HEALTHEDGE
BECOME A DIGITAL PAYER

Clean Room Policy

Non-Disclosure Statement:

HealthEdge Software, Inc. (Company) is the sole owner of the information contained in this document. The content of this document is considered company confidential and may contain information that is protected under various federal and state statutes. Disclosure of this information without the express written consent of an authorized legal agent of HealthEdge is strictly prohibited. Any unauthorized distribution or use of this information may constitute a criminal act under various statutes and HealthEdge will fully cooperate with all law enforcement investigations regarding the disclosure of any content contained herein. HealthEdge retains the right to pursue criminal and civil remedies in the event of any unauthorized disclosure.

HealthEdge Software, Inc.
30 Corporate Drive
Burlington, MA 01803

Table of Contents

1 Objective

1.1 Purpose

The purpose of this policy is to enable execution and maintenance of the Clean Room to continue business operations for the Company's offshore Workforce Members while maintaining viable safeguards to protect customer environments and protected health information (PHI).

Data clean rooms provide a secure environment where sensitive information can be processed without fear of it being accessed by unauthorized personnel or malicious actors. This type of environment allows organizations to safely store and analyze confidential information in a manner that reduces security risks.

1.2 Scope

This Policy applies to Workforce Members in HealthEdge's Bengaluru, India office working in, or requiring access to, any Customer Data.

1.3 Management Commitment

The management of HealthEdge is committed to providing a safe and secure service to our customers. We understand the importance of protecting our customers' covered information and company assets from cybersecurity attacks. We have implemented cybersecurity measures and continuously assess and update them to align with industry standards and best practices. Our HealthEdge Users are trained and held accountable for adhering to our cybersecurity policies and complying with the industry standards and regulations.

1.4 Roles & Responsibilities

Role/Title	Responsibility
Chief Information Security Officer (CISO)	• Develop and maintain the policy. • Ensure that an appropriate level of access is granted and maintained. • Ensure that an annual review and recertification of users and their access is completed on an annual basis. • Complete annual review of privileged accounts. • Develop and recommend requirements for user-IDs and passwords. • Ensure enforcement of user-ID and password requirements.

Role/Title	Responsibility
Information Technology Team	• Ensure only authorized individuals are provided access to HealthEdge network devices and the clean room's information systems. • Provide updates and status reports to the CISO as needed or when a change occurs. • Create, implement, and maintain documented procedures that support HealthEdge's security policy requirements for protecting confidential, proprietary, or sensitive HealthEdge information and critical Information Assets.
HealthEdge Information Users	• Protect login credentials provided by HealthEdge. • Report any potential compromise or loss of login credentials to the CISO. • Comply with Clean Room Policy and all other HealthEdge policies.

2 Policy

This policy defines rules for access to the Clean Room and HealthEdge Information Assets and specifies administrative, technical, and physical security controls that are required.

A data clean room is a secure environment that is used to process and analyze sensitive data. It is designed to protect the integrity of the data and ensure that it is not compromised or corrupted in any way. The clean room is typically used for activities such data mining, analytics, data analysis, and troubleshooting.

Access to the Clean room is restricted to authorized personnel only. This ensures that only those who have been granted permission can access sensitive data.

The Clean Room is not a standard work area and shall be used exclusively as an exception when access to customer data is required. Workforce Members who are not actively engaged in supporting customers in a manner requiring access to said data are prohibited from the clean room.

This policy is reviewed and updated according to applicable laws and regulations at least every year and following any HealthEdge-defined events (e.g. assessment or audit findings, security or privacy incidents, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

2.1 Security Requirements

Data clean rooms are secured with controls such as specialized hardware and software designed to protect the confidentiality and integrity of the data. This includes firewalls, encryption, authentication protocols, and other security measures.

The Information Security department has established the following requirements for the implementation and maintenance of the Clean Room that must be met prior to its use by Workforce Members.

2.2 Technical Controls

- Access to Customer Data shall only be granted via the physical systems within the Clean Room. Workforce Members are prohibited from accessing customer data while remotely connected to HealthEdge's network.
- No creation, transmission, processing, or storage of Customer Data outside of the United States. Customer Data, where permitted, may be viewed by using remote access technology that ensures Customer Data remains within the United States.
- Access to Customer Data shall be solely through a secured Virtual Desktop Interface (VDI) with multi-factor authentication through a secure, encrypted connection (VPN).
- VDI shall prevent screen capture, copy, paste, print, download of data, and saving data locally or to an external drive.
- Access to wiring rooms and other areas housing servers and network components shall be controlled.
- Facility access will be restricted and monitored.
- Entry points that limit access to only Workforce Members providing Services must be controlled.
- Each Workforce Member should be assigned a unique key, access card, or key code for access to the high-security areas. Any workforce member entering the Clean Room must use two forms of authentication, such as a key card and a PIN, for example.
- Systems inside the Clean Room will have their USB drives and ports disabled to ensure data security.
- Only the corporate Internet network will be allowed for use; no guest or alternate connections.
- Print capability shall be disabled.
- Firewalls shall be installed, enabled, and centrally managed on computers that are connected to the Internet and used to access Company networks that transmit, process, or store Customer Data.
- The company shall implement (a) policies, (b) procedures, and (c) technical or compensating controls to prohibit users from installing software that has not been approved by HealthEdge Information Security management. Approved software must

be supported by the manufacturer, must not be used past the end of life, and must have the most recent security patches applied.

2.3 Physical Controls

To maintain its secure environment, the clean room must be built with the following Physical Controls:

- Floor-to-true ceiling walls separating the clean room from other areas.
- All doors located on the outer perimeter must be (i) constructed to prevent unauthorized access, (ii) alarmed, (iii) monitored, and (iv) designed to resist forced entry.
- All workstations must be physically anchored or fastened within the clean room and prevented from being moved from the designated work area.
- No internal windows.
- A security camera for monitoring ingress and egress.
- An identity verification system to access the clean room, systems, and data.

2.4 Administrative Controls

- Access cards shall not display anything associated with the Company's corporate name or logo or the location of the facility to which they permit access on personnel identification badges or locations outside of the production area.
- To prevent the capture, creation, transmission, processing, or storing of Customer Data, mobile devices shall not be permitted into the Clean Room.
- Have a process for logging and escorting visitors. Said process shall require visitors to sign in and out, be escorted at all times, and only be granted access for specific, authorized purposes.
- An inventory of equipment must be completed on a regular basis, and no less than annually.
- Workforce Members are prohibited from downloading or uploading Customer Data to mobile devices.
- To prevent the capture, creation, transmission, processing, storing, downloading or uploading of Customer Data, the following items are prohibited in the Clean Room:
- Bags, briefcases, backpacks and other similar items.
- Papers, books, and other writing materials.
- Cell phones, smartphones, personal computing devices, tablets, any form of writable or re-writable media, cameras, videotaping, or any other recording devices.

- Personnel performing services for Customer shall be in work areas where conversations containing Customer Data cannot be overheard by unauthorized individuals.
- Workforce Members desiring entry into the Customer's production area are subject to search by security personnel prior to admittance.
- Tailgating or allowing unapproved individuals into the Clean Room may result in sanctions.
- Any system assigned to the Clean Room must have a business justification along with approval from Technology Operations and Compliance prior to its removal.
- Access authorizations to systems and equipment are reviewed, updated, or revoked when there is any change in responsibility, or employment.
- Meetings and work discussions needed with unauthorized individuals must occur outside the Clean Room.
- Workforce members not abiding by any of the mentioned controls are subject to sanctions as appropriate.
- The India-based product teams and leadership are accountable for working with the TechOps team to ensure that the appropriate people are assigned and activated within the VDI, VPN and MFA controls.

3 Exceptions

Under rare circumstances, certain employees or contractors will need to employ systems that are not compliant with these policies. The CISO, or an authorized designee, must approve in writing all such instances.

4 Authority

The designated CISO, Legal Team, and Risk and Compliance Governance Committee (RCGC) have responsibility over the enterprise IT and Information Security policies.

5 Non-Compliance with This Policy

Failure to comply with HealthEdge Policy may result in disciplinary action including termination of employment, services, or relationship with HealthEdge

6 Terms and Definitions

Chief Information Security Officer – The CISO has authority over the Information Security and Compliance Program with oversight by HealthEdge Legal Team and the Risk and Compliance Governance Committee (RCGC).

Confidential – Data should be classified as Confidential when the unauthorized disclosure, alteration, or destruction of that data could cause significant risk to HealthEdge or its customers. This data should always be secured from unauthorized access. Data falling into this category includes proprietary business information, such as unannounced product specifications, business-related information that is designated for internal use only, any information containing one or more of the Sensitive Data Elements listed in Appendix B of the Data Classification, Handling, and Destruction Policy, data elements that are subject to regulatory and legal protection, or information that the Data Owner or Data Steward feels requires the consistent use of the extra controls involved with this classification. Confidential data is identified by a required "Confidential" stamp or watermark on the data or information.

Contractor - Throughout Company security policies, the term 'contractor' is defined as temporary workers who undertake a contract to provide materials, labor or services.

Employee - Throughout Company security policies, the term 'employee' is defined as full, part-time and per diem persons, non-contract workers, volunteers, and trainees where the Company has the right to dictate the resource's work duties.

Encryption - Throughout Company security policies, the term 'encryption' is defined as the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key that is compliant with the respective federal information processing standard published by NIST.

Information Assets - Throughout Company security policies, the term 'information assets' is defined as any data, devices, or other components of the Company environment that have value to the organization and support Company business operations. Company information assets must be protected against unauthorized access, use, disclosure, alteration, destruction, and/or theft, resulting in loss to the Company.

Information User(s) - Throughout Company security policies, the term 'information user(s)' is defined as all Company employees, contractors, collectively known as Company workforce, who are authorized to access Company information systems that are owned or controlled by the Company and used to support its business processes.

Personally Identifiable Information – Throughout Company security policies, the term ‘personally identifiable information’ is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

Private - Data should be classified as Private when the unauthorized disclosure, alteration, or destruction of that data could result in a moderate risk to HealthEdge or its customers. By default, Private data is any information generally intended for use within HealthEdge by HealthEdge Associates. For HealthEdge projects, it isn’t sensitive or subject to regulatory and legal protection requirements. Private Data is identified by a required “Private Data” stamp or watermark on the data or information.

Protected Health Information – Throughout Company security policies, the term ‘protected health information’ is defined as individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations.

Protected Information - Throughout Company security policies, the term ‘protected information’ is defined as a data classification level that includes personally identifiable information in any form (hard copy or electronic) subject to state or federal laws or regulations restricting the use and disclosure of that data.

Risk Assessment - The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Workforce - Throughout Company security policies, the term ‘workforce’ is defined as all users who are authorized to access Company information systems that are owned or controlled by the Company and used to support its business processes.