Data Classification, Handling, & Destruction Policy

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

Table of Contents

1 Objective

1.1 Purpose

The purpose of this policy is to establish certain data classification, handling, and destruction requirements, along with roles and responsibilities, for protecting data throughout its lifecycle from collection or creation through processing/use and retention, until destruction of electronic and paper-based data. HealthEdge and HealthEdge Users are expected to implement these data protection requirements and, when applicable, oversee the implementation of requirements by Suppliers to comply with policies, laws, regulations, and contractual obligations.

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. • Work with organizational leaders to assign classification labels to data handled by the organization. • Renew and update classification labels when necessary. • Provide ongoing workforce education and awareness at it pertains to data classification, handling, data retention, and data destruction.

Role/Title	Responsibility
Management	• Provide support through active enforcement, funding, and resources needed to meet the requirements of this policy.
Legal	• Advise on legal, regulatory, and contractual data handling and destruction requirements as needed.
Data Owner / Data Trustee	• Categorize and classify the data within the scope of their ownership or trust. • Document and communicate requirements for data protection and appropriate use of data. • Limit data collection to only the data required for permitted, legal basis and stated purpose(s). • Restrict and periodically revalidate that data user(s) have a legitimate purpose and legal basis for the data they access. • Ensure the transfer or replication of data to systems outside their span of control are documented (including the identification of the recipient's Data Owner or Trustee) and applicable data protection requirements are communicated and enforceable prior to transferring or replicating the data. • Apply appropriate controls for data based on the highest-level classification of the individual data elements when the data is combined from multiple sources. • Take reasonable and appropriate measures designed to ensure that the collection of data, including confidential and personal data, complies with all laws, regulations, contractual obligations, and internal policies. • Designate Data Custodian(s) and communicate data protection requirements to them. • Be accountable to the external entity from which the data is collected and for complying with known contractual obligations and protection requirements agreed upon by HealthEdge and the external entity.
Data Custodian	• Implement requirements (including contractual obligations) based on the data classification and risk. • Grant and maintain data access consistent with the data protection requirements established by the Data Owner or Data Trustee.
HealthEdge User	• Abide by all rules and requirements specific to the data they handle.
Chief Privacy Officer	• Conduct incident risk assessments where required (HIPAA) • Manage the activities of any external notification for vendors retained to assist with the incident. • Ensure, in conjunction with Legal, Information Services and CISO, that evidence is appropriately gathered and preserved, and the chain of custody is documented and maintained. • Facilitate notifications to relevant parties including regulatory required notices under state and federal laws working with legal counsel and impacted individual notifications where applicable.

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

2 Policy

- Review and update this Data Classification, Handling and Destruction 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 Data Classification Scheme

Data Classification	Description
Public	Data should be classified as Public when the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to HealthEdge or its customers. Unlike the other two classifications, a watermark or a stamp is optional for Public Information. Protecting information that is considered Public is not required; after all, it is meant to be shared.
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.
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

Data Classification	Description
	Elements listed in Appendix B, 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.

2.2 Data Protection Across the Data Lifecycle

- Technical, physical, and administrative measures must be in place throughout the HealthEdge Data lifecycle. Information must be protected from loss, destruction, and falsification, based on its importance to HealthEdge, classification level, and in accordance with statutory, regulatory, contractual, and business requirements.
- Physical media creation, handling, and destruction will be treated according to its classification and will comply with all requirements in the Data Retention Policy.
- Security controls, such as access controls, encryption, backups, electronic signatures, locked facilities, and lockboxes, etc., must be implemented to protect HealthEdge Data based on its classification.
- Conduct annual reviews of the data classification scheme and processes to identify potential gaps and re-classify data when needed.
- Covered Information usage will be monitored to ensure compliance with this policy, related guidelines, and procedures, as well as with all applicable contractual, federal, state legislative and regulatory requirements, and industry guidelines.
- All HealthEdge Data incidents must be immediately reported to the Information Security organization following the established communication process. The Information Security organization must evaluate the criticality of the incident and where subject to federal and/or state reporting requirements, report it to authorities following consultation with the Legal team.
- Suppliers that process data on HealthEdge behalf must have appropriate data protection contractual provisions in place and must complete a security assessment before accessing HealthEdge Data, with periodic re-assessments, thereafter, as the Third Party Assurance Policy.
- HealthEdge Information Users must be notified and made aware when the data they are accessing contains PHI.
- Further information can be found in the Portable Media Security Policy and the Data Protection and Privacy Policy.

2.3 Data Access

- Private and confidential data is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated.

- Workstations are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token, or similar user authentication mechanism that conceals information previously visible on the display when unattended, and protected by key locks, passwords, or other controls when not in use.
- Documents containing covered or critical information are removed from printers, copiers, and facsimile machines immediately.
- When transporting documents with covered or confidential information within facilities and through inter-office mail, covered or critical information is concealed during transit (e.g., using opaque envelopes).
- Access to a delivery and loading area from outside of the building is restricted to identified and authorized personnel.
- The external doors of a delivery and loading area are secured when the internal doors are opened.
- Further information can be found in the Access Control Policy and Physical & Environmental Security Policy.

2.4 Data Collection and Creation

- HealthEdge must collect data in compliance with its legal obligations while respecting privacy and confidentiality and maintaining trust.
- Data classification should be applied upon collection and creation of data. All HealthEdge Data falls into one of the three categories of information (i.e., Public, Private, Confidential) based upon its confidentiality, criticality, and business value, in accordance with the above Data classification scheme.

2.5 Data Usage and Sharing

- HealthEdge Data must be used only for the business purposes for which the data was created or collected. HealthEdge Data owners and data custodians must ensure that information subject to special handling is identified and appropriate labeling and handling requirements are expressly defined and implemented consistent with applicable contractual, federal, and state legislative and regulatory requirements, and industry guidelines.
- HealthEdge Information Technology will apply appropriate technical controls to Information Assets based on classifications designated by the Data Owner.
- An appropriate set of processes and procedures for information labeling and handling must be in place in accordance with the classification scheme adopted by HealthEdge.

- When handling HealthEdge Data, HealthEdge Users and applications must be compliant with the Acceptable Use Policy and follow formal operating procedures on processing and handling data securely based on its classification level.
- When sharing HealthEdge Data, HealthEdge Users and Information Assets must only share what they are authorized to share by the Data Owner, as reflected in the HealthEdge application inventory or other governing documentation.
- Regardless of ownership, the use of any information processing equipment outside the organization's premises, including equipment used by remote workers, even where such use is permanent (e.g., a core feature of the employee's role), is authorized by management.

2.6 Data Handling & Data Destruction

- Media is labeled, encrypted, and handled according to its classification.
- HealthEdge Users must not share HealthEdge Data to anyone outside of the company without permission from the Data Owner or their approved designee(s).

Control	Confidential	Private	Public
Copying /Printing	• May only be printed when there is a legitimate need and only for authorized individuals (e.g., customers, regulators or individuals with appropriate contractual confidentiality provisions). • Must not be left unattended or unsecure. • Must be sent via tamper sealed envelope.	• May only be printed when there is a legitimate need and only for authorized individuals (e.g., customers, regulators or individuals with appropriate contractual confidentiality provisions. • Must not be left unattended or unsecured.	No restriction
Paper Records	• Should be securely destroyed by a third-party service or and approved shredder. • Must be disposed of by the Data Owner according to the Records Retention Schedule.	• Should be securely destroyed by a third-party service or an approved shredder. • Must be disposed of by the Data Owner according to the Records Retention Schedule.	No restriction
Physical Security	• Endpoint devices such as laptops and mobile devices must be locked or logged out when unattended. • Servers or virtual devices hosted in a secure Data Center. • Physical Security must be monitored and limited to authorized individuals.	• Endpoint devices such as laptops or mobile devices must be locked or logged out when unattended. • Servers or virtual devices hosted in a secure Data Center. • Physical Security must be monitored and limited to authorized individuals.	No restriction

Control	Confidential	Private	Public
Data Storage	• Must be stored on a secure file server or secure data archive (i.e., limited access and encrypted). • Must not be stored on unapproved endpoint devices, personal computers, or mobile devices. Where permitted: • Whole disk encryption is required. • Must be protected with a passcode. • For Mobile devices the data must be stored in an encrypted container. • For Mobile devices, HealthEdge must have the ability to remote wipe the encrypted container. • Must not be stored on connected external storage. • Unless an exception is granted, an end compliance solution must deny external storage devices. • Paper/hard copy cannot be stored where others can access it.	• Must be stored on a secure file server or secure data archive (i.e., limited access). • Must not be stored on unapproved endpoint devices, personal computers, or mobile devices. Where permitted: • Whole disk encryption is required. • Must be protected with a passcode. • For Mobile devices, the data must be stored in an encrypted container. • For Mobile devices, HealthEdge must have the ability to remote wipe the encrypted container. • Must not be stored on connected external storage. • Unless an exception is granted, an end compliance solution must deny external storage devices. • Paper/hard copy cannot be stored where others can access it.	No restriction
Removable Media	• Must not be stored on removable media. • If an exception is granted, the drive must be secured using encryption.	• Must not be stored on removable media. • If an exception is granted, the drive must be secured using encryption.	No restriction
Transmission	• Encryption is required (i.e., TLS 1.2). • Must not be transmitted via email unless encrypted. • Must not be transferred outside of HealthEdge unless encrypted. • Must have a Data Loss Prevention system to prevent unauthorized information from leaving HealthEdge.	• Must not be transferred outside of HealthEdge unless encrypted. • Must have a Data Loss Prevention system to prevent unauthorized information from leaving HealthEdge.	No restriction
Disposal	• Paper and hardcopy must be securely destroyed via	• Paper and hardcopy must be securely destroyed via	No restriction

Control	Confidential	Private	Public
	approved shredder or third-party vendor. • Electronic media (CD, tapes, hard drives) must be securely destroyed by an approved party.	approved shredder or third-party vendor. • Electronic media (CD, tapes, hard drives) must be securely destroyed by an approved party.	

2.7 Data Retention and Destruction

- Management of data assets through their lifecycles should follow proper retention and disposition requirements to minimize the data that must be managed and protected. The following retention and destruction requirements must be met:
    - Retention and destruction of HealthEdge Data must comply with all legal, regulatory, and contractual obligations.
    - Ensure that surplus equipment is stored securely while not in use and disposed of or sanitized when no longer required.
    - Data retention must follow the Data Retention Policy which provides guidance for data lifecycle management, identifies the different types of data, and specifies the length of time data must be retained.
    - Destruction of data should follow the Data Retention Policy which governs the disposal of data once it has reached the end of its lifecycle.
    - More information can be found in the Data Retention Policy.

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, 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	MA-2, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, PE-22
HITRUST	0301.09o1, 0305.09q1; 0408.01y3, 0701.07a1, 1114.01h1, 1767.07d1, 1871.08f1, 1793.10a2, 18122.08k1, 18127.08l1, 0301.09o1, 0305.09q1, 0408.01y3, 0701.07a1, 19142.06c1, 10165.07e1
HIPAA & NIST SP 800-66 rev2	164.308(a)(3)(ii)(A), 164.310(a)(2)(iv), 164.310(d), 164.310(d)(2)(i), 164.310(d)(2)(iii), 164.310(d)(2)(ii), 164.310(d)(2)(iv), 164.310(c), 164.310(d), 164.312(c)

Appendix A. Calculating Classification

The goal of information security, at HealthEdge, is to protect the confidentiality, integrity and availability of HealthEdge data. Data classification reflects the level of impact to HealthEdge if confidentiality, integrity or availability is compromised.

Unfortunately, there is no perfect quantitative system for calculating the classification of a data element. In some situations, the appropriate classification may be more obvious, such as when federal or state laws require HealthEdge to protect certain types of data (e.g. personally identifiable information). If the appropriate classification is not inherently obvious, consider each security objective using the following table as a guide. It is an excerpt from Federal Information Processing Standards ("FIPS") publication 199 published by the National Institute of Standards and Technology, which discusses the categorization of information and information systems.

Security Objective	Potential Impact		
	Low	Med	High
Confidentiality **Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information**	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity **Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity**	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability **Ensuring timely and reliable access to and use of information.**	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

As the total potential impact to HealthEdge increases from Low to High, the classification of data should become more restrictive moving from Public to Confidential. If an appropriate classification is still unclear after considering these points, contact the Information Security or Legal for assistance.

Appendix B. Sensitive Data Elements

- Social Security Number
- All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89)
- Health plan beneficiary numbers
- Medical record\claim numbers
- Financial Account Number with a security code, access code or password that would permit access to the account (including debit card number)
- Driver's License or State ID Number
- Passport Number
- Passwords and/or PINs
- Digital Signature
- Tax Identification Number (EIN)
- Full name when used with Date of Birth and Birthplace.
- National identification number
- Picture of Face or fingerprints
- Digital identity
- Biometric information
- Health care/Medical information
- Credit Card Number, CVC2, PIN