Cartagenia Data Security & Confidentiality Policy

Document title	Cartagenia Data Security & Confidentiality Policy
Version number	V06 (☐ draft ☑ for release)
Publication date	2014-01-06
Authors (* primary)	BCO(*), SVV, HVE, GJA, LEW
Document type	☐ agenda ☐ agreement ☐ contract ☐ letter ☐ memo ☐ minutes ☐ paper ☑policy ☐ procedure ☐ report
Intended audience	☐ Internal and confidential ☑ prospects and customers ☐ public

Contents

Cartagenia Data Security & Confidentiality Policy 1
Contents 1
Document scope 2
Introduction 2
Process 2
Data ownership 2
Confidentiality 2
Platform maintenance & support 2
Customer data protection and backup 3
Customer data security 3
Product 4
Quality Management System 4
Authentication & Authorization 4
Technology 4
Authentication implementation 4
Authorization implementation 5
Logging & audit trails 5
Encryption 5
Production environment & security 5
Internal references 5
External references 6

→ Technologielaan 3
B-3001 Leuven - Belgium

→ T +32 16 40 40 66
F +32 16 40 20 66
info@cartagenia.com

→ VAT BE.0807.353.962
RPR Leuven
IBAN BE72 7343 0040 0016 - BIC KREDBEBB

Document scope

This document describes the measures Cartagenia takes to keep its customers' data secure and confidential, both on a process and product level. This document complements the Cartagenia Software Business Associate Policy documentation and is an integral part of Cartagenia's ISO13485:2003 Quality Management System.

Introduction

Process

Data ownership

Cartagenia's customers control the PHI (protected health information) entered in and submitted to the Bench platform. Cartagenia acts as a data processor and does this processing on behalf of its customers – in no way is ownership of the data transferred. This setup is in line with European (the European Data Protection Act), US (the Privacy Rule of the Health Insurance Portability and Accountability Act), and Canadian (Personal Information Protection and Electronics Regulations Act and Personal Health Information Protection Act (Ontario)) regulations on patient data processing.

When transferring PHI (protected health information) from and into Cartagenia software tools through 'front end' access (i.e., through regular use by the customer's identified users through Cartagenia forms, wizards, portals and other user interfaces), data transfer is encrypted using industry standard encryption technology (Secure Socket Layer, discussed below). Access to data is protected by an access-rights-based login system. All data are maintained within a dedicated and protected database that is specific and private to the customer as a Covered Entity.

When providing PHI information to Cartagenia via another way than through using the Bench platform, e.g., for purposes of performing bulk loading of data sets to the Bench platform, all received data will be removed or returned to the customer after processing and loading of the data. The only copy of the data accessible to Cartagenia will be in active storage in the customer's Bench platform instance where access to it will be subject to the rules defined in section 'Platform maintenance & support'.

Upon termination of the contract with Cartagenia all PHI information in the Bench platform databases is returned to the customer and removed from Cartagenia's active storage in accordance to the Cartagenia Software Business Associate Policy. Backups of the information might still exist and kept in Cartagenia's offline storage facilities.

Confidentiality

Cartagenia commits to keep confidential all confidential information received from its customers and to protect the confidentiality thereof in the same manner as it would protect the confidentiality of its own confidential information. All Cartagenia employees and subcontractors are bound by a confidentiality clause present in their respective employment and subcontractor agreements.

Platform maintenance & support

As a general rule no Cartagenia personnel will access any proprietary or confidential data from a customer, except with the customer´s written consent (e-mail or otherwise) or if the customer explicitly requests a task from Cartagenia that requires having access and actively using or disclosing data or information provided by the customer.

- **Support user access** - Cartagenia authorized Help Desk personnel can acquire front-end access to hosted Bench platform instances through a specifically authorized support user account/profile.
    - The support user is an administrative user who is not authorized to access any of the available patient records in the platform and, hence, cannot access any patient information available in the platform.

- The support user can be used to access administrative functionality in the platform to resolve issues or help with configuration.
- If necessary and only after written consent is received from the customer, the privileges of the support user can be temporarily heightened to allow access to a specific patient record and the information herein.
- All access to the platform and information within is always logged and auditable.

- **Back-end access** - Cartagenia authorized Help Desk personnel can acquire back-end access to the databases underlying the hosted Bench platform instances. Back-end access is only granted from within Cartagenia's offices at the registered Cartagenia business addresses and is limited to a number of authorized Cartagenia employees only. All back-end communication is fully encrypted using industry-grade 256-bit encryption. Back-end access can happen in following situations:
  - Upon initial configuration of the Bench platform for the customer.
  - Upon bulk loading of historical or other data sets in the customer's Bench platform.
  - When a Help Desk call requires access to information or configuration in the Bench platform database or back-end.
  - Upon performing Bench platform maintenance or migration work (e.g., in case of updating the platform to a new release, in case of migrating the platform to a new genome build, etc.).
- **Protected information** - In case protected information is handed over to Cartagenia authorized Help Desk personnel, the information is accessed to perform any work requested and required by the customer. After the required work has been performed the data are removed from any local storage or returned in full to the customer (see also Section 'Data ownership' and 'Customer data security').

Customer data protection and backup

Any file uploaded to or created by the Bench platform is immediately replicated across multiple devices located within multiple data centers. The file storage system is designed in such a way that it can survive the outage of at least 2 of these data centers. A combination of MD5 checksums and cyclic redundancy checks is used to detect file corruption. Files at rest are also regularly checked for corruption. The system is able to quickly detect and repair any loss of redundancy, thereby being able to sustain multiple concurrent device failures. Every change to a file, even a delete, results in the creation of a new file or delete marker, while all previous versions of that file are maintained. This ensures that it is always possible to retrieve any version of any file.

A daily snapshot is made of all database servers and kept for a period of at least 30 days. This snapshot is durably stored using the same storage system our regular files are stored on. Additionally, starting from the last snapshot time, every 5 minutes the database transaction logs are backed up, allowing point-in-time restores to no longer than 5 minutes in the past. This ensures that data loss is limited to data entered or updated by the user within the last 5 minutes. Should it be necessary to dig further into the past, monthly snapshots are also preserved.

Customer data security

Customer data are only kept outside of the Cartagenia production environment for as long as necessary, e.g., to perform data manipulation and processing. Cartagenia takes following measures to keep customer data secure:

- All computers of Cartagenia personnel authorized to work with customer data are password protected and are configured with auto-lock after 5 minutes of inactivity.
- Transfer of customer data via open networks is performed using industry-grade 256-bit encryption (secure copy (SCP), secure file transfer (SFTP), HTTPS). If a customer needs to transfer data to or from Cartagenia, Cartagenia will only accept transfer of the data via its dedicated secure file transfer service (Amazon AWS S3).
- Transfer of customer data via unprotected mobile storage devices (e.g., mobile hard disks, USB storage, etc.):
  - is strictly limited to internal transfer of data -
  - mobile storage devices carrying customer data will remain at all time within Cartagenia's premises;
  - all customer data are removed from the storage device as soon as the transfer is complete.

Product

Efforts are taken to ensure Cartagenia products comply with the needs and requirements set forth by the compliance policy as well as with best practices in software and databases that process and store PHI information. This means technical measures are put in place to ensure data security and confidentiality (such as authentication and authorization for access control, encryption, audit trails and production environment security), and equally, that a well-defined process is put in place for software development, testing and release, and that this process is governed by a quality management system. These aspects are introduced below.

Quality Management System

Cartagenia's commercially available software and services are being developed, maintained, and serviced according to the procedures in Cartagenia's ISO13485:2012 Quality Management System. Cartagenia's Quality Management System aims to:

1. Guarantee product conformance and safety;
2. Efficiently solve problems and complaints;
3. Increase customer satisfaction;
4. Enable continuous learning and improvement;
5. Comply with the regulatory and statutory requirements.

Authentication & Authorization

Technology

The Bench platform security system is implemented using the Java-based Spring Security library. Spring Security is a powerful and highly customizable authentication and access-control framework and the *de facto* industry standard for securing Java web-based applications. It is one of the most mature and widely used stacks, used to secure numerous demanding environments including government agencies, military applications and central banks.

Authentication implementation

- **Platform access** - Bench platform user accounts are personal and should only be used by the person it is appointed to. Only one concurrent authenticated session is granted to a user account. If the platform is accessed from multiple locations with the same user account, the oldest session is automatically destroyed and the user logged out.
- **Password protection** - Logging in to the Bench platform requires the use of a password.
    - At platform setup, or when a passwords needs to be reset, a temporary password is provided by Cartagenia. This temporary password is only valid for 12 hours and needs to be changed upon first log on with the respective user account. If the password is not changed within this period of the time, the user account is disabled.
    - Only strong passwords are accepted. A strong password is defined as a string that contains at least 8 characters consisting of upper case and lower case characters, as well as at least one numerical character, and at least one special character.
    - Three failed log in attempts (i.e., log in with a wrong password) automatically result in disabling of the user account. Only Cartagenia authorized Help Desk personnel can re-enable the account and reset its password.
    - Lost passwords cannot be recovered. Passwords are stored in the Bench platform in an encrypted format (one-way encryption or 'hashing') and cannot be seen in clear text.
- **Session time-out** - Authenticated sessions are automatically destroyed and the user logged out after 30 minutes of inactivity. This is to avoid unauthorized access to the Bench platform via a computer that is left unattended.

Authorization implementation

- **User types** - Three types of users are available in the Bench platform. Each user type has a different set of privileges:
    - **Read-only user** - A read-only user is a regular Bench platform user with no write permission, i.e., he/she cannot change any information in the platform, only visualize it if in projects he/she has access to. The user does not have access to the platform Administration pages.
    - **Read/Write user** - A read/write user is a regular Bench platform user with both read and write permissions, i.e., the user can change information in the platform within the projects he/she has access to. He/she does not have access to the platform Administration pages.
    - **Administrator** - An administrative user has full access to all functionality in the platform.
- **Project-based authorization** - In Bench a project-based authorization system is in place. A user either has or has not access to a project. If the user does not have access to a project no assay and patient information available in this project can be accessed and visualized: nor directly, nor in searches, nor in advanced analyses.
- **Other types of authorization** - More granular authorization for both access to information in the platform as well as platform functionality can be set up upon request.

Logging & audit trails

The application level security of Cartagenia Bench is based on individual user access accounts. On top of the authorization system, a logging and auditing system is in place. Every user has a unique access code, and all major operations this user performs on the system are logged in an audit trail. Detailed activity logs are recorded so that reports can be made to see who performed an operation at what time and what data were accessed, etc. These data are tracked, logged, and stored in a central location for extended periods of time.

Encryption

Server authentication and communication with a private Bench platform installation hosted by Cartagenia is protected using industry-grade 256-bit encryption. Encrypted communication is enforced, no un-encrypted communication is possible. Cartagenia's SSL certificates for server authentication and data encryption are issued by an international and widely-recognized Certification Authority and are hence recognized by most common and recent web browsers.

Production environment & security

Cartagenia's production servers run in highly-secured and fully HIPAA compliant data centers in Europe, the United States, and Australia.

Following network access to Cartagenia's production hosting environment is allowed:

- HTTPS over TCP/IP access from anywhere; this global access can be restricted upon request to the customers' premises or computer infrastructure.
- SSL access ONLY from within Cartagenia's offices and only by authorized Help Desk personnel.

No other server ports are accessible from anywhere; an active firewall blocks all requests *not* directed to port 22, 80, 430. Port scanning and ping requests are actively blocked.

Dedicated database servers backing the Bench platform are only accessible from servers in the production hosting environment and are locked down to only accept valid and encrypted database connections.

Internal references

- Internal contact / Security official: Bert Coessens <bert.coessens@cartagenia.com>
- Cartagenia Software Business Associate Policy
- Cartagenia Quality Manual
- Cartagenia ISO13485:2012 Quality Management System
- Cartagenia Bench Platform technical file
- Cartagenia Services Terms & Conditions

External references

- HIPAA Act
- European Data Protection Act
- Canadian and Ontario PIPEDA and PHIPA Acts
- Amazon Security & Compliance:
  - http://aws.amazon.com/security/
  - http://aws.amazon.com/compliance/