ISO 27001 CERTIFIED by schellman

HIPAA Compliant
Verified by Pivot Point Security

caregility

UHE Platform

Security Whitepaper

Release Version 1.2

10/09/2019

Contents

Contents

Introduction 2
Logging/Auditing 2
Access Controls (Management) 2
Password Complexity 3
Privileged User Access 3
Network Security 4
Physical and Environmental Security 4
ISO 9001:2008 Quality Management Systems Standard 5
ISO 14001:2004 Environmental Management System Standard 5
OHSAS 18001: 2007 Occupational Health & Safety Management System Standard 5
ISO / IEC 27001:2005 and 27001:2013 Information Security Management System Standard 5
ISO 50001:2011 Energy Management System Standard 6
PCI-DSS Payment Card Industry Data Security Standard 6
Privacy & Identity Management 6
Personal Identifiable Information (PII) 6
Conference Recording 7
Microsoft Skype for Business Federation 7
Conference Security 7
Encryption 7
Encrypted connections between UHE and Patient Room Systems use: 7
Encrypted connections between UHE and the UHE Sync Clinician Application use: 8
Encrypted connections between UHE and Microsoft Skype for Business 8
Resiliency, Load Balancing & Backup 8

Introduction

Before the adoption of any cloud-based service, the customer and service provider must first asses the safeguarding of any data transmitted, processed or stored through the service provider.

Caregility takes security very seriously and as such became ISO 27001 certified in 2014 for Cloud and Managed Services. This ensures that we have controls in place for Risk assessment, Security policy, Organization of information security, Asset management, Human resources security, Physical and environmental security, Communications and operations management, Access control, Information systems acquisition, development and maintenance, Information security incident management, Business continuity management and Compliance

A copy of the Caregility ISO 27001 certificate can be viewed here: https://cert.schellmanco.com/?certhash=4bKp7Rl1c7j8

This document describes the various security measures currently employed at Caregility for our Univago HE services. Maintaining security and data protection is of upmost importance to us at Caregility and as such we use the following security measures:

Logging/Auditing

Caregility keeps activity logs of tasks that are used to identify non-compliance with policies and other security-relevant events to assist in future investigations and access control monitoring. Logged data is retained on the device, in device backup files, or in data extracts used for analysis and reporting.
Logged data on Caregility's UHE infrastructure components may include:

- user ID's and email address
- dates and times for log-on and log-off
- records of successful and rejected authentication access attempts

Access Controls (Management)

There are different User Profile Roles that are available for each UHE user. They will provide different levels of operation:

Root Administrator: The root administrator is a Caregility internal employee who can access and manage ALL channel and customer entities. This person has full visibility to everything as a single dashboard. All capabilities and permissions are provided to this person.

Channel Administrator: The channel administrator is a person who works for an organization who may be providing their services to other hospital systems. The channel administrator can see each customer individually and assign technicians and clinicians at the customer level or be shared over multiple customers.

Customer Administrator: The customer administrator is a role configured in the system that allows that user to have full access to controls and settings for their company only. This person can create users, groups and profiles to assign to their end users, setup new patient room systems ready for installation and can create new clinical application users. The administrator can load certified technicians into the system.

Clinician: A clinician is a person who is using the system to initiate and manage calls to patient room systems. This role can have varying permissions set by the administrator. Only authenticated and authorized clinicians can call a patient room system.

Technician: A technician is a user who is responsible for installing or servicing a patient room system. Technicians must be certified and complete the online training course prior to installing or servicing a unit.

Patient: A patient is a person who is in a room where a patient system resides and is a participant in calls initiated by a clinician. The patient has no user interface. The room system only has a button which is used to request a call to the room. This is usually pressed by a nurse or local clinician in the room. The patient would not be the person initiating a call request.

Guest: A guest is a call participant that is not authenticated or authorized. A guest is only invited to a call or dialed out to by a clinician. The guest has no call control except for their own camera and audio controls or to disconnect from the call. Only the clinician has control of the call and camera during a call. A guest can be muted or ejected from a call by the clinician. If a clinician is no longer participating in the call, the call is terminated, and all guests and the patient room are disconnected from the call.

The platform is very granular with its access controls and various access groups are configured to allow Caregility employees varying levels of access dependent on their role.

All access to our systems and data are logged, tracked and audited wherever possible.

All user accounts are secure using the following technologies and security measures:

- Every user account is secured with a unique username and password
- All authentication requests are sent via HTTPS secure communication
- Passwords are hashed in our databases and are never viewable in plain text
- Passwords are never visible or communicated via email or other forms of electronic transfer
- Passwords are set and re-set using a password reset procedure

Password Complexity

Passwords must be at least six characters in length and must contain characters from three of the following four categories:

- Uppercase characters of European languages (A through Z)
- Lowercase characters of European languages (a through z)
- Base 10 digits (0 through 9)
- Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Privileged User Access

Sensitive data processed outside the enterprise carries an inherent level of risk, because outsourced services bypass the "physical, logical, and personnel controls" of IT departments. As such Caregility employees who manage and have access to customer's secure data are subjected to extensive background checks. In addition, employees are required to:

- Agree to and sign a Confidentiality Agreement
- Agree to and sign a Non-Disclosure Agreement
- Abide by the Caregility Policy handbook
- Employees attend regular training regarding their access rights to personal data
- Policies for disciplinary action against employees who access unauthorized data
- Policies controlling the retention of backup data

Network Security

Whether deployed within Caregility's data center or within a customer's data center, network security is as equally important as physical security and encryption. Caregility utilizes industry standards and best practices for our network security.

- Uptime: Continuous uptime monitoring, with immediate escalation to Caregility Technical Services staff for any downtime
- Internal Scans: Caregility performs its own security and vulnerability scans once a month
- Third Party Scans: Quarterly security and vulnerability scans are performed externally by Pivot Point
- Testing: System functionality and design changes are verified in an isolated test "sandbox" environment and subject to functional and security testing prior to deployment to active production systems
- Firewall: Firewall restricts access to only required ports of the service
- Patching: Latest security patches are applied to all operating system and application files to mitigate newly discovered vulnerabilities
- Access Control: Secure VPN, multifactor authentication, and role-based access are enforced for systems management by authorized engineering staff
- Logging and Auditing: Central logging systems capture and archive all internal systems access including any failed authentication attempts

Physical and Environmental Security

UHE services are set up in highly secure and hardened Equinix data centers. This ensures that all core infrastructure is secure and that access to these devices, and all relevant customer data, is restricted and access is documented. Our service infrastructure is co-located across the globe in three geographical locations. Our services are available in the Americas, Europe and Asia serviced from our data centers located in Secaucus NJ USA, Slough UK and Singapore.

Our carefully selected data centers have the following accreditations and certifications;

ISO 9001:2008 Quality Management Systems Standard

ISO 9001 is the world's leading quality management standard. An effective quality management system provides a clearly structured, systematic approach to maintaining and improving customer experience, and:

- minimizes the potential for incidents and mitigates any impacts
- ensures cost-effectiveness and clear lines of responsibility
- supports effective communication with hard facts and figures
- optimizes staff competences, commitment and motivation

ISO 14001:2004 Environmental Management System Standard

ISO 14001:2004 provides a framework for ensuring that any and all interfaces between Equinix and the environment are closely controlled in a manner that avoids or minimizes any negative environmental impact. The ISO 14001 standard:

- promotes procedures that have been made in an environmentally friendly and sustainable manner
- requires proactive management of any design and operational environmental risks
- supports Equinix and its customers in achieving lasting environmental and economic goals

OHSAS 18001: 2007 Occupational Health & Safety Management System Standard

This standard ensures that Equinix locations are safe and healthy environments to work in and visit. OHSAS 18001 requires that:

- any risks to staff, visitors and contractors have been assessed
- where necessary controls are put in place to reduce the risk of harm to a minimum
- all national/local legal and regulatory health and safety requirements are met

ISO / IEC 27001:2005 and 27001:2013 Information Security Management System Standard

Security is of paramount importance to Equinix and Caregility, and ISO 27001 is the most widely- accepted certification available for supporting information and physical security and business continuity ISO 27001 ensures that:

- risks and threats to the business are assessed and managed
- physical security processes such as restricted/named access are enforced consistently
- audits are conducted regularly at each site that include tests of security and cctv planning and monitoring

ISO 50001:2011 Energy Management System Standard

Leading the way in environmental standards, Equinix was the first data center provider in Europe to achieve ISO 50001 accreditation. ISO 50001 provides organizations with a recognized framework for integrating energy performance into their management practices.

PCI-DSS Payment Card Industry Data Security Standard

The PCI Data Security Standard (PCI DSS) ensures the safe handling of sensitive information and is intended to help organizations proactively protect customer account data.

For further information on ISO compliance please refer to: http://www.equinix.com/services/data-centers-colocation/standards-compliance/iso/

Some of the more visible security measures are as follows:

Reliability: All of Caregility's data centers are equipped with full UPS power, back-up systems and N+1 (or greater) redundancy, with a proven, industry-leading >99.9999% uptime record.

Power Density: With robust heating, ventilation and air conditioning (HVAC) systems, Caregility's data centers exceed the requirements of even the most power-hungry deployments.

Security: Caregility data centers utilize an array of security equipment, techniques and procedures to control, monitor, and record access to the facility such as;

24x7 Security Officers: Equinix uses the most senior level officers from one of the world's largest and best known security agencies. All guards undergo complete background/criminal checks and participate in forty hours of Equinix training.

Facility Access: Customers control access to each facility. No individual will gain access to the facility without having his or her visit previously scheduled. Moreover, Equinix can track individuals. All physical assess to the facility and customer cage is obtained via biometrics. Scheduled access provides tickets with audit logs for all access.

Biometric Hand Reader: Access to the front entrance to the facility is controlled using a biometric hand reader combined with an assigned access code. A customer must pass through 5 readers to gain access to their cage. Exterior security monitored – all points of ingress/egress are monitored by intrusion detection systems.

VNOC Security Access: Caregility's Video Network Operations Center (VNOC) and Help Desk area are restricted to key card access and is coupled with security camera identification.

Privacy & Identity Management

Personal Identifiable Information (PII)

Caregility ensures that all critical data (client name, PIN access codes, for example) are segregated, and only authorized users have access to data in its entirety. Moreover, Personal Identifiable Information

(PII) and credentials are protected as well as any data that Caregility collects or produces in relation to customer activity in the Univago HE platform

Conference Recording

No conferences are recorded. All real-time media communication is considered transient in nature and is not stored in a database or in any other storage type after a communication sequence has been completed.

Microsoft Skype for Business Federation

For Microsoft Skype for Business integration, Caregility employs Federation practices for Univago HE security. Federation establishes trust relationships between Caregility and Client that allows information sharing across domains. It provides inter-company or business-to-business (B2B) interactions that enable enterprise users to securely communicate and share information with colleagues, partners, and customers that are outside the corporate firewall. All Federated communications are encrypted between the Caregility Univago HE Servers and the external Skype services. This enables a Skype for Business Client to participate in the same meeting on the Univago HE platform along with patient room systems and the clinician application.

Conference Security

Univago HE offers the highest security with controls and privacy protocols in place to ensure that communications are delivered securely and privately. The service is HIPAA Compliant – verified by Pivot Point Security, and built on an ISO 27001 certified globally distributed platform hosted in hardened start-of-the-art SOC2 certified data centers. All logins are secured and authenticated before access is granted and all real-time audio and video, all media is encrypted. At no time is patient information stored by the service. For added session integrity, all sessions use randomized consultation ID's which are unique to every call.

Encryption

UHE video calls support several encryption methods, including Advanced Encryption Standard (AES), HTTPS/SSL/TLS, RTMPS and SRTP for securing transmission of both user access and call media. AES specifies a FIPS-approved cryptographic algorithm that can be used to protect electronic data for securing sensitive but unclassified material by U.S. Government agencies. Encryption converts data to an unintelligible form called cipher text. Decrypting the cipher text converts the data back into its original form, called plaintext. The AES algorithm can use cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits.

Where multiple levels of encryption are supported, the highest level of encryption is chosen based on the capabilities exchange with the endpoints

Encrypted connections between UHE and Patient Room Systems use:

- HTTPS TLS for signaling (Supports TLS 1.2) Note: TLS 1.0 and TLS 1.1 are deprecated and no longer supported

- DTLS 1.2 and SRTMP (encrypted RTMP) for media
- AES 128 bit encryption for media

Encrypted connections between UHE and the UHE Sync Clinician Application use:

- HTTPS TLS for signaling (Supports TLS 1.2)
- DTLS 1.2 and SRTMP (encrypted RTMP) for media
- AES 128 bit encryption for Media

Encrypted connections between UHE and Microsoft Skype for Business

- TLS for SIP call control (Supports TLS 1.2)
- SRTP for SIP media

Resiliency, Load Balancing & Backup

The UHE platform is a fully resilient solution utilizing various best practices such as Virtual Routing Redundancy Protocol (VRRP), Geo-location DNS services, Proxy Services and Distributed Media Architectures. The service is available across multiple physical locations across the globe and the distributed architecture allows overflow capacity between nodes and locations, providing support for conferences that span multiple physical servers/locations. This also keeps media as local to each endpoint as possible, reducing the negative impacts of latency, jitter, and packet loss commonly experienced on centralized deployments.

caregility

Changing the Point of Care