HEALTHEDGE
BECOME A DIGITAL PAYER

Data Protection & Privacy 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

1.1 Purpose 1

1.2 Scope 1

1.3 Management Commitment 1

1.4 Roles & Responsibilities 1

1.5 Applicable Law, Standards, and Regulator Requirements 2

2 Policy 2

2.1 Confidentiality Agreements 2

2.2 Addressing Security When Dealing with Customers 3

2.3 Intellectual Property Rights 3

2.4 Protection of Organizational Records 3

2.5 Data Protection and Privacy of Covered Information 4

2.6 Regulation of Cryptographic Controls 5

2.7 Information Labeling and Handling 5

2.8 Publicly Available Information 5

2.9 Control of Internal Processing 5

2.10 Output Data Validation 5

2.11 Protection of System Test Data 6

3 Exceptions 6

4 Authority 6

5 Non-Compliance with This Policy 6

6 Terms and Definitions 6

7 Security Framework Mapping 8

1 Objective

1.1 Purpose

The purpose of this Data Protection and Privacy Policy is to outline HealthEdge's commitment to protecting the privacy and confidentiality of personal and sensitive data in accordance with applicable data protection laws and regulations. This policy 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. The goal is to safeguard HealthEdge Data while enabling the organization to meet its operational needs, comply with legal obligations, and mitigate the risks associated with data breaches or misuse.

1.2 Scope

This Policy 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 Officer (CISO)	• Revise, implement, interpret, and enforce this policy. • Ensure collaboration with legal, regulatory, and risk management requirements. • Conduct a compliance review of current retention process on an annual basis.

Role/Title	Responsibility
Legal & Privacy Team	• Provide guidance to CISO, Corporate Users, product owners regarding how to protect confidential data.
Information Technology (IT)	• Work closely with the Legal Team, Privacy Team, and CISO is protected and ensure that data is maintained and/or destroyed as required.
HealthEdge Product Owners	• Provide guidance to the Legal Team, Privacy Team, and 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 Systems and Organizations
- NIST SP 800-66, rev 2, Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide

2 Policy

- Review and update the Data Protection & Privacy Policy at least every year and following 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

- Requirements for confidentiality and non-disclosure agreements are reviewed at least annually and when changes occur that influence these requirements.
- Confidentiality and non-disclosure agreements comply with all applicable laws and regulations for the jurisdiction to which it applies.

2.2 Addressing Security When Dealing with Customers

- Ensure that the public has access to information about its privacy activities and can communicate with its senior privacy official (e.g., Privacy Officer, Chief Data Protection Officer).

2.3 Intellectual Property Rights

- Establish restrictions on the use of open-source software.
- Open-source software used by HealthEdge is legally licensed, authorized, and adheres to HealthEdge's Configuration Management Policy.

2.4 Protection of Organizational Records

- Guidelines are issued and implemented by HealthEdge on the ownership, classification, retention, storage, handling, and disposal of all records and information.
- Establish and implement a record retention program that addresses:
  - The secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of private and/or confidential information.
  - All storage of private and/or confidential information.
  - A review process (automatic or manual) to identify and remove covered and/or confidential information that exceeds the requirements of the data retention policy on a quarterly basis.
- A retention schedule is drawn up identifying essential record types and the period for which they must be retained.
- An inventory of sources of key information is maintained.
- Any related cryptographic keys are kept securely and made available only when necessary.
- Any related 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.
- Records are securely destroyed when retention is no longer necessary per HealthEdge's record retention schedule.
- Designated senior management within HealthEdge reviews and approves the security categorizations and associated guidelines.
- Important records, such as contracts, personnel records, financial information, and client/customer information are protected from loss, destruction, and falsification.

- Security controls, such as access controls, encryption, backups, electronic signatures, locked facilities, or containers are implemented to protect these essential records and information.
- HealthEdge's formal policies, formal 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

- 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 logs.
- Exceptions to encryption requirements are authorized by management and documented.
- 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.
- 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 policy.
- Private and/or confidential information storage is kept to a minimum.
- Implement technical means to ensure private and/or confidential information is stored in HealthEdge-specified locations.
- 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 conversation, or otherwise disclosed to parties external to HealthEdge.

2.6 Regulation of Cryptographic Controls

- Address the type and strength of the encryption algorithm and when used to protect the confidentiality of information.
- Employ cryptographic modules that are certified and that adhere to the minimum applicable standards.

2.7 Information Labeling and Handling

- Physically and/or electronically label and handle sensitive information commensurate with the risk of the information or document.
- Labeling reflects the classification according to the rules in the information classification policy.

2.8 Publicly Available Information

- Designate individuals 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

- Develop and document System and Information Integrity Policy and Procedures.
- Disseminate the system and information integrity policy and procedures to appropriate areas within the organization.
- Review and update defined system and information integrity requirements no less than annually.

2.10 Output Data Validation

- When doing system development (e.g., applications, databases), output validation:
    - Is manually or automatically performed.
    - Includes plausibility checks to test whether the output data is reasonable.
    - Includes reconciliation control counts to ensure processing of all data.
    - Includes 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).
    - Includes procedures for responding to output validation tests.

  - Includes defining the responsibilities of all personnel involved in the data output process.
  - Includes creating an automated log of activities in the data output validation process.

2.11 Protection of System Test Data

- The use of operational databases containing private and/or confidential information for non-production (e.g., testing) purposes is avoided; however, if private and/or confidential information is used for testing purposes, all sensitive details and content is removed or modified beyond recognition (i.e., de-identified) before use.

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.

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)