Planmeca Romexis Best Practices related to GDPR

Personal data processing guideline for Planmeca Romexis use

v.1.0 - 7th Jun 2018

GENERAL 2

RELATED PLANMECA ROMEXIS VERSION CHANGES 3

SUGGESTED WORKFLOWS RELATED TO CONFIDENTIALITY AND INTEGRITY OF DATA 4

Identity and Access Management **4**
- Access control 4
- Role-based access rights defined according to least privilege-principle 5
- Revocation of access rights 5
- Password quality 5
- Privileged access rights 6
- Authentication of users 6

Audit trail and log entries **6**
- Log Capabilities 6
- Log Management 7
- Right of access to log data 7

SUGGESTED WORKFLOWS RELATED TO SECURITY OF DATA 7
- Security of data processing 7
- Personal data breach detection and notification 8

SUGGESTED WORKFLOWS RELATED TO ACCURACY OF DATA 8
- Accuracy and keeping data up-to-date 8

SUGGESTED WORKFLOWS RELATED TO ERASURE OF DATA 8
- Erasure at the end of retention period 8

Right to erasure 9

SUGGESTED WORKFLOWS RELATED TO DATA SUBJECTS' RIGHTS 9
Access to data 9
Right to rectification 10
Right to portability 10
Right to restriction of processing 10

General

This guideline is intended to assist Planmeca Romexis administrative users in the configuration and use of the Planmeca Romexis software for patient data processing. The guideline provides suggestions on different workflows and configurations to use the software in a secure manner and in compliance with applicable legislation, in particular the EU General Data Protection Regulation (EU) 2016/679 ("GDPR"). The customer should pay particular attention to the GDPR whenever the customer is established in the EU or offers products or services within the EU or to EU individuals and processes personal data in such context.

In relation to the configurations and workflows in this guideline, the customer should pay attention to the fact that these best practices should be used not only to protect medical or patient data, but to protect **personal data,** meaning any information relating to an identified or identifiable natural person.

For the purposes of the GDPR, when using Planmeca Romexis for collecting and processing medical data about their patients, the customer will act as a controller. **Controller** means the entity that determines the purposes and means of the processing of personal data. As controller, the customer is responsible for complying with the GDPR and other applicable legislation on personal data protection and processing of medical and patient data.

These guidelines provide best practice guidance on how the customer may configure Planmeca Romexis to improve their level of GDPR compliance and may be used for improving compliance with other applicable legislation on personal data protection and processing of medical and patient data. The recommendations provided by this guideline complement the customer's organizational and technical measures and are not intended to create compliance as a sole control mechanism. Furthermore, these best practices require that the customer has implemented appropriate processes and transparency in its organization in relation to applicable data privacy rights. In the light of the EU GDPR, such key areas where the customer is responsible for ensuring compliance with and accountability are the following:

- **Lawfulness, fairness and transparency:** the customer has ensured that the processing of personal data is lawful and fair and it may only process personal data if it has an appropriate legal basis for doing so. The GDPR lists six legal bases for processing in Article 6 and a further ten legal bases

for special categories of personal data in Article 9. The principle of lawfulness, fairness and transparency further requires the controller to ensure that individuals (data subjects) are informed about data processing activities affecting them.

- **Purpose limitation:** the customer has ensured that personal data is collected and processed for pre-defined, specified, explicit and legitimate purposes. Personal data must not be further processed for purposes that are incompatible with those pre-defined purposes.
- **Data minimization:** the customer has ensured that it only collects and otherwise processes personal data that is necessary and relevant for the purposes for which it intends to process personal data.
- **Accuracy:** the customer has ensured that it keeps personal data correct and, where necessary, up to date in regard of the purposes for which it processes personal data.
- **Storage limitation:** the customer has defined retention periods and triggers for the personal data it processes. Having regard to national requirements, personal data must only be kept for as long as necessary for fulfilling the purposes for which the data are processed. When no longer needed for such purposes, personal data must be erased or rendered anonymous.
- **Integrity and confidentiality:** the customer has identified the technical and organizational measures securing the personal data, providing a baseline to guarantee that personal data is processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful use and against accidental loss, destruction or damage.

Related Planmeca Romexis version changes

The following Planmeca Romexis versions may include technical improvements that facilitate the controller in reaching GDPR compliance.

Version	Change	Impact
4.6.2.R	TLS encryption implemented in all traffic between Planmeca Romexis server and client.	Reduces probability that an intruder can eavesdrop patient data after having gained access to local network.
5.1.0.R	TLS encryption client certificate added. Allows customer to use their own client certificate.	Further reduces probability an intruder can eavesdrop patient data after having gained access to local network.

Suggested workflows related to confidentiality and integrity of data

Identity and Access Management

Requirement	Best Practice
Access control Controllers and processors have to implement measures to prevent unauthorized access and unlawful processing of personal data.	The customer must adopt user permissions in Planmeca Romexis to authenticate and authorise use. 1. Define user groups and their permissions to suit required access level of each user group. 2. Provide each user personal user account and password. 3. Attach users to the correct user groups. Note! Microsoft Active Directory can be used where available to centrally manage groups, users and their login credentials. Active Directory also works with PMS integrations using PMBridge so that PMBridge specifies patient in Planmeca Romexis and user is authenticated against Active Directory. API user authentication: PMBridge has a function “SetUser” that can be implemented by PMS to provide a new user with limited access to Planmeca Romexis. The “SetUser” functionality leaves an audit trail of who has accessed what data but it does not authorise the user and trusts the authorisation done by the PMS. The user and group used by PMBridge must be configured correctly to limit users' access to for example read/write access to currently open patient only. Note! Planmeca does not have any default access to information stored by Planmeca Romexis. Any access to customer systems by remote desktop or other means by Planmeca or its distributors shall be agreed upon separately.

Role-based access rights defined according to least privilege-principle Access to ICT environments containing personal data is role-based and granted when necessary for the performance of duties. Access rights are changed upon change of role or task to reflect the new role/task. Scope of access rights granted to certain roles are defined according to least privilege principle. In relation to medical data, there may be national and sectoral requirements setting specific requirements that define more specifically the roles entitled to process medical data.	The customer is responsible for defining the roles on which access rights are based. Please note that default installation of Planmeca Romexis sets up an admin level default login to allow configuration of the system to meet local requirements. Suitable admin user, groups and permissions should be set up before the software is used to process personal data. See previous item on users and groups.
Revocation of access rights Access rights of all employees and external users to systems processing personal data are removed upon termination of employment or third party contract. It should be noted that although access rights must be removed, it may be necessary to maintain the accounts in order to keep audit trail intact.	The customer is responsible for defining and enforcing an Identity and Access Management process that ensures revocation of unnecessary user accounts and access rights. Access rights can be revoked by inactivating the user in Planmeca Romexis Admin module. Note that inactivating a user revokes all access to the software for that user but it does not remove the personal data or audit trail information related to that user stored in the database. When Active Directory is used, the validity of user access rights is checked at every Planmeca Romexis login.
Password quality System must support password quality settings for all passwords. E.g. administrative and also user passwords.	The customer is responsible for ensuring adequate password quality. The following password quality requirements can be set in Planmeca Romexis Configuration application: • Maximum age • Minimum length • Maximum retries • Require at least one digit • Require at least one special character

Privileged access rights Allocation and use of privileged access rights to systems processing personal data is restricted and controlled.	The customer is responsible for ensuring separation of duties so that clinical users do not have admin rights by defining authentication criteria and enabling authentication of users with correct privileges in Planmeca Romexis.
Authentication of users Medical data may be processed only by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies	The customer is responsible for defining authentication criteria and for enabling authentication of users in Planmeca Romexis.

Audit trail and log entries

Requirement	Best Practice
Log Capabilities Log capabilities should be in place in order to identify attacks to personal data assets and to provide accountability over unauthorised use, disclosure and modification of personal data. The details of log capability and management depend on the sensitivity of the data processed. As medical data is treated as highly sensitive data in the GDPR and in most data protection regimes, log capabilities must reflect this.	The customer is responsible for defining a log policy. Planmeca Romexis creates a high level audit trail entry in its database for starting the client, opening a patient's file, and for exporting and printing data. Additionally, every modification to data is logged in detail (timestamp + identity of modifier). The audit trail entries can be connected to an individual user only if: • individual user accounts are created in Planmeca Romexis; • Active Directory user accounts are used for Planmeca Romexis; or • PMBridge SetUser command is used to specify who is currently accessing the Planmeca Romexis session If none of the above alternatives are implemented, the audit trail does not identify the individual accessing/modifying the data and will not provide accountability. **For accountability reasons, individual user accounts must be made default so that audit trail entries can be used to identify the individual user.**

For example, the Finnish legislation concerning patients' right to data protection in regard to their medical data provides that all activity (read, modify, delete) are logged, and that the log entry identifies the patient, the individual accessing/modifying the data, the action performed on the data, and the time it was performed.	
Log Management Logs must be protected from unauthorized access and tampering.	The customer is responsible for log management. Audit trail entries are currently stored in Planmeca Romexis database and can be viewed with correct user rights that allow access to the audit trail report in the Report Module in Planmeca Romexis client. The report allows view only access to the audit trail. Planmeca Romexis server and database admin access must be adequately limited to prevent unauthorized access to and tampering of the audit trail in the database.
Right of access to log data	The customer is responsible for responding to the patients' access to logs requests. Planmeca Romexis provides a report for listing high level log events and the database can be reported using 3rd party tools to retrieve detailed modification history.

Suggested workflows related to security of data

Requirement	Best Practice
Security of data processing Appropriate technical and organisational measures must be implemented by the Controller and the Processor to ensure a level of security appropriate to the risk to rights and freedoms of individuals caused by the processing.	In the current deployment, ensuring the security of processing is the responsibility of the customer. This encompasses not only the definition and adoption of overall technical and organizational security measures to protect personal data, but also the appropriate deployment and configuration of the Planmeca Romexis solution. Security of the current deployment is described in the Planmeca Romexis Application Security Assessment Report. When configured correctly, the security status of the Planmeca Romexis client and server is **good** in version 5.1.0.R. No high or medium severity vulnerabilities were found in an assessment of this version.

Personal data breach detection and notification In case of a personal data breach, controller must notify the breach to the competent supervisory authorities within 72 hours after having become aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.	The customer is responsible for ensuring that it has the capability to detect personal data breaches. The customer is responsible for notifying a personal data breach to the relevant national supervisory authorities when it becomes aware of it.

Suggested workflows related to accuracy of data

Requirement	Best Practice
Accuracy and keeping data up-to-date Personal data must be accurate in regard to the purposes for which they are processed and, where necessary, kept up to date.	The customer is responsible for defining and maintaining a process for keeping data accurate and up-to-date. Planmeca Romexis enables adherence to this principle by making it possible to modify patient and user data. When Planmeca Romexis is not the primary patient record, information processed in it is usually automatically updated by the master patient record (patient management software) using update call issued via the PMBridge integration library when the patient is accessed. In such cases, Planmeca Romexis should not be relied upon as the primary source of patient data.

Suggested workflows related to erasure of data

Requirement	Best Practice
Erasure at the end of retention period	For the purpose of the GDPR, the customer has the responsibility to define the retention periods for all personal data, whether related to patients or users. Although the retention period for dental images may be very long, it is not indefinite in most jurisdictions.

Personal data must be 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. This means that at the end of its lawful retention period, personal data must be permanently erased or irreversibly anonymised.	Personal data such as users and their history can be permanently erased only by directly accessing Planmeca Romexis database. Database access requires admin user rights. Planmeca Romexis is usually not the primary patient record and does not have primary information about new patients or users and their expiry. Therefore it is not feasible to implement automatic data erasure in Planmeca Romexis. It is recommended to deploy a 3rd party data erasure or anonymisation tool that allows erasure of all data related to a patient or user when that entity is to be permanently removed from the system.
Right to erasure Under certain circumstances, data subjects have the right to have their data erased by the Controller.	See previous section "Erasure at the end of retention period".

Suggested workflows related to data subjects' rights

Applicable data subjects' rights vary in different national, regional or sector specific legislations. The customer as controller is responsible for defining the scope and applicability of different rights to their processing activity. The functionalities of Planmeca Romexis described below support the customer in executing data subject requests. The following table describes the most relevant rights provided in the GDPR applicable to personal data use in Planmeca Romexis. The right to erasure is covered in the previous section and the right to information and transparency is solely the responsibility of the customer.

Article 15 GDPR	
Requirement	**Best Practice**
Access to data Data subjects have the right to know when their data is processed, and to have access to that data. Medical data may be subject to specific requirements regarding to access rights in many jurisdictions that may further define the way in which access to data must be provided.	The customer is responsible for assessing the applicability and scope of the right in Planmeca Romexis, and for responding to data subjects' access requests. Planmeca Romexis allows generation and printing of reports for basic data. Full audit trail of changes to data is maintained in the database and can be reported using 3rd party tools.
Article 16 GDPR	

Right to rectification Data must be kept up-to-date, and in addition data subjects have the right to have their data rectified when it is outdated or invalid. Rectification of medical data is often subject to specific requirements in many jurisdictions.	The customer is responsible for assessing the applicability and scope of the right in Planmeca Romexis, and for responding to data subjects' access requests. Planmeca Romexis allows editing of patient data which should only be used when it is the primary patient database. When Planmeca Romexis is used together with patient management system (primary patient database) the patient management system is responsible for updating information in Planmeca Romexis using the integration SDK calls when the patient is requested to be opened.
Article 20 GDPR	
Right to portability The GDPR provides data subjects the right to receive their personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. The right only applies to data supplied by the data subject to the controller, and not to data obtained by the controller from other sources.	The customer is responsible for assessing the applicability and scope of the right in Planmeca Romexis, and for responding to data subjects' access requests. Planmeca Romexis allows generation and printing of reports for basic data. Images can be exported in standard DICOM standard including patient personal data.
Article 18 GDPR	
Right to restriction of processing In certain circumstances, data subject has the right to have the controller restrict the processing of their data.	The customer is responsible for assessing the applicability and scope of the right in Planmeca Romexis, and for responding to data subjects' access requests. It is possible to inactivate patients in Planmeca Romexis admin module which prevents further changes to the data.

END OF DOCUMENT