HealthEdge Corporate
Data Protection & Privacy Procedure

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

Table of Contents

1 Objective

1.1 Purpose

The purpose of this Data Protection and Privacy Procedure is to document how HealthEdge Corporate provides controls to protect the privacy and confidentiality of personal and sensitive data in accordance with applicable data protection laws and regulations. This procedure establishes the principles and practices for the collection, use, storage, processing, and sharing of HealthEdge data, ensuring that data is handled securely, ethically, and transparently.

1.2 Scope

This procedure applies to all global HealthEdge Information Users who are authorized to access HealthEdge Information Assets that are owned or controlled by HealthEdge and used to support its business processes.

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 Official (CISO)	• Revise, implement, interpret, and enforce the Procedure that supports this procedure. • Ensure collaboration with legal, regulatory, and risk management requirements. • Conduct a compliance review of current retention processes on an annual basis.
Legal & Privacy Team	• Maintain this procedure. • Ensure that HealthEdge Users are aware of their role and responsibility in protecting confidential data.

Role/Title	Responsibility
	• Provide guidance and support to HealthEdge Corporate and product owners on controls that must be implemented and/or require to be implemented by third parties hosting HealthEdge confidential data.
Information Technology (IT)	• Work closely with the Legal Team, Privacy Team, and CISO to ensure that data is maintained and/or destroyed as required.
HealthEdge Users	• Provide guidance to the CISO on how long data and records must be maintained based on regulatory and legal requirements.

1.5 Applicable Law, Standards, and Regulator Requirements

This document has been implemented as mandated by and/or in support of the following applicable laws:

- HITRUST Cybersecurity Framework (CSF) v11.3.0
- HIPAA Security Rule
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, rev 5, Security and Privacy Controls for Information Assets and Organizations
- NIST SP 800-66, rev 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

1.6 Tools

The following tools are used in support of this procedure:

Tool Name	In-house, SaaS, COTS, IaaS, PaaS	Purpose
Malbek CLM	SaaS	Malbek CLM is used for the creation, management, storage and milestones to streamline HealthEdge enterprise-wide contract lifecycle management and risk management of contracts.
Coupa	SaaS	Coupa is a cloud-based platform for Business Spend Management (BSM). It helps HealthEdge to manage and optimize their spending across procurement, supply chain, and finance.
Non-Disclosure Agreement	In-house	HealthEdge Users must sign an NDA upon hire and annually thereafter.
Privacy Notices	In-house	Privacy Notices are posted on every HealthEdge product website.
Outside Counsel	N/A	HealthEdge has a contract with an outside counsel firm to provide guidance and support.
Dune Security	SaaS	Dune Security is an advanced AI-powered platform specifically designed for comprehensive employee risk management. Used for training, acknowledgment of policies, etc.

2 Procedure

These procedures apply to access controls managed by HealthEdge and fall under the responsibility of the following:

Responsible Parties:

- **HealthEdge Legal Team:**
  - Manage Data Protection and Privacy Program within HealthEdge. Provide guidance and support to HealthEdge Executive Leadership Team (ELT), Managers, Product Management Teams, CISO, Human Resources (HR), IT Technology Team Members, and HealthEdge Users on how to understand data classification, how to label data, how long to maintain private and confidential data, etc. Management of contracts via Malbek CLM. Contract language and clauses are contained within the Malbek tool.
  - Management updates to Security Agreements and Non-Disclosure Agreements signed by HealthEdge Users.
  - Management of Conflict of Interest (COI) documents signed by HealthEdge Users.
  - Review and approve Privacy Notices posted on HealthEdge customer portals and Websites.
  - Management of data retention requirements for HealthEdge based on customer data retention requirements.
- **HealthEdge Product Management Teams:**
  - Manage data retention based on HealthEdge customer data retention requirements.

Review and update the Data Protection & Privacy Procedures at least every year and after any HealthEdge-defined events (e.g., assessment or audit findings or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines).

2.1 Confidentiality Agreements

- The HealthEdge Legal Team is responsible for the following:
  - Creation of Non-Disclosure Agreements.
  - Annual review and update to Non-Disclosure Agreements.
  - Working with HealthEdge HR to ensure that all HealthEdge Users review and acknowledge the Non-Disclosure Agreement upon hire and annually thereafter. Data is captured in Dune Security (security awareness & training tool).

- The HealthEdge Legal Team, along with outside counsel when needed, ensure that NDAs comply with all applicable laws and regulations for the jurisdiction to which it applies.
- HealthEdge Legal Team assist CISO, Information Security & Compliance Team, SecOps, ELT, Managers, HR, and HealthEdge Users in understanding the role they play in providing adequate controls for private and confidential data.

2.2 Addressing Security When Dealing with Customers

- The HealthEdge Legal Team is responsible for ensuring that the privacy statement, on HealthEdge public site and HealthEdge product portals include details on the Privacy Program and who to contact within HealthEdge if they have a concern.

2.3 Intellectual Property Rights

- All purchases of software, by HealthEdge, must be approved by management and go through legal to ensure that the organization remains in compliance with any software licenses.
- HealthEdge Legal ensures that there are licenses in effect for all open-source software used by HealthEdge.
- Open-source software used by HealthEdge must be legally licensed, authorized, and must follow the HealthEdge Corporate - Configuration Management Procedure.

2.4 Protection of Organizational Records

- HealthEdge provides data classification, handling, and destruction guidelines to all HealthEdge Users. It is the responsibility of the Data Owner to ensure that data is properly classified, handled, and destroyed based on the HealthEdge Corporate Data Retention Schedule or based on the contracts signed by HealthEdge with the customer.
- Data classification, handling, and destruction is covered during the HealthEdge awareness & training provided upon hire and annually thereafter.
- The HealthEdge Legal Team provides guidance to Data Owners regarding the disposal and/or destruction of confidential or private data.
- The HealthEdge Legal Team maintains a Data Retention Schedule that provides information related to how long certain HealthEdge data must be retained. The HealthEdge Legal Team relies on the HealthEdge Product Management Team to ensure that any disposal of private or confidential information is:

    - Securely disposed of when no longer needed for legal, regulatory, or business reasons, including disposal of private and/or confidential information.
    - Data is encrypted at rest and when in transit.
    - Data is identified and removed when required by the customer who ultimately owns the data.
- The HealthEdge Legal Team relies on the Data Owner to maintain an inventory of Information Assets where private and/or confidential data is stored.
- Cryptographic keys are managed by either the third-party provider or by HealthEdge Information Asset Owners, Product Management Teams, etc. and are kept securely and made available only when necessary.
- Cryptographic keying material and programs associated with encrypted archives or digital signatures are also stored to enable decryption of the records for the length of time the records are retained. Managed by Product Management Teams or Information Asset Owners.
- Records are securely destroyed when retention is no longer necessary per the HealthEdge record retention schedule or based on customer requirements.
- The HealthEdge Legal Team and ELT review and approve the security categorizations as well as guidelines in place to assist Data Owners in categorizing data.
- Important records, such as contracts, personnel records, financial information, and client/customer information are protected from loss, destruction, and falsification. The HealthEdge Legal team uses Coupa to manage contracts. The HealthEdge HR Team keeps HR related records in COTS SaaS applications. Financial data is managed by the Finance Team and is stored in tools like Coupa.
- The HealthEdge SecOps Team, Product Management Teams, Data Center Teams and others are responsible for physical, administrative, and operational security controls such as access controls, encryption, backups, electronic signatures, locked facilities, or containers are implemented to protect these essential records and information. These controls are captured in other HealthEdge Corporate procedures or specific Product Management Team procedures.
- HealthEdge Data Retention Schedule covers how long policies, procedures, other critical records (e.g., results from a risk assessment), and disclosures of individuals' protected health information are retained for a minimum of six years.
- For electronic health records, HealthEdge must retain records of disclosures to carry out treatment, payment and healthcare operations for a minimum of three years.

2.5 Data Protection and Privacy of Covered Information

- HealthEdge Information Asset Owners and Product Management Teams have controls in place to encrypt private and/or confidential information, at minimum, is

rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in audit logs.

- Any exceptions to the data encryption requirements must be authorized by management and documented.
- Encryption controls in place for HealthEdge Corporate Information Assets and product specific Information Assets, at a minimum include:
    - Encryption is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures.
    - For full-disk encryption, logical access is independent of operating system access.
    - Decryption keys are not tied to user accounts.
    - If encryption is not applied because it is determined to not be reasonable or appropriate, HealthEdge documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.
- The HealthEdge Corporate Legal Team relies on the Product Management Teams to limit the private and/or confidential information storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention Procedure. Typically, HealthEdge maintains data based on customer requirements.
- HealthEdge Product Management teams are responsible for ensuring that private information storage is kept to a minimum.
- The HealthEdge Product Management Teams have implemented technical means to ensure private information is stored in HealthEdge-specified locations for that product. The HealthEdge Corporate Service Desk Team and others provide technical controls for confidential data stored on Endpoint devices.
- The HealthEdge Legal Team along with the Product Management Team explicitly identify and ensure the implementation of security and privacy protections for the transfer of HealthEdge records, or extraction of such records, containing sensitive personal information to a state or federal agency or other regulatory body that lawfully collects such information.
- Where required by legislation, consent is obtained before any PII (e.g., about a client/customer) is emailed, faxed, or communicated by telephone, or otherwise disclosed to parties external to HealthEdge. The HealthEdge Legal Team must be consulted if this is required to happen.

2.6 Regulation of Cryptographic Controls

- HealthEdge Corporate works closely with HealthEdge Product Management Teams to ensure that they address the type and strength of the encryption algorithm and when it must be used to protect private or confidential data.
- Cryptographic modules, used in HealthEdge products, meet FIPS, NIST, and other regulatory requirements. HealthEdge Product Management Teams are responsible for ensuring that the cryptographic controls meet regulatory requirements.

2.7 Information Labeling and Handling

- All Data and Information Assets within the individual product environments are considered private. Everything within these environments is treated the same regarding how the Information Assets and private data are secured and handled.
- Labeling and handling reflect the classification (i.e., private) according to the rules in the HealthEdge Data Protection & Privacy Procedure.

2.8 Publicly Available Information

- HealthEdge Corporate has a designated team that is authorized to post information onto a publicly accessible information system and train these individuals to ensure that publicly accessible information does not contain nonpublic information.

2.9 Control of Internal Processing

- HealthEdge has multiple policies and procedures that discuss system and information integrity. This data is covered in policies such as:
    - HealthEdge Access Control Procedure.
    - HealthEdge Transmission Protection Procedure.
    - HealthEdge Configuration Management Procedure.
    - HealthEdge Audit Logging & Monitoring Procedure.
- HealthEdge policies and procedures are disseminated to appropriate HealthEdge Users within the organization as well as maintained on secure shared sites and in their GRC tool and Dune.
- HealthEdge requires that all system and information integrity requirements are reviewed no less than annually. HealthEdge Corporate Information Security & Compliance Team manages this process on behalf of the organization. Further information can be found in the HealthEdge Corporate – Risk Management Procedure.

2.10 Output Data Validation

- Data input and output validation is managed by the HealthEdge Product Management Teams. Information related to how this is managed can be found in the HealthEdge configuration management procedure for each product.
- Automated output data validation controls differ across each HealthEdge product and system development process (e.g., applications, databases. Output data validation includes:
    - Plausibility checks to test whether the output data is reasonable.
    - Reconciliation control counts to ensure processing of all data.
    - Providing sufficient information for a reader (e.g., to ensure that the client/customer they are serving matches the information retrieved, or subsequent processing system to determine the accuracy, completeness, precision, and classification of the information).
    - Procedures for responding to output validation tests.
    - Defining the responsibilities of all personnel involved in the data output process.
    - Creating an automated log of activities in the data output validation process.

2.11 Protection of System Test Data

- HealthEdge Product Management Teams do not use private data in their test environments unless it is approved by the customer as well as the HealthEdge management team. Typically, this happens if the only way to remediate an issue reported by a customer and the only way to do that requires the use of private data. Once the issue is resolved, the private data is wiped out from the test environment.

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 Procedure

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

6 Terms and Definitions

Chief Information Security Official (CISO) - 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 Procedure, 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.

Critical Information Assets – Information assets that are required to be operational in support of critical business processes.

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.

Ephemeral Storage: Temporary storage that is deleted once the instance using it is terminated.

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 Assets that are owned or controlled by the Company and used to support its business processes.

Non-Persistent Components: Components of an information system that are temporary and do not retain data or configuration after their lifecycle ends.

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.

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

7 Security Framework Mapping

Framework	Controls
NIST 800-53 rev 5	AC-16(2), AC-18(1), AC-19(4)b1, AC-19(4)b3, AC-20a, AC-22a, AC-22b, AC-22c, AC-22d, AC-4(24), AC-4(32), AU-11(1), AU-16(3), AU-5(4), CA-3(7)a, CM-10(1), CM-10b, CM-10c, CM-3(5), CP-12, CP-9, CP-9(7), IA-7, IR-5(1), PS-6(2)c, PS-6a, PS-7a, PS-7b, PS-7c, PS-7e, PT-3(2), RA-2c, SA-10(4), SA-10(5), SA-10(6), SA-3(2)a, SA-3(2)b, SA-4(12)b, SA-8(33), SA-9(7), SC-12(2), SC-13, SC-16, SC-28, SC-28(1), SI-13(4)b, SI-14(1), SI-14(2), SI-15, SI-17, SI-21, SI-23, SI-2a, SI-6, SI-7(12), SI-7(2), SI-7(5), SI-7(6), SI-7(7), SI-7a, SI-7b, SR-2(1), SR-3(3), SR-4(4), SR-5, SR-5(1), SR-8, SR-9(1)
HITRUST	19131.05e1Organizational.45, 19134.05j2Organizational.5, 19249.06b1Organizational.2, 19142.06c1Organizational.8, 19144.06c2Organizational.1, 19145.06c2Organizational.2, 19143.06c2Organizational.3, 19141.06c2Organizational.4, 19140.06c2Organizational.5, 1903.06d1Organizational.3456711, 1904.06d2Organizational.1, 19245.06d2Organizational.2, 1911.06d2Organizational.3, 1902.06d2Organizational.4, 19922.06f1Organizational.2, 19165.07e1Organizational.13, 19180.09z1Organizational.2, 1908.10c1System.5, 19199.10e1System.12, 19204.10i1System.1
HIPAA & NIST SP 800-66 rev2	164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.308(a)(7)(ii)(E), 164.316(b)(2)(i)