the patient safety company®

INFORMATION SECURITY

COMPLIANCE TO INTERNATIONAL STANDARDS

Version	1.4
Date published	18 June 2012
Last modified	22 January 2013
Author(s)	J. Sijm

Table of Contents

INTRODUCTION

Information security statement

The Patient Safety Company (TPSC) acknowledges the importance of information security and privacy of data. TPSC is fully committed to reduce potential risks and to take all necessary measures within its power in order to guarantee data availability and to provide secure process data management and storage.

This document sets out a framework of governance and accountability for information security management. It forms the basis of an Information Security Management System (ISMS) to protect The Patient Safety Company's and its client's data by maintaining:

- Confidentiality: protecting information from unauthorized access and disclosure
- Integrity: safeguarding the accuracy and completeness of information and preventing its unauthorized amendment or deletion.
- Availability: ensuring that information and associated services are available to authorize users whenever and wherever required.

An effective Information Security Management System is essential to:

- Ensure our business continuity.
- Protect our intellectual property rights, financial interests and competitive edge.
- Protect our clients' process data.
- Safeguard the interests and privacy of our clients, staff and other stakeholders and retain their trust.
- Comply with the law and defend ourselves against legal action.
- Maintain our reputation.

Governance and Responsibilities

All employees of The Patient Safety Company are responsible for complying with the information security policy:

- Ensuring that no breaches of information security result from their actions.
- Reporting any breach, or suspected breach of security.

The **senior management** is accountable for information security, and for actively supporting security within The Patient Safety Company through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

The **Research and Development department** is responsible for implementing and improving the security measures, within software and infrastructure.

The **Executive Management** is responsible for setting the strategic vision; ensuring information security is secured in procedures and process.

The **Director of Human Resources** is responsible for ensuring that day to day responsibilities for maintaining information security are identified within the job descriptions of individual posts and embedded in induction, training, and reporting accountabilities.

Each customer of the TPSC Cloud™ is responsible for:

- The accuracy, quality and legality of Process Data and of the means by which customer acquired Process Data.
- Using commercially reasonable efforts to prevent unauthorized access to or use of TPSC Cloud™.
- Notifying TPSC promptly of any such unauthorized access or use.
- Preventing the use of TPSC Cloud™ to store or transmit Malicious Code.

One of the most important concerns, besides securing our own process and management controls, is selecting our **Third Party Providers, Hosting partners**. Our hosting partners have all been selected carefully to ensure 24x7 availability and to comply with international and local standards for the region or country. Certifications and audit reports can be shared on request and by signing a Mutual Non Disclosure Agreement with the hosting partner.

The following chapters will describe the main controls and measures regarding:

- TPSC Organization:
  - Confidentiality
  - Business continuity
  - Logical security
  - Physical security
  - Security Incident Management
- TPSC Cloud™ Security
- Third Party Providers – Hosting partners

Before you proceed with reading this document don't forget:

Information security is <u>EVERYONE'S</u> responsibility!
The Patient Safety Company, it's Employees AND Clients!

Yours sincerely,

Niels Greidanus
CEO
The Patient Safety Company

TPSC ORGANIZATIONAL CONTROLS

Confidentiality

The Patient Safety Company requires all employees to act in a professional and ethical manner to assure a high quality of product and services. Different measures and controls have been established to minimize the risk of violation of confidentiality policies.

Screening of personnel

All staff are screened during the job application process. Screening includes:

- Availability and check of positive references, minimum of two;
- Check of completeness and accuracy of the curriculum vitae of the candidate;
- Confirmation of educational background, prior relevant experience, past accomplishments;
- Identity check (passport or similar document);
- Declaration of Good Behavior.

Confidentiality agreements

All staff are required to sign a confidentiality agreement to prevent any disclosure of confidential information of clients, including patient information. In case of an incident with the proven involvement of employee TPSC will take the necessary disciplinary measures.

Termination of a work relationship with an employee will not affect the confidentiality agreement.

Return of assets

All assets given to employees are tracked in the asset management system. When a contract is terminated the employee will be obligated to return all assets.

Business continuity

Healthcare organizations operate 24 hours a day, 365 days a year. The Patient Safety Company will, at any time of the day, always be ready for you, so your round the clock care will not be disrupted. The Service Level Agreement is part of your subscription for the TPSC Cloud™, at no additional cost!

Service levels

The Service Level Agreement consists of:

- Constructive and Preventive Maintenance - The TPSC Cloud™ is periodically updated, you always have the latest release and version available.
- Corrective maintenance - If an error occurs in the TPSC Cloud™, availability of service or software error, we will solve this within the SLA, including 24x7* in case of a critical system error.

Customers who experience an error in the TPSC Cloud™ are requested to report this immediately to TPSC.

The service level applicable will be determined by the impact of the error as shown in Table 1. The client is obliged to provide all required and requested information, necessary for error recovery, to TPSC.

Scheduled preventive and constructive maintenance, updating of the TPSC Cloud™, will take place after (local) business hours. In case of critical errors TPSC can make an exception.

New releases or versions may affect the business process. At your request TPSC will inform you about the advantages and disadvantages of the new release or version. Maintenance does not include the implementation of new functionality or answers to "what and how" - questions. Additionally a support contract or package can be purchased from us or one of our agents.

If an error appears to be a configuration issue, TPSC will invoice the work on a time basis or if they are available, book the hours against the support contract or package.

When reporting an error the following information must be completed:

- Coordinator / contact information, customer name, email and direct telephone number.
- Details of the environment: domain, URL, and app.
- The Priority Code applies in principle to the error.
- Expected result and actual result.
- Description of the error or error-log and how to reproduce the error.
- Part of the application where the error occurred (app, screen, menu, or signaling, etc.).
- Clear screenshot (s).
- In the case of multiple errors these should be submitted separately, otherwise they will not be processed.
- Other details that can help to isolate the fault (eg reporting of recently installed applications that can cause this behavior).

** The TPSC service engineer on duty will be automatically alerted by the TPSC Cloud™ in case of a critical system failure, such as unavailability of the TPSC Cloud™.*

The following Priority Codes and Service Levels apply to maintenance and the reporting of errors.

Priority Code	Description	Service Levels	Comments
1	The Product cannot be used; the Error has a critical impact on the business process. A Bypass is not available; the situation requires an immediate solution.	Response time 30 minutes, 24/7 (automatic notification). TPSC will take those actions, which will possibly lead to a solution as soon as possible. TPSC will strive to provide a solution within 4 (four) hours. If a Bypass is provided parties will give the Error a lower Priority Code.	Critical system failure: • System not available. • Unable to report.
2	The use of the Product is limited; certain functions cannot be used. A Bypass is available; the situation requires a solution as soon as possible.	TPSC will take those actions, which will possibly lead to a solution within 5 business days. TPSC will strive to provide a solution within one business day. If a Bypass is provided parties will give the Error a lower Priority Code.	• File cannot be closed • E-mails not being sent • Empty dashboard • Glitches in Reports
3	The Product is operational; the use of several functions has minor restrictions. A Bypass is available allowing business process to continue.	TPSC will take those actions, which will possibly lead to a solution as soon as possible. TPSC will strive to provide a solution within 15 business days.	Other, i.e.: • Unable to open file from dashboard, but can be opened through data grid • Form only accessible through direct link • Audit trail not displayed

Table 1: Service Levels.

Back up and recovery

To secure its own business process TPSC is performing a daily back up of all its own critical business data. A back up is collected weekly by a secured data transport and storage company, which is ISO 9001:2008 and ISO 27001:2005 certified.

Back ups are available 24 hours a day on demand and can be restored instantly when needed.

The back-up policies of our third party services providers, hosting partners, who are storing your client data, are stated in the chapter 'Third Party Services'.

ESCROW

The TPSC Cloud™ brings quite some advantage compared to traditional software licensing like, eliminating the need to install and run the application on the customer's own infrastructure and alleviating the customer's burden of ongoing operation and support.

However, along with these potential advantages comes an element of risk. Supplier failure or poor service and availability could seriously affect an organization's business continuity and its ability to carry out everyday

operations.

In order to ensure that TPSC Cloud™ is protected against such risk, TPSC pays its third party supplier (hosting partner) three months in advance to ensure that the TPSC Cloud™ will be operational even in case of bankruptcy of TPSC. Beside this, an organization can even consider our Escrow solution to reduce the risk and protect its investment in the TPSC Cloud™. If our business fails or we cannot maintain our contractual obligations, the required application and data will be accessed and released or provided to your organization quickly and legally, leaving your organization free to carry on without disruption.

Return of process data

Within 30 days after the effective date of termination of a subscription contract, Customer can make a request to TPSC to return its process data. TPSC will make available to Customer a database dump, including attachments in their native format. After such 30-day period, TPSC shall have no obligation to maintain or provide any of process data and shall thereafter, unless legally prohibited, delete all of Process Data in TPSC's systems or otherwise in TPSC's possession or under TPSC's control.

Logical Security

TPSC has taken all necessary logical security measures to eliminate the risk of unauthorized access to its internal network. Each employee has a specific username and password. The password must be of certain strength and has to be renewed each month. Based on the employees responsibilities access is granted to specific parts of the TPSC Network and specific applications, for example the Electronic Password Safe.

The Patient Safety Company internal network is restricted to external access by network security devices (firewalls). The Wi-Fi and VPN access codes are periodically changed

TPSC supports different authentication methods to access client networks (only applicable in case of private cloud), which need to be provided by the customer:

- Token Authentication - small devices that authorized users of computer systems or networks carry to assist in identifying that who is logging in to a computer or network system and is actually authorized to do so.
- Password Authentication – Password Authentication uses secret data to control access to a particular resource.
- Two-Way Authentication - involves both the user and system or network convincing each other that they know the shared password without transmitting this password over any communication channel, for example Kerberos.

In case of a contract termination, employee will be obligated to return its ID badge to prevent entrance to the location. User ID's and passwords are inactivated to prevent access to the TPSC Network and client data.

If your organizations security information policy requires an additional confidentiality agreement to be signed by TPSC, we'll fully cooperate with this.

Physical security

The office location is protected by an ID badge security system and an intrusion detection system. All personnel have ID badges that ensure that they are authenticated in the correct manner. Access to specific rooms is granted based on job function and responsibilities.

If an active badge becomes misplaced or broken, the badging officer is notified so it can be removed from the system. The holder of the badge will then be issued a replacement badge and may be required to update their badge request form.

Access to and administration of the badge system is restricted to authorized personnel based on job responsibilities. Upon notification of employment termination, the badging office removes the physical access of the terminated party.

The office building is equipped with a, yearly certified, fire detection system and fire extinguishers according Dutch laws. Business critical documents are stored in fireproof safes. The Patient Safety Company has building insurance to insure continuity in case of a flood or fire.

Tokens, and other physical authentication hardware are stored in a safe and only accessible to authorized personnel.

Vulnerability Report

Security Incident Management

The Patient Safety Company encourages the reporting of any potential vulnerability or security (near) incident. Keeping your data secure is our top priority. Any information that might help us to improve our service and security is appreciated. We're very willing to work with you to respond to any potential vulnerability.

Incidents can be emailed to servicedesk@patientsafety.com. Please provide full details of the vulnerability or incident to help our technical team to validate, reproduce and solve the issue.

Each report will be filed in our security incident management system and analyzed. Reporters will be notified about the actions taken and closure of case.

The Patient Safety Company will, in case of intentional harm, prosecute any organization:

- Causing, or attempting to cause, a Denial of Service (DoS) condition.
- Accessing, or attempting to access, data or information that does not belong to you
- Destroying or corrupting, or attempting to destroy or corrupt, data or information that does not belong to you

TPSC CLOUD™ SECURITY

TPSC Cloud™ Security

The TPSC Cloud™ software offers different features to assure that your data is completely secured. Each customer with access to the platform is responsible for its own users and access controls to the TPSC Cloud™.

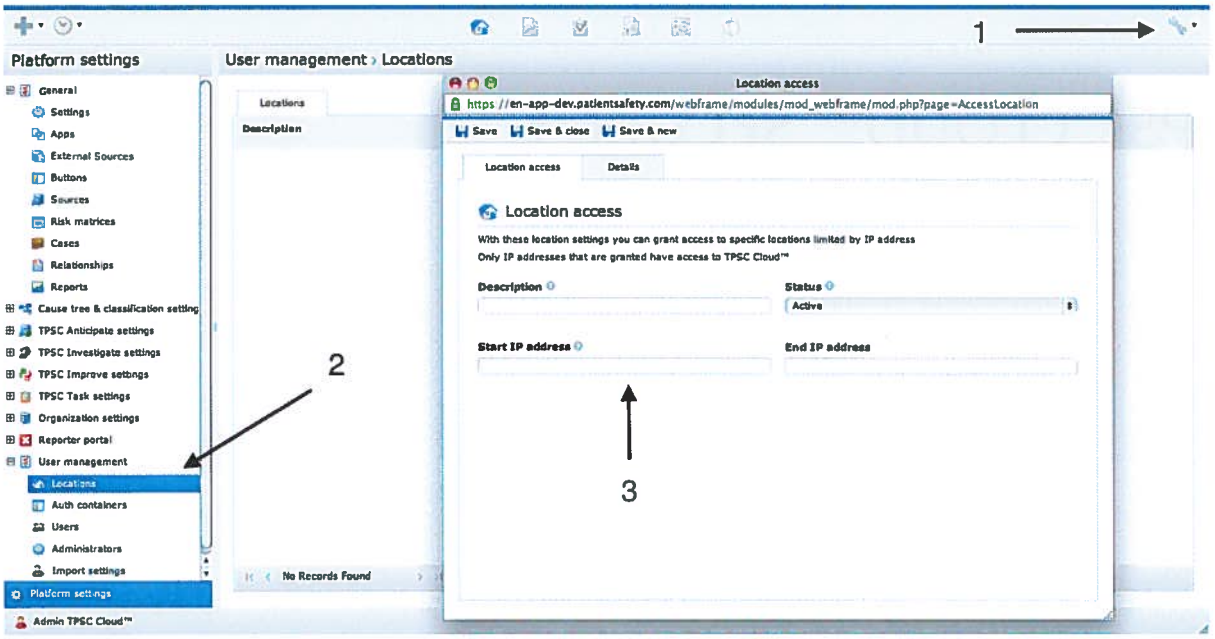
Below you'll find an overview and description of the available security features.

IP Blocking

A great tool for protecting your applications is to restrict login to those IP addresses that you specifically approve.

To restrict IP addresses, click:

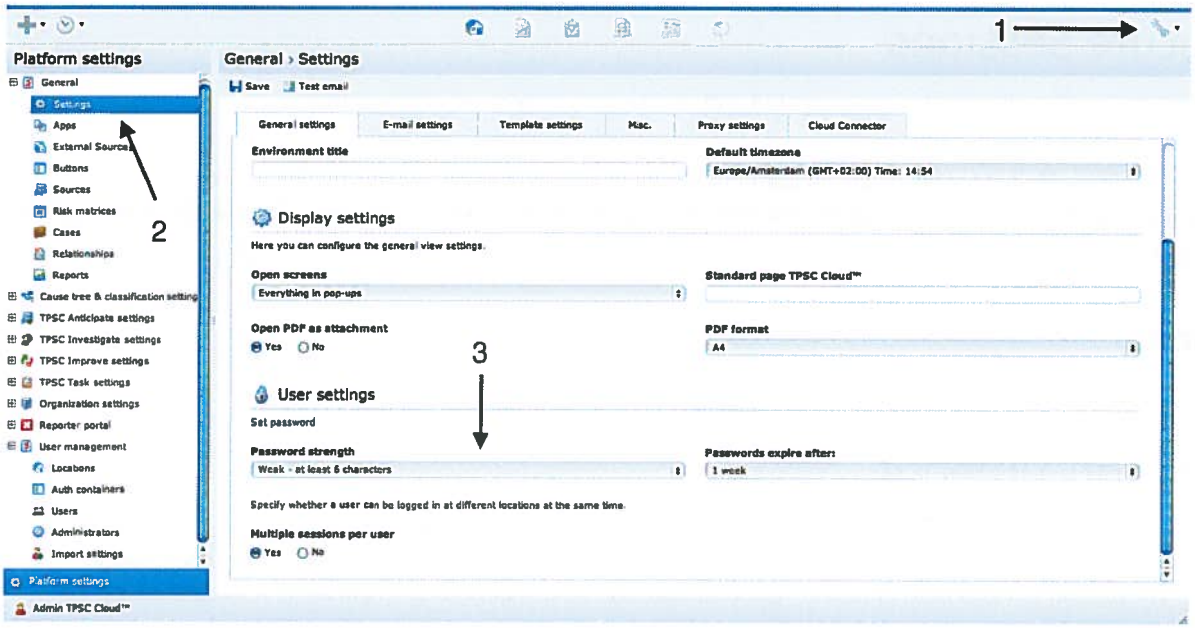
Platform settings --> User management --> Locations



Strong Password Policies

You can make passwords more secure and harder to break by requiring users to define complex passwords, setting up password expirations, and implementing lockouts.

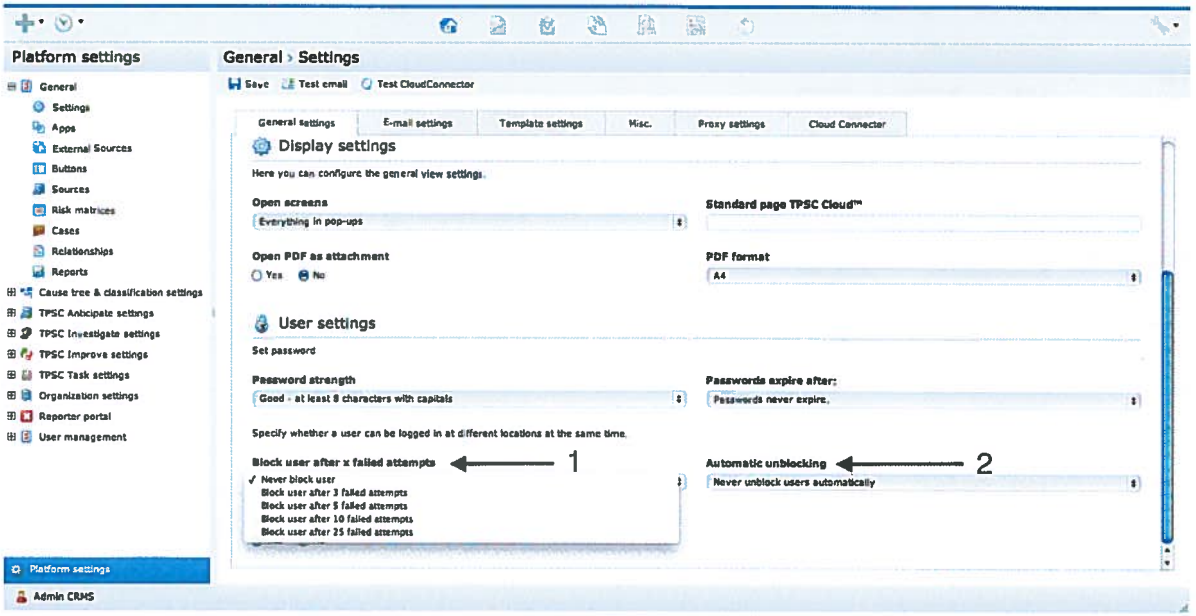
To set password policies, click: Platform settings --> Setting --> General settings.



Block users

Users can be blocked after an x number of failed logon attempts. The unblocking policies can be configured as well. If no automatic unblocking has been configured, the application administrator will need to unblock users manually.

To set the block user policies, click: Platform settings --> Setting --> General settings.



Secure Sessions

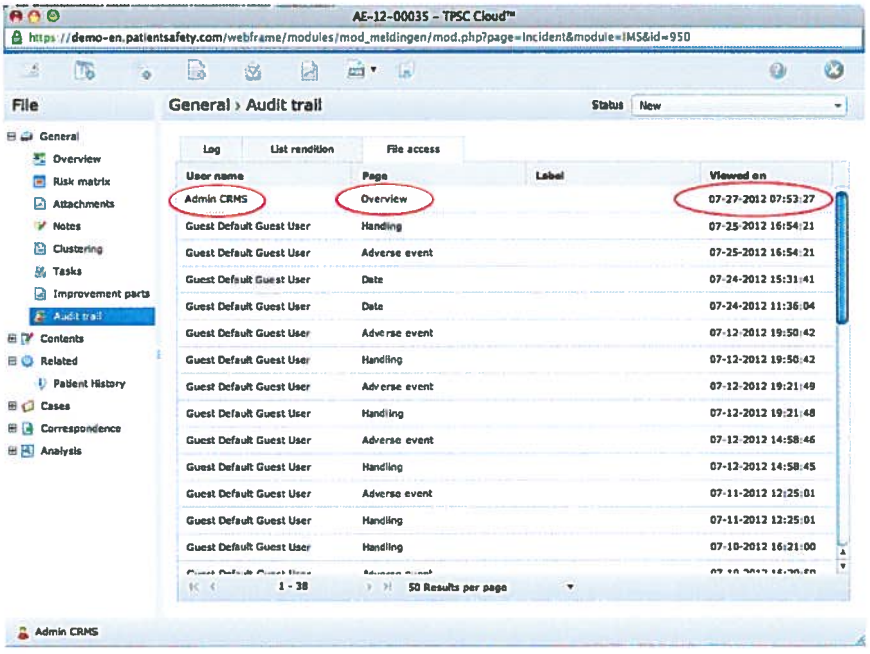
By mandating that all sessions are encrypted and secure, you protect messages in transit.

Session Timeout

Users sometimes leave their computers unattended or they don't log off. You can protect your applications against unauthorized access by automatically closing sessions when there is no session activity for a period of time. The default timeout is 20 minutes. Please contact our service desk to set a different session time out value.

Audit trail

All file access as well as the changes made to a file are tracked within the audit trail. Within a file you'll be able to view that accessed the file, what section, at what time and date.



About Wireless Connection

The Patient Safety Company offers SSL 3.0/TLS 1.0 encryption ("https") for login and communications between the TPSC Cloud™ and the end user's web browser. Your login credentials and business data are protected from hijacking even when you login to the TPSC Cloud™ over an unsecured wireless network.

Security recommendations

Online users are potential targets for attempts to steal login credentials and other sensitive information. Sometimes users are targeted by scam emails (phishing and malware) or even by phone calls attempting to gather information that can be used to gain unauthorized access or privileged knowledge.

Below some important recommendations:

- Don't use the same username and password for all (or even many) of your online accounts.
- Don't share your passwords with anybody, neither colleagues; don't write them down or send them via email.
- TPSC service desk personnel will never ask you for your password!
- Configure strong password policies such as password strength and aging.

Identify a Primary Security Contact

Please identify a person in your company who is responsible for application security. He or she should have a thorough understanding of your security policies.

Phishing and Malware

Phishing is known as the attempt to acquire information (and sometimes, indirectly, money) such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware. Very often logos of companies of government agencies are used to give the impression that it is legitimate. These emails will ask you to verify or update information.

- Poor spelling of email
- URL's don't match with the company they claim to come from.
- Links or attachments to install malicious code
- Beware of unusual links.

If you receive a suspicious email that involves the patientsafety.com, submit a report to servicedesk@patientsafety.com.

Suspicious phone calls

Be aware of persons who misrepresent themselves as employees or agents of The Patient Safety Company. They might attempt to steal your TPSC Cloud™ credentials. Never give your username and password over the phone.

If one of your users discloses his or her login credentials, you should reset that person's password immediately.

If a caller identifies him or herself as a TPSC employee and you do not recognize his or her name, ask for a callback number and email address. Write the details and mail them to servicedesk@patientsafety.com.

THIRD PARTY SERVICES - HOSTING PARTNERS

Hosting partners

The Patient Safety Company understands that client information and in particular patient information needs to be treated in the most secure and sensitive way. Selecting hosting partners is a critical step to assure privacy and secure data storage that is available 24x7.

Physical security

Key card protocols, biometric scanning protocols and round-the-clock interior and exterior surveillance monitor access to every one of our data centers.

Only authorized data center personnel are granted access credentials to our data centers. No one else can enter the production area of the data center without prior clearance and an appropriate escort.

Every employee undergoes multiple and thorough background security checks before they're hired. Every employee has signed a Confidentiality Agreement.

Precision environment

Every data center's HVAC (Heating Ventilation Air Conditioning) system is N+1 redundant. This ensures that a duplicate system immediately comes online should there be an HVAC system failure.

Every 90 seconds, all the air in our data centers are circulated and filtered to remove dust and contaminants.

Our advanced fire suppression systems are designed to stop fires from spreading in the unlikely event one should occur.

Conditioned power

Should a total utility power outage ever occur, all of our data centers' power systems are designed to run uninterrupted, with every server receiving conditioned uninterruptible power supply (UPS) power.

Our UPS power subsystem is N+1 redundant, with instantaneous failover if the primary UPS fails.

If an extended utility power outage occurs, our routinely tested, on-site diesel generators can run indefinitely.

Core routing equipment

Only fully redundant, enterprise-class routing equipment is used in data centers.

Fiber carriers enter our data centers at disparate points to guard against service failure.

Transfer of all data is done over SSL secured connections.

Infrastructure security

Our infrastructure is equipped with the latest security measures to prevent any unauthorized access to your data. The following protocols and systems are in place:

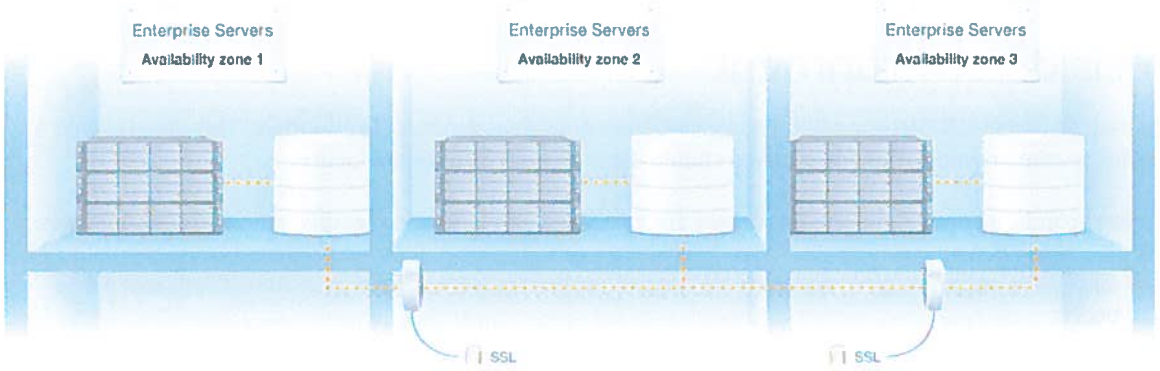
- SSL encryption
- Intrusion detection

- Multi-level IPS (network intrusion protection)
- Real time event monitoring / alerting
- Data encryption (256bit AES)

Back-up and recovery

Your data is fully secure within our state of the art datacenters.

- Daily backups with 14 recovery points (two weeks).
- 1 backup per month of the last 6 months.
- Backups are also saved in multi availability zones in encrypted format.
- We transfer backups only via a secure SSL connection.



Compliance and certification

Our hosting partners are independently audited and certified to meet the standards of SSAE16 Soc-1 Type II (formerly known as SAS-70 Type II) and equivalent standards. With these certifications these hosting providers have proven to have implemented the necessary procedures and processes correctly and to work accordingly.

The following subjects are part of the SSAE16 Soc-1 Type II audits:

- Facilities and asset management
- Logical access and access control
- Network and information security
- Computer operations
- Backup and recovery
- Change and incident management
- Organizational and administrative controls
- Security policies, reporting, and monitoring
- Physical and logical security

The CSAE 3416 Type II certification is the Canadian equivalent for the SSAE16.

Below you'll find an overview of the main security features of our carefully selected hosting partners including their compliancy:

	America	Europe	Canada	Australia	Asia
Security:					
SSL secure	✔	✔	✔	✔	✔
Intrusion detection system (IDS)	✔	✔	✔	✔	✔
Multi-level IPS (network intrusion protection)	✔	✔	✔	✔	✔
Real time event monitoring / alerting	✔	✔	✔	✔	✔
Periodic Risk assessment	✔	✔	✔	✔	✔
Managed backups with 14-day retention	✔	✔	✔	✔	✗
Backups saved in multi availability zones in encrypted format	✔	✔	✗	✗	✗
Certifications[1]:					
SSAE16 Soc-1 Type II (SAS 70 Type II)	✔	✔	✔	✗	✔
ISO-27001	✗	✔	✗	✗	✗
CSAE 3416 Type II	✗	✗	✔	✗	✗
Compliant to:					
HIPAA[2]	✔	✔	✗	✗	✗
PCI DSS[3]	✔	✔	✔	✔	✔
PHIPA	✗	✗	✔	✗	✗
NEN-7510	✗	✔	✗	✗	✗

Table 2: overview of the main security features and compliancy.

[1] Available on request.
[2] Health Insurance Portability and Accountability Act - Full overview of HIPAA Ready plan is shown in Appendix 1.
[3] Overview of the features to ensure PCI 2.0 Compliance are shown in Appendix 2.

Appendix 1 - HIPAA Ready

Web Application level protection

- Helps detect and contain undesirable traffic on public networks
- Helps prevent malware invasions like viruses, worms, and trojans
- Helps stop hacker attempts like SQL injections and XSS (Cross-site scripting) attacks
- Customizable security rules ensure WAF is calibrated to protect your unique vulnerabilities

Application Level Monitoring and Intrusion Detection

- Alerts administrators and managers every time files, directories, or hardware are accessed and by whom
- Detects active hosts, bad logon attempts, and inappropriate content

Business Continuity with HIPAA Compliant Encryption

- Managed backup snapshots with 14-day retention
- Provides data encryption at rest in storage
- Requires a "key" to securely decrypt the data from backup

Virtualized, HIPAA Compliant Hosting Architecture

- Provides separate and privatized web application and database hosting environments
- Makes creating a development/beta testing environment affordable
- Runs on enterprise level hardware
- Forces password expiration
- Automates SSH & RTD timeouts

HIPAA Compliant System Architecture

- Separate web and database environment
- Exclusive environment for development, separate from production environment
- Password expiration
- Automatic SSH & RTD timeouts

Log Retention

- Provides a valuable, detailed audit trail during a forensic investigation

Managed Patching, Version Control, and Security Updates

- Upgrades hardware and OS automatically, and applications on request
- Provides support for Linux and Windows OS
- Alerts administrators when security vulnerabilities are detected

Physical and Logical Security

- Includes stringent data destruction policies
- Controls data movement inside and outside of our facilities
- Records any changes to the hosting environment
- Secures the datacenter environment with man-traps, surveillance, and controlled access

Vulnerability Scanning

- Tests HTTP services, virtual domains, ports, and IP addresses for 10,000+ known vulnerabilities every day
- Delivers a detailed notification every time a vulnerability is found

Appendix 2 - Features to ensure PCI 2.0 Compliance

Access Control and Physical Security

- 24/7/365 support and physical monitoring
- Physical environment has restricted access and man traps
- Surveillance monitoring with video retention

Log Maintenance and Process Management

- Log storage and customizable retention

Systems Monitoring and Testing

- IDS (Intrusion Detection System)
- Real-time security event notifications
- Network security scans
- IP Logging
- Two-factor authentication

Website – Admin and Form Encryption

- SSL certificates with extended ID validation

Hardened Hosting Infrastructure

- Antivirus protection
- Firewalls
- Web application firewall
- Patching and maintenance
- Web server separated from database server
- Port control – unnecessary ports are closed
- Strong encryption during data transfer and transmission
- Redundant power and cooling