Dentsply Sirona THE DENTAL SOLUTIONS COMPANY™

CAD/CAM
Data Protection and Product Security

Whitepaper

Content

1 Introduction

This Whitepaper describes the technical aspects of CAD/CAM SW products that are relevant for IT Security and Data Protection in general. Please revise applicable laws in your countries for details.

It is mainly intended for the service and customer personnel that are responsible for installation, configuration, maintenance, and operation, for the Controller of Data Protection and for Marketing and Sales to support the procurement process. But it also should be made available to customers on demand for transparency.

This Product Security Whitepaper contains all required information to:

- Give guidance of how to fulfill the requirements of the “General Data Protection”
- Support the evaluation process for the Medical Product.
- Provide information needed for generic questionnaires.
- Provide this information to customer and service personnel.
- Securely install, configure, maintain, and operate the Medical Product (this Whitepaper does not replace installation manual and user manual).

Purpose of this Document

IT Security of Medical Products, also called “Product Security” is an important aspect of their function. It is absolutely necessary to ensure their safe operation, and to ensure:

- Confidentiality of patient data
- Integrity of the Medical Product, i. e. the product functions as intended
  Availability of the Medical Device

To ensure Product Security, a Medical Product, has to be designed, implemented and tested properly – but it also needs to be installed, configured, maintained and operated as intended. If any of these aspects is not observed, the Medical Product’s Product Security can be easily compromised, with potential grave consequences for its safety.

Data Protection is in close relationship to Product Security. The “General Data Protection Regulation” of the European Union enforces the protection of personal data also for Medical Products.

The intention of the Whitepaper is to ensure that people and institutions responsible for installation, maintenance and operation of Medical Products as well as Controllers for Data Protection have all required information to do their work properly:

- Provide additional information regarding the requirements of the “General Data Protection Regulation” and how the Medical Product supports the Controller to fulfill the requirements.
- Provide information regarding all relevant Product Security aspects to customer and service personnel.
- Ensure that all data and guidance are available which are required to prepare to install, configure, maintain and operate the system securely.

Please note, that this Whitepaper does not replace any installation manual and user manual. It is meant to give the necessary information in a comfortable way.

In addition, the Security Whitepaper is intended to provide all information that may be required during the procurement and selection process for the Medical Product, thus avoiding the need for customer specific questionnaires.

2 Data Protection

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

The General Data Protection Regulation of the EU of April 27, 2016 which came into effect as of May 25, 2018 (GDPR) directs that the responsible person under Data Protection Law has to avoid the unapproved access to personal-related data (e.g. patient data) which he has received or collected. The responsible person in the sense of the Data Protection Law may not be only an individual but also a company.

This chapter will give you a short overview about some important passages of the GDPR.

Quoted pass ages of the GDPR are formatted in "*italic*".

Definitions in GDPR

(Chapter I, Article 4)

What does ‘personal data’ mean?

'personal data' means any information relating to an identified or identifiable natural person …, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

The GPDR lists some roles for the process of data protection and defines their responsibility.

Controller

“'controller' means the natural or legal person, …, alone or jointly with others, determines the purposes and means of the processing of personal data;…”

Processor

“'processor' means a natural or legal person, … which processes personal data on behalf of the controller;”

Recipient

“'recipient' means a natural or legal person, …, to which the personal data are disclosed, whether a third party or not.”

Principles

The GDPR defines some principles concerning how personal data should be collected and processed.

(Chapter II, Article 5)

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner ('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 on medical purposes

All kind of medical data concerning a natural person is under special protection by the GDPR. The following passage describes the basis of processing this kind of data.

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…"

Responsibility of the controller

In a dental practice or a dental laboratory the “Controller” of data protection is usually the legal entity that owns this practice or laboratory, respectively. In a dental clinic that might be a group of people. It is important to understand that the Controller is fully responsible to perform all necessary measures to fulfill the requirements of the GDPR.

Chapter I, Article 4

> *“'controller' means the natural or legal person, …, alone or jointly with others, determines the purposes and means of the processing of personal data;…”*

Chapter IV, Article 24

1. *“… the controller shall implement appropriate technical and organizational 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.”*

It is important to understand that the GDPR does not prefer either technical or organizational measures to perform data protection. In fact, technical measures will never fully replace organizational measures.

Data Protection Officer

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

This 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,…, 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, …, and to consult, where appropriate, with regard to any other matter.

3 Strategies and Best Practices

FOR DATA PROTECTION

This chapter gives some advice about best practices for organizational and technical measures and shows how CAD/CAM SW can support data protection.

Consent of patient

From a legal standpoint, the safest way to process personal data is to obtain the consent of the patient. The GDPR defines some rules how this consent shall be acquired.

(Chapter II, Articles 7,8)

- *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 other matters, in an intelligible and easily accessible form, using clear and plain language*
- *The patient has the right to withdraw his or her consent at any time. This must be possible as easy as to give consent.*
- *Where a child is below the age of 16 years, the processing of his or her personal data shall be lawful only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child. Member States of the EU may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.*

In particular, patient consent should not only be obtained to store and process patient data in the dental office but also to transmit necessary patient data to sub-contractors, i.e. the dental lab, in order to provide adequate treatment for the patient.

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.

Pseudonymisation / Anonymisation

Ensure patient data confidentiality by transmitting anonymised files or pseudonymised patient data, e.g. using patient IDs instead of names.

- Pseudonymise (if possible) patient data based already in the acquisition software. For example, use patient IDs from the Patient Management System (PMS) in CEREC SW, Connect SW, Ortho SW, prepCheck SW or inLab SW
- Pseudonymise patient data when using export functions to share with dentists or third party entities, e.g. laboratories. It is strongly recommended to use the Connect Portal for transmitting data to third party entities and take advantage of the individual anonymisation (on/off button) that is provided by Connect SW 4.6 and above as well as inLab 18 and above.
- When sharing data with customer support services anonymise data explicitly or use the “support-zip” export that provides automatic anonymisation for
    - CEREC SW 4.6.1 and above
    - Connect SW 4.6 and above
    - Ortho SW 1.3 and above
    - inLab SW 18.1 and above.

Confidentiality and integrity of data

Ensure the ongoing confidentiality and integrity of processing systems and services (Please also check the individual SW license agreement and terms of usage):

- Infrastructure
    - Use a firewall to protect the network
        - Grant access only as an exception (secure by default)
        - Limit internet access to a minimum
        - Update all network components (e.g. routers) regularly
        - Change standard passwords in all used network components
        - Limit internal network access and visibility to a minimum
    - Use a professional security software on all computers in the network → keep that security software updated constantly
        - Check all external drives (USB sticks, CD ROM etc.) with the security software
        - Let the security software check all websites and emails including attachments
    - Use remote maintenance with care
        - Check where and when remote maintenance is absolute necessary and allow access only on these workstations during the requested timeframe

- Set up a legal contract with service provider about remote maintenance
- Tip: Check authenticity of the service provider. You may ask for information only the service provider knows, e. g. your customer ID Monitor remote maintenance and record the process
- Tip: Record the remote session as video (that might need the consent of the service provider)

- Minimize access to workstations running CAD/CAM software
  - Set up an individual Windows login when using CAD/CAM SW (Make sure that this user has administrative permissions). Use strict guidelines for passwords (concerning length, the use of special characters and the frequency to change the password)
  - Instruct all users to logout as soon as a workstation is not needed for the moment or set up an automatic logout
  - Tip: Instead of a logout, you can also use the possibility to lock the workstation with a screensaver. Configure the screensaver to display the logon screen on resume.

- Connect Portal: Only business data supplied by participants is stored for the purpose to establish and document the business between the two legal entities. Patient specific data is only exchanged between the participants.
  - Ensure patient data confidentiality → Make use of pseudonymisation (see above) as there is an obligation to avoid and/or minimize the collection of data. For example, use abbreviations or reference numbers instead of the patient's name.
  - Explicit confirmation for linking to laboratories or central production facilities
    - Conclude an order processing contract with any third parties, e.g. laboratories or central production facilities, as this constitutes the delegation of data processing under the terms of Art. 28 GDPR. This article specifies extensive material and formal requirements e.g. a written agreement, regulations on data handling, defined supervision rights and obligations or the definition of subcontracting relationships. (This should include a subcontractor clause when work can be or is already partially done, e.g. only use a milling service)
    - Check existing terms of usage in existing order processing contracts with third party central production facilities, e.g. Invisalign or Dentsply Sirona Implants

- Use the multi user environment provided by Connect Portal

➔ Set up a different login for all people working with the Connect Portal. This can be done using the Connect Portal user management settings

- 3rd party software
  - Install and use 3rd party software only if this is necessary for the work in the dental practice
  - Use latest versions including all security patches

    ➔ Tip: Choose a security software, which informs actively about available security updates of 3rd party software

Availability of data

Ensure the ongoing availability and resilience of processing systems and services:

- Use the Hub for increased local availability and data backup
- If no Hub is used, manually increase availability by using an external redundant system that allows creating backups periodically: Backup your applications data path. The location can be found within the application under Settings / Configuration / Patient Database. Most ACs have “D:\Data” configured to be used as data path
- Set up an emergency plan for the case of data loss (e.g. caused by a crashed hard disc)
- Adjust user access control (UAC) on each Windows PC to at least level 3 (notification when programs try to make changes to computer settings), which is the default setting.
- Limit access to CAD/CAM SW and Connect Portal
  - Minimize access rights
- Manage access rights for the Connect Portal
- Use very strict guidelines for passwords (concerning length, use of special characters and frequency to change the password)
- Logout as soon as possible

Organisational measures

- Define a Code of Conduct concerning data protection in the respective dental practice or dental laboratory. Particularly taking different practice and laboratory settings into account, e.g. one owner or a shared ownership.

- Qualify your dental employees to follow this Code of Conduct
  - Save a record for each training for the employees
  - Choose only qualified employees (concerning expertise and reliability) for the processing of personal data
  - Employees, who are involved in the processing of personal data should be in a permanent employment (bound by contract)
- Create a Record of processing activities in your dental practice or laboratory

(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

(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.

Some important rights of the patients

There are some additional rights of patients concerning how to handle 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,…

  - Personal data can be erased by deleting the cases in the corresponding SW.
  - Any data transferred via the Connect Portal will be deleted automatically.
  - Beware, the right to erasure personal data does not overrule national laws for archiving medical data.
- *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,…

- CAD/CAM SW allows to export data in a readable format (PDF) with respect to SW-specific data. For example CEREC SW allows a case export (digital model of scan or design) whereas CEREC Ortho allows an export of the model analysis including treatment parameters.

- *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

  - Beware, this right does not overrule national laws for archiving medical data.

4 System Information

This chapter gives an overview of the technical system of CAD/CAM Software and provides all relevant information for IT administrators to decide how to place CAD/CAM Software into a secure system environment.

Brief overview of CAD/CAM SW:

Intended use, indication and contra-indication

This information is provided in the corresponding CAD/CAM SW user manuals

Approval

CEREC SW, Connect SW and Ortho SW bear the CE mark in accordance with the provisions of the Council Directive 93/42/EEC of June 14, 1993 concerning medical devices.

Intended operational environment

CAD/CAM Software is built to be operated primarily on Dentsply Sirona hardware. Each of the products can therefore be operated independently. Nevertheless, a more sophisticated usage is based on a working (wireless) local area network. The smooth and qualitative operation of a local area network requires uncompromising conformity of the building electrical installation with the internationally applicable basic standard ISO/IEC 11801 or with the European standard EN 50173 or the North American standard EIA/TIA 568 A which are derived from this basic standard. At the same time, all network connections of Dentsply Sirona hardware products, e.g. acquisition center, extra-oral scanner or milling machine, must be observed.

System Requirements

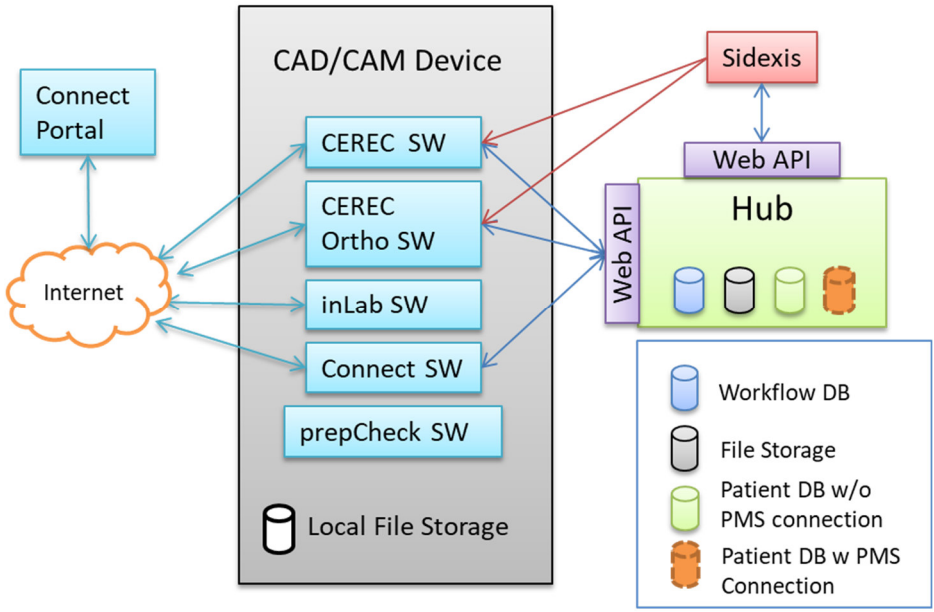
Please always check the latest system requirements in the corresponding user manuals or on: www.dentsplysirona.com

CAD/CAM SW Family

Technical Overview

The following diagram shows data flow and possible data exchange of

- CAD/CAM Software
  - CEREC SW (including CAM)
  - Connect SW
  - Ortho SW
  - inLab SW (including CAM CAM)
  - prepCheck SW
- Hub
- Connect Portal
- Sidexis



Software Components

CAD/CAM Software

CAD/CAM Software is usually installed on specific hardware devices running Microsoft Windows. There can be multiple installations on a single device sharing the same local file storage.

prepCheck SW

The prepCheck SW is an addon module for CEREC and Connect SW. Data is read from local storage or inter process communication protocols. Hence prepCheck is meant to be executed on the same device as CEREC or Connect SW.

Data Exchange

Connect Portal

The Connect Portal links dentist and dental laboratories via Sirona owned applications. The communication exchange between the involved parties is based on the state-ofthe-art implementation of TLS protocols, which uses 256-Bit secure hash algorithm (SHA256) using an asymmetric 2048-Bit RSA cryptosystem preventing downgrade attacks. The Sirona Connect Portal supports TLS1.1 handshakes, secure renegotiation and Online Certificate Status Protocol stapling.

The Connect Portal is hosted in a dedicated German Microsoft Azure Cloud and abides by the high standards of German law regarding data security and data protection, particularly the European General Data Protection Policy (EU GDPR) and the German Data Protection Law (BDSG).

Hub

There are several applications that support Hub communication:

- CEREC SW
- Connect SW
- CEREC Ortho SW

Hub offers Web API only. That is Hub communication is performed by using a REST like protocol. All communication is secured using an SSL based encryption with security keys that are individual to each Hub. Data stored on Hub is encrypted using individual encryption keys. Web API is secured using authorization and authentication protocols.

Sidexis

Sidexis provides REST like API for reading patient, media, and indications. For CAD/CAM SW and Hub only patient information is of interest.

There are two ways to integrate Sidexis patient database into CAD/CAM SW.

Direct communication

CEREC SW and CEREC Ortho SW can read patient data directly from Sidexis Web API. CEREC SW and CEREC Ortho SW can modify patient data if they don't origin from a SLIDA exchange.

Hub Patient Data Converter

Hub can connect to Sidexis reading patient data like CAD/CAM SW does. This information is stored internally and used for further integration of case and workflow integration. CAD/CAM SW that supports Hub communication is therefore able to read patient data that origins from Sidexis. Hub prevents other clients (like CAD/CAM SW) to alter patient data coming from Sidexis.

Third Party Software

Third party software here refers to software supplied by other suppliers (3rd party suppliers) with the system / solution or required to operate it. May be Off-The-Shelf Software (OTS) or Open Source Software (OSS)

Camera Driver MV Blue COUGAR 1.12.50

Camera driver used for Omnicam operation. Driver utilities can be found in the Windows start menu under MATRIX VISION/mvIMPACT acquire.

Acrobat Reader XI

Adobe Acrobat Reader can be found in the Windows Start Menu.

Team Viewer 12

Remote maintenance application can be found in the Windows Start Menu.

Auto Updater

An auto updater is provided on all systems. If an update is available, please follow the instructions to update the system.

Security Patching

- If security patches are necessary, the patches will be provided by Dentsply Sirona as a download in the restricted dealers area of the Dentsply Sirona website.
- Dentsply Sirona will inform dealers and subsidiaries worldwide about the patches and give instructions on how to install them.
- The patches will then be supplied by the local dealers or subsidiaries to the customers.

Sensitive Data

- CAD/CAM Software processes personal data of patients in terms of the "General Data Protection Regulation" like:
    - Name
    - Birthday
    - Digital Impressions
    - Intraoral photos or other pictures
    - Diagnostic findings and therapeutic information
- Furthermore, general data from Connect Portal users (dentists and lab) is processed for transmission:
    - Name and professional contact details (telephone, email, address etc.)
    - Job title
    - Possibly professional qualification

Adding comments to free-text fields

Free-text fields or comment fields are used to allow users to describe something in their own words. Entries should be factual and value-free.

Please do not use this free text fields and comment fields to add personal data e.g. patient name.

5 Legal Statement / Disclaimer

Legal Statement / Disclaimer

Please be advised that this Data Protection and Product Security Whitepaper cannot replace legal advice on how to fulfill the requirements of General Data Protection Regulation.

The author reserves the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims against the author, which refer to material or immaterial nature, which were caused by the use or disuse of the information provided or by the use of incorrect and incomplete information, are excluded, unless the author proves intentional or grossly negligent fault is present.