paper Best Practices for Communicating Cybersecurity Vulnerabilities to Patients, October 2021

- Japan Guidance on Ensuring Cyber Security of Medical Devices, Japan's Ministry of Health, Labor and Welfare (MHLW), 2018

Your organization and your systems must fulfill the specific requirements governing IT security (cybersecurity) applicable under international, national or local legislation.

Definitions according to international standards

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

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

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

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

Incident

"Incident": An occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences.
Extended Definition: An occurrence that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Source: U.S. National Initiative for Cybersecurity Careers and Studies (NICCS), Cybersecurity Glossary (https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#I)

Interoperability

The ability of two or more systems or components to exchange information and to use the information that has been exchanged.
Source: U.S. National Initiative for Cybersecurity Careers and Studies (NICCS), Cybersecurity Glossary (https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#I)

Principles of IT security (cybersecurity)

Technical regulations and standards for cybersecurity (see previous section) define 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 international, national and local statutory requirements as well as by international standards such as AAMI TIR57:2016 and ISO/TR 24971.

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 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 defined briefly in the U.S. FDA Guidance "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" as follows:

(Section 5 Cybersecurity Functions – Identify and Protect, p. 4)
The extent to which security controls are needed will depend on the device's intended use, the presence and intent of its electronic data interfaces, its ***intended environment of use****, […]*

In addition, technical reference works and standards for cybersecurity point out the need for cooperation between the various stakeholders in the development, supply and sales chains.

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

Various reference works for cybersecurity, including for example 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), have 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)

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.

In this connection, requirements also arise for all stakeholders in the development, supply and sales chain, as described in the following paragraph *Duties of those responsible for IT security (cybersecurity)*.

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 all stakeholders in the development, supply and sales chains and the manufacturer to clarify a cybersecurity incident and to jointly define a field safety corrective action.

To ensure the successful and secure integration of Sidexis 4 into the intended environment, all stakeholders 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).

All stakeholders in the development, supply and sales chain are responsible for fulfilling the IT security (cybersecurity) requirements across the entire lifecycle through to withdrawal from the market. This is a shared responsibility.

I. Definition of operators and obligations for cybersecurity from relevant standards:

   Your organization and your systems must fulfill the specific requirements governing IT security (cybersecurity) as defined in the relevant standards applicable under international, national or local legislation. Examples include the definitions of the manufacturer, distributor, etc. in Regulation (EU) 2017/745 MDR or importer (adverse event) in U.S 21 CFR § 803.42.

II. Operators and obligations from international technical 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.

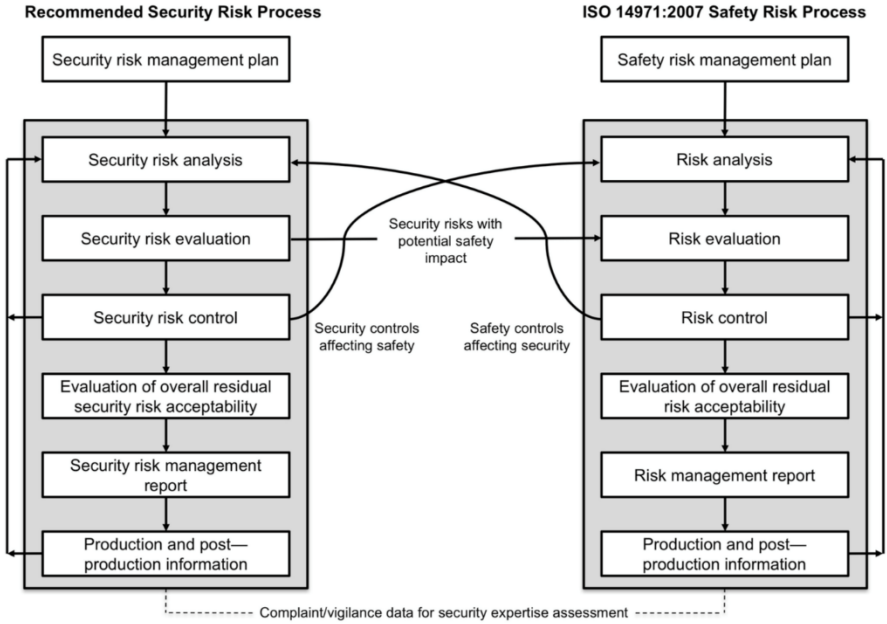
(*IEC 80001-1:2021 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software — Part 1: Application of risk management)*

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 their potential impact on patient safety takes place across the entire lifecycle according to the recommendation of international standard AAMI TIR57:2016 Principles for Medical Device Security – Risk Management, based on the definition in standard ISO14971:2020-7.



Source: AAMI TIR57:2016 .

In conjunction with the manufacturer, all stakeholders including for example manufacturers, suppliers, contractors, system integrators for IT systems and those responsible for IT security and risk management of the IT systems have a duty to monitor cybersecurity incidents (security 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:

- U.S. National Cybersecurity & Infrastructure Security Agency (CISA) https://www.cisa.gov/uscert/ncas
- The MITRE Corporation Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org/cve/search_cve_list.html
- CERT Germany https://www.cert-bund.de and CERT European Union https://cert.europa.eu.

Medical IT risk manager

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

Contact details for queries regarding data protection (data protection and data privacy) 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 (DATA PRIVACY AND DATA PROTECTION) AND DATA AND 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: general precautionary measures for protecting your data (data protection and data privacy)

The previous sections gave an informative overview of general useful recommendations and best practices for better data protection.

In this section, you will find specific points of reference on data protection to ensure the secure handling of Sidexis 4.

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.

Sensitive data

- Sidexis 4 processes the following personal data of patients:
  - 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.

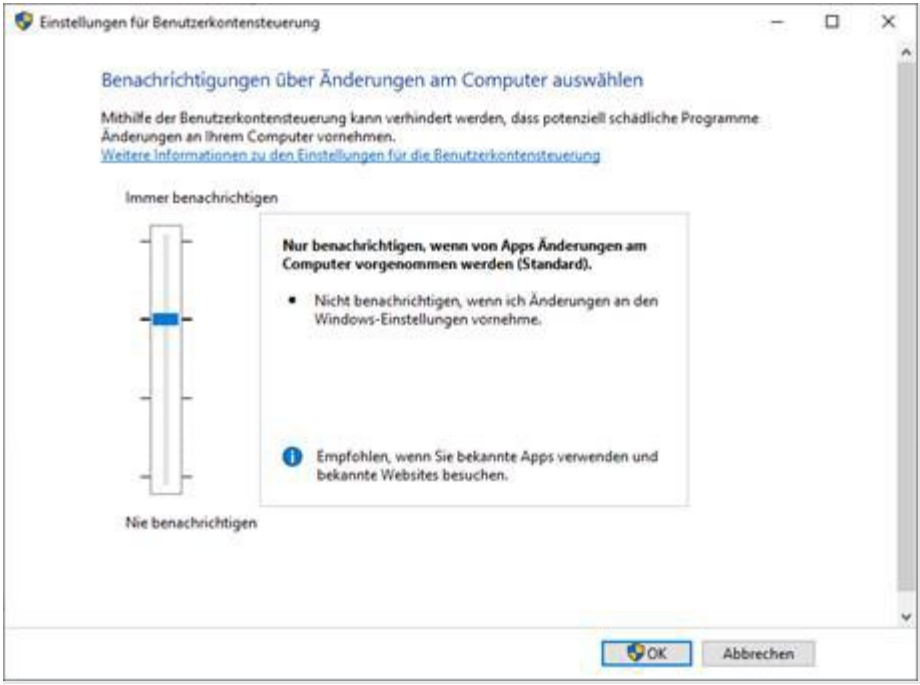
Please do not use these free text fields and comment fields to add personal, patient or health data such as the patient's name.

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)”.



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

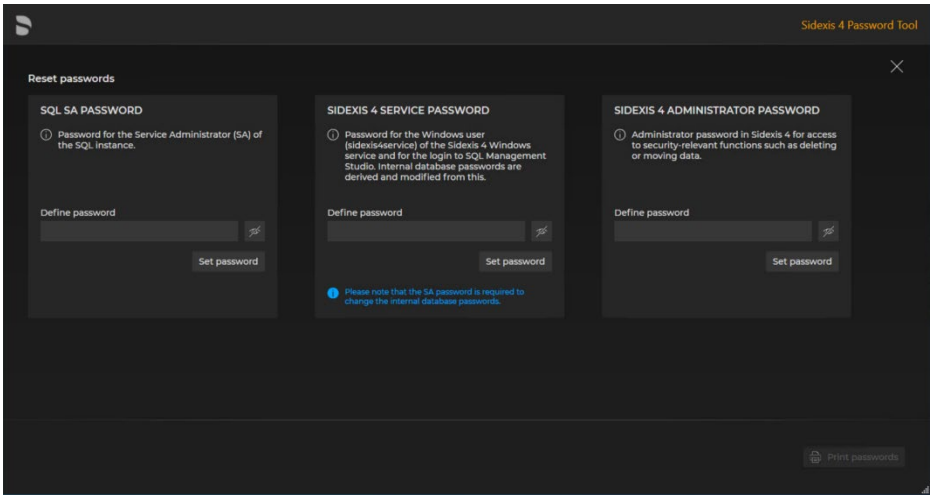
During operation, we recommend changing the passwords at regular intervals.

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.

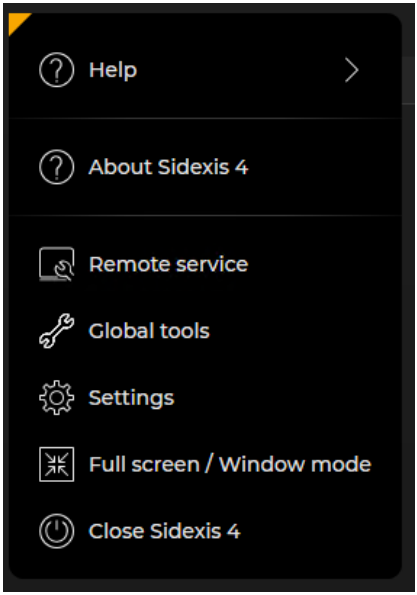

Sidexis 4 Password Tool
Reset passwords
SQL SA PASSWORD
Password for the Service Administrator (SA) of the SQL instance.
Define password
Set password
SIDEXIS 4 SERVICE PASSWORD
Password for the Windows user (sidexis4service) of the Sidexis 4 Windows service and for the login to SQL Management Studio. 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
Print passwords

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.

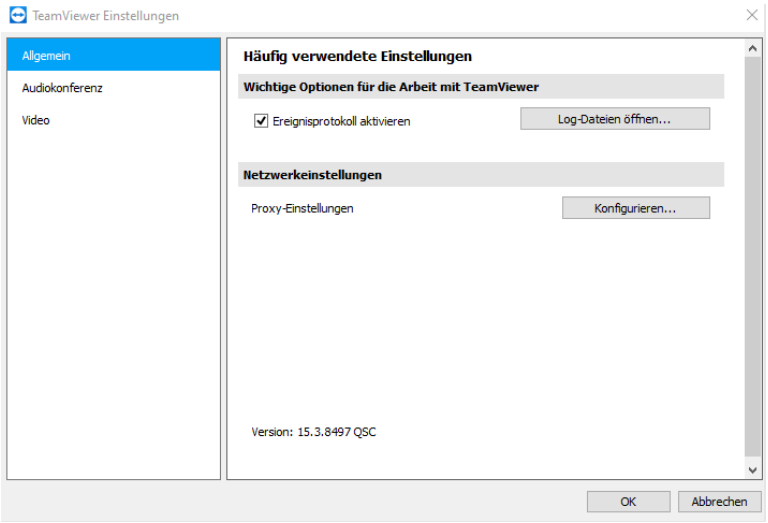
You can access the most important information about your Sidexis 4 installation via the “Anzeige Programminfo” (Show program info) menu of the user interface under the submenu "Remove Service".



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.



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.

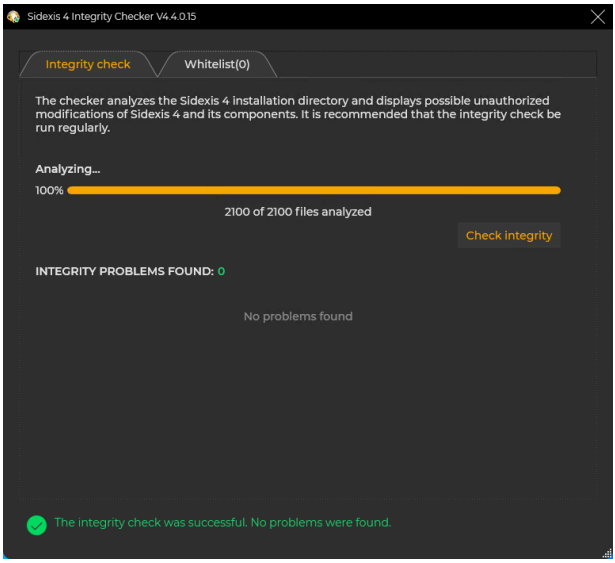
During the integrity check, the installation files are scanned and their integrity examined. Any identified integrity violations (*integrity issues)* are displayed on the user interface or, where appropriate, on the Windows command line console.

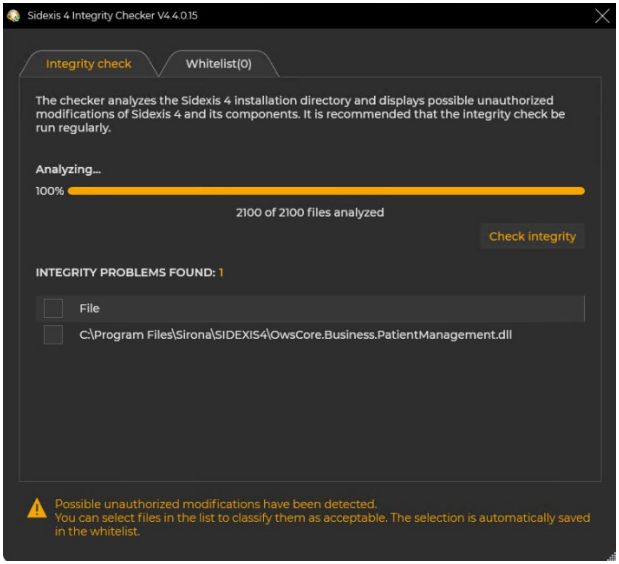
You also have the option of entering your assessment of the identified integrity violations (*integrity issues)* for certain unknown modules or tools as plausible (false positive) integrity violations (*accepted issues*) permanently in a whitelist (authorization register). Administrator rights are required 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
Integrity check
Whitelist(0)
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
Check integrity
INTEGRITY PROBLEMS FOUND: 0
No problems found
The integrity check was successful. No problems were found.


Sidexis 4 Integrity Checker V4.4.0.15
Integrity check
Whitelist(0)
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
Check integrity
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

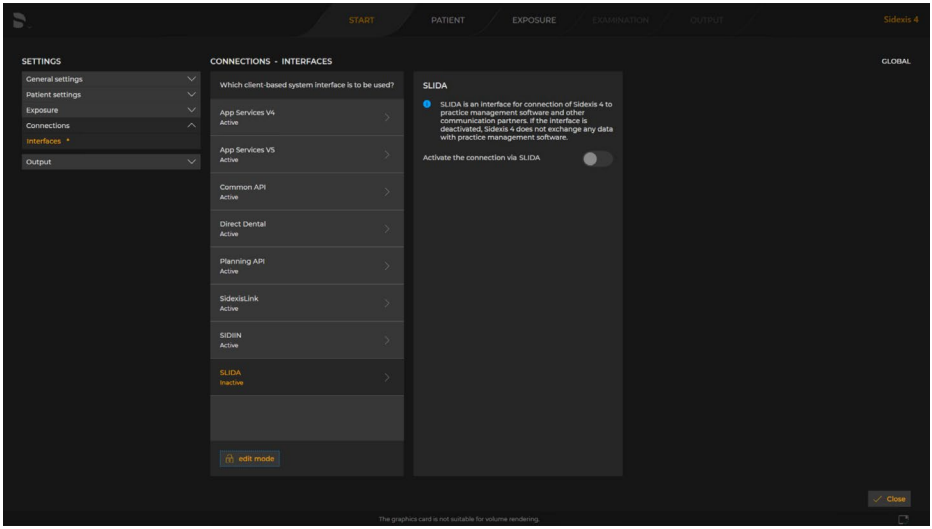
Sidexis 4 has security measures that enable a certificate-based authentication of the adjacent systems and Sidexis 4 system components and the deactivation of insecure interfaces.

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”.

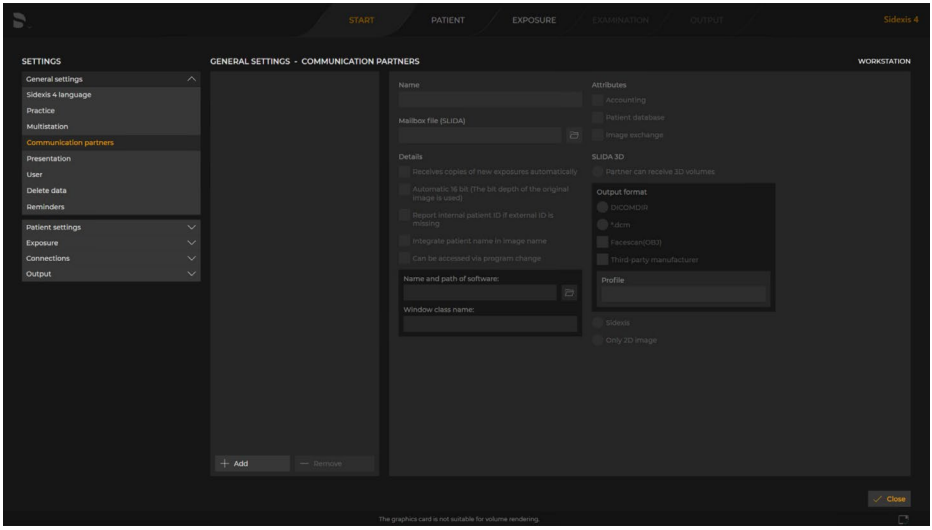
To complete the Sidexis 4 installation, the service engineer can carry out further security measures such as the deactivation of insecure interfaces for the additional hardening of the Sidexis 4 software.



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”.



Cybersecurity: Data security. Availability of data and data backup

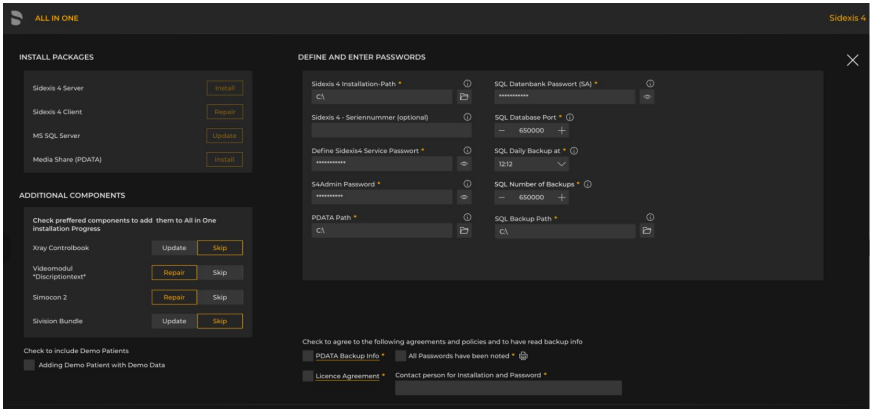
Ensure the availability and resilience of your IT systems, IT computer networks and MEDIA SHARE (PDATA) and SECURE MEDIA SHARE (PDATASEC) data at all times:

- 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



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 stakeholders in the supply and sales chains (cyber supply chain risk management).

Together with the manufacturer, all stakeholders in the supply and sales chains 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
- 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, as listed in *International reference works for cybersecurity*.

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 6774587).

Release

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

Intended 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 internationally recognized standards such as

- international standard ISO/IEC 11801 (basic standard)
- European standards EN 50173 and EN 50174
- German standards VDE 0800-173 and 0800-174
- U.S. standard EIA/TIA 568 A/B
- and/or any technically equivalent international, national or local regulations.

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 *intended environment of use*.

See *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.

It is generally the responsibility of the user, the operator, the healthcare facility and, where appropriate, the medical IT risk manager (in accordance with IEC 80001-1:2021-09) to implement a secure operational environment and a global target degree of interoperability (*interoperability level*) for all medical devices in an operational environment or IT network.

Consult the competent department in your organization, for example Operations or Regulatory Affairs, to clarify the different responsibilities of your organization and your contractors and suppliers.

You will find useful information in this regard in the following technical regulations, standards and guidelines:

- *(EU and EEA): EU MDCG 2019-16 to Regulation (EU) 2017/745 (MDR, April 5, 2017)*
- *(U.S.A): FDA Guidance "Design considerations and pre-market submission recommendations for interoperable medical devices" (September 2017, final)*
- *(International): Guidance (IMDRF/CYBER WG/N60FINAL:2020) "Principles and practices for medical device cybersecurity" of the International Medical Device Regulators Forum (IMDRF, March 18, 2020)*
- *(International): IEC 80001-1:2021-09 Safety, effectiveness and security in the implementation and use of connected medical devices or connected health software - Part 1: Application of risk management*

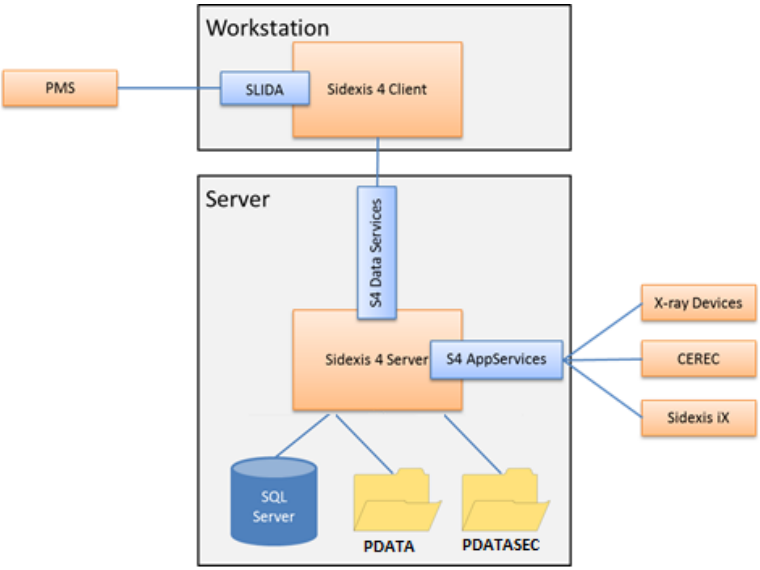
See also *International reference works for cybersecurity.*

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:* SidexisRestService.exe *Process name:* Sidexis4service	The executable file with the name SidexisRestService.exe represents the server component (Service) of the Sidexis 4 software, which can be 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 is used to read out, write and search for patient and device data. This does not apply to media files (such as images, DVTs).

Microsoft SQL Server *Process name:* ▪ Sidexis_SQL ▪ PDATA_SQLEXPRESS Interfaces: ▪ Microsoft SQL Server 2017 Express ▪ Open Database Connectivity (ODBC)	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 <u>User accounts - User Access Management</u> • **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 <u>Data backup</u> 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) *File folder or network share:* PDATA	The file-based database MEDIA SHARE (PDATA) is used by the Sidexis 4 server to store general data (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.

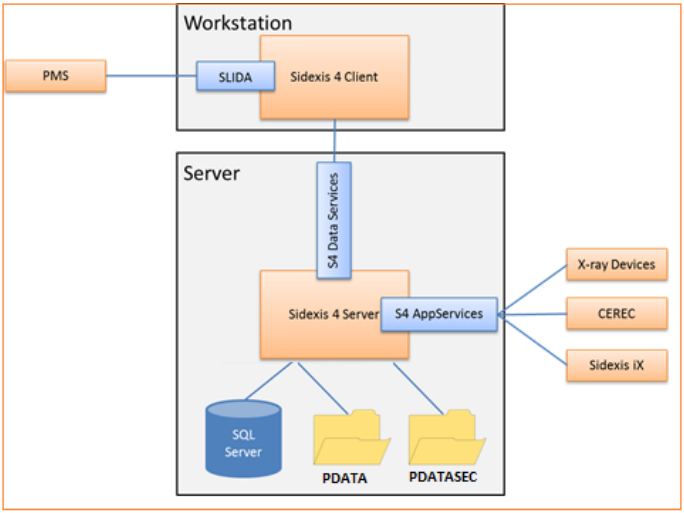
Overview of the system environment: IT networks, network zones and secure communication links (conduits)

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.

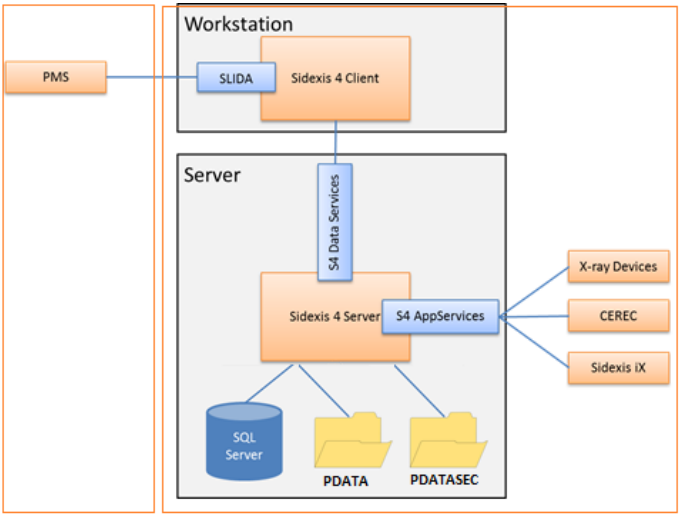
Please ensure that your IT networks are configured securely by your IT administrator in coordination with your medical device safety officer and, where appropriate, your medical IT risk manager. You can find useful information on the secure configuration of IT networks in the industry standard *DIN EN 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.

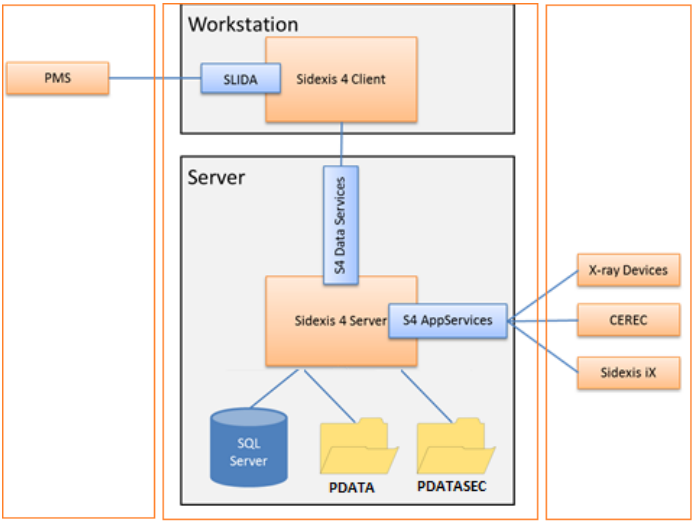
Example 1: only one IT network for all systems



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 governing data protection and/or product security (including cybersecurity) under international, national or local legislation 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.