HealthEquity

Privacy Policy

Original effective date:	4/29/2011
Date of last approval:	10/2/2025
Approved by:	Executive Sponsor
Business unit:	HealthEquity, Inc.
Owner:	Executive Sponsor
Executive sponsor:	General Counsel

TABLE OF CONTENTS

1 PURPOSE AND SCOPE 2
2 DEFINITIONS 2
3 RESPONSIBILITIES 5
4 REQUIREMENTS 8
4.1 Compliance with Laws and Regulations 8
4.2 Standards 8
4.3 Safeguards for Protected Information 8
4.4 Requirements for Access, Use, and Disclosure of Protected Information 8
4.5 Privacy Compliance Assessments 9
A. General/Periodic Assessments 9
B. New Product/System Privacy Impact Assessments 10
4.6 Security Risk Assessment and Risk Management 10
4.7 Operations Partners 10
4.8 Privacy Risk Management 11
4.9 Incident Management 11
A. Mandatory Issue Reporting 11
B. Breach Response 11
C. Government Agency Investigations 12
4.10 Training 12
4.11 Reports 12
5 ENFORCEMENT / VIOLATION 12
6 POLICY REVIEW 12

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

1 PURPOSE AND SCOPE

The HealthEquity, Inc. ("Company") *Privacy Policy* ("Policy") sets forth the Company's general requirements for the collection, use, transmission, storage, and protection of sensitive financial, medical, and other information. This Policy applies to all members of the workforce ("Workforce"), including Team Members, volunteers, trainees, Operations Partners, and other persons whose conduct, in the performance of work for the Company, is under the Company's direct control, whether they are paid by the Company.[1] This Policy applies to all Company affiliates and subsidiaries, unless a separate policy is approved for the specific entity.

The goals of this Policy include the following:

- Provide a high-level view of the Company's privacy obligations and emphasize the importance of sound privacy practices to the Company.
- Define governing principles for processing Protected Information.
- Define relevant privacy terminology; and clarify roles and responsibilities.
- Create a general framework for identifying, understanding, and guarding protected information, including privacy requirements.
- Require the creation of formal, topical Privacy Standards that address the many privacy laws, regulations, and practices that apply to the Company.
- Help maximize the value of data and minimize the associated privacy related risks.

2 DEFINITIONS

Listed below is a survey of privacy terminology. The list is not comprehensive but highlights major considerations and shows the spectrum of data that must be managed by the Company under various legal standards.

Category	Terms and Definitions
Protected Information ("PI")	• Protected Information is a broad category, that includes other privacy categories such as NPI, PHI, and PII (defined below). • Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, Protected Information is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online

[1] This definition is based on the HHS definition of "Workforce". See 45 CFR § 160.103 – Definitions, available at https://www.law.cornell.edu/cfr/text/45/160.103 (last visited 9/3/2025).

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

	contacting of a specific individual is the same as Protected Information. This information can be maintained in either paper, electronic or other media.[2] • The Company does not collect Protected Information from children under the age of 18, however, plan sponsors and participants, and HSA owners may upload dependent information for payment or recordkeeping purposes.
Nonpublic Personal Information ("NPI")	Product: HSA, Commuter, Dependent Care FSA, Employer-Sponsored Programs subject to GLBA (check with Privacy Team) Source: Account holder directly or through their agent (e.g., employers/partners) Owner: HSA Custodian, subject to IRS record retention requirements • Defined by the Gramm Leach Bliley Act ("GLBA") Privacy Rule. • Any "personally identifiable financial information" that a financial institution[3] collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available".[4] • NPI includes, among other things, an HSA member's name and contact information, information submitted an individual (either directly or through an employer or other agent) in an HSA application, transaction information, and the mere fact that an individual has an HSA administered by the Company.
Protected Health Information ("PHI")	Client PHI Product: Health FSA, HRA, Retiree HRA, Continuation Coverage (e.g., COBRA, Direct Bill), Employer-Sponsored Programs subject to HIPAA (check with Privacy Team) Source: HIPAA covered entity (and related parties) Owner: HIPAA covered entity / plan participant • Defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). • The HIPAA Privacy Rule provides federal protections for PHI held by HIPAA covered entities and business associates and gives patients an array of rights with respect to that information.[5] • The Privacy Rule protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information PHI. "Individually identifiable health information" is information, including demographic data, that relates to: (i) the individual's past, present or future physical or mental health or condition, (ii) the provision of health care to the individual, or (iii) the past, present, or future payment for the provision of

[2] Department of Labor, "Guidance on the Protection of Personal Identifiable Information" available at https://www.dol.gov/general/ppii (last visited 9/3/2025). Note that this is just one definition from one federal agency. The definition might vary depending on which authority the Company interacts with and will vary from state to state.

[3] The Company is a "financial institution" when operating as the custodian of HSAs. GLBA might also apply to DCRA and Commuter services (see Section 4.4.E of Privacy Standard - Inquiry, Complaint, Incident, Breach). All new products and services should be analyzed to determine whether NPI restrictions under GLBA would apply to them.

[4] Federal Trade Commission, "How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act" > "What information is covered". Available at https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act (last visited 9/3/2025).

[5] Department of Health and Human Services (HHS), "What is PHI?" available at https://www.hhs.gov/answers/hipaa/what-is-phi/index.html (last visited 9/3/2025).

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

	health care to the individual, and that (iv) identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).[6] • The Company is not a HIPAA covered entity in the provision of products or services. Rather it is a HIPAA business associate or subcontractor business associate. Company PHI Product: n/a Source: HIPAA covered entity and employer plan participant Owner: HIPAA covered entity / teammate • The Company is a HIPAA covered entity in its capacity of an employer health plan sponsor that provides benefits to team members. • Data collected and stored in connection with the Company's employer plan is PHI and must be treated in compliance with HIPAA.
Personally Identifiable Information ("PII")	Product: Eligibility Enrollment Administration, Commuter, Employer-Sponsored Programs not subject to HIPAA or GLBA Source: Program sponsor, program participant Owner: Program sponsor • Data collected in connection with non-medical programs are not PHI but would constitute Personal Identifiable information ("PII"). The data is owned by the program sponsor and often subject to the privacy and security provisions of an agreement or other limitations. • This data is subject to state privacy laws.
Payment Card Information ("PCI")	Product: All with associated cards Source: Assoc., program sponsor, issuer / BIN owner, processor, production vendor Owner: Card issuer • See Security Standard - Payment Card Industry Data.
Internet and Potential Customer PI	Internet PI Product: n/a Source: Individual Owner: Individual • Information collected from an individual when accessing the Company website, including data collected via a webform or other method for processing user preferences, usage behavior, including location data from mobile devices, identifiable web cookies, or geolocations, etc. • Subject to state laws, such as CCPA.

[6] HHS, "Summary of the HIPAA Privacy Rule" > "What Information is Protected" > "Protected Health Information". Available at https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#:~:text=The%20Privacy%20Rule%20calls%20this,health%20care%20to%20the%20individual%2C (last visited 9/3/2025).

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

	Potential Customer PI Product: Varies Source: Individual Owner: Individual • Information collected about Company's customers and prospective customers such as, geographic location, gender, age, buying behaviors, website interaction, and communication preferences. Customer references and success stories is also Marketing Information.
Company PI and Proprietary Information	Company PI Product: n/a Source: Individual Owner: Company, subject to legal restrictions and requirements • Teammates' PII collected and processed before, during, and after employment. Proprietary Information Product: n/a Source: Company / teammates Owner: Company • Proprietary information collected or created in the ordinary course of doing business, including policies, procedures, financial records, etc.
Employer or Partner Records and Proprietary Information	Product: Varies Source: Employer or partner Owner: Employer or partner • Data collected from employers and partners in connection with Company services that belong to the employer or partner and are subject to the terms of the services agreement.

3 RESPONSIBILITIES

The teams involved in implementing this Policy are listed below, along with a description of their respective responsibilities. The list is not intended to be comprehensive; rather it illustrates the types of activities each team performs. Every member of the Workforce is required to comply with and implement this Policy.

Team	Duties
CCO (Commercial)	Marketing • Help determine how the requirements of this Policy and various Privacy Standards will be implemented in the Company's products and services. • Help ensure that statements in marketing and communications are consistent with this Policy and various Privacy Standards. • Manage Internet and Potential Customer Protected Information (both defined above) in accordance with the applicable Privacy Standard.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

	Sales • Help ensure that the provisions of this Policy and various Privacy Standards are accurately represented in sales interactions. Relationship Management • Help ensure that the provisions of this Policy and various Privacy Standards are accurately represented and enforced.
CCO (Customer)	Operations • Develop formal programs, processes, and procedures that help ensure the implementation of this Policy and various Privacy Standards. • Report operational issues that have privacy implications.
CDS	• Safeguard Protected Information when acquiring HSA portfolios and other strategic matters. • Protect Marketing Information (as defined above) in accordance with the Privacy Standards applicable to sales operations.
CFO	• Help ensure that reports are generated and maintained in accordance with this Policy and various Privacy Standards. • Assist the Privacy Team with data analytics as needed in connection with privacy events and incidents, and partner and regulatory inquiries.
CPO	• Help define and enforce the Privacy Standard – Privacy and Security Sanctions Matrix. • Protect Workplace Protected Information (as defined above) in accordance with the Privacy Standards, including standards for Consumer Privacy and HIPAA . • Implement this Policy and Privacy Standard – HIPAA Protected Health Information (PHI) in connection with the Company's internal role as a plan sponsor and benefits provider (i.e., as a HIPAA covered entity), including any necessary Notice of Privacy Practices.
CSO	• Maintain security controls, security compliance, and implements all applicable regulations, frameworks, policies, and standards for protecting information.
CTO	Information Technology • Help determine how the requirements of this Policy and various Privacy Standards will be implemented in internal systems, tools, and repositories. Technology Development • Work with the Privacy Team and the Marketing Team (Product) to implement this Policy and various Privacy Standards into Company product technologies.
General Counsel	Privacy • Monitor developments in privacy laws and regulations. • Document Privacy Standards and related procedures. • Help Company teams integrate privacy requirements into their operational processes and procedures. • Review products and recommend methods to ensure "privacy by design". • Respond to stakeholder inquiries.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

	• Define and approve privacy related forms (e.g., HIPAA authorization), privacy notices, and disclosures. • Draft privacy provisions for agreements, and for public facing terms and conditions. • Review Business Associate Agreements ("BAAs"), data security agreements, single-sign-on and data display agreements, and confidentiality agreements regarding the sharing of adjudicated claims information. See the Contracting Policy. • Approve privacy terms within Operations Partner agreements. See the Purchasing Policy and Operations Partner Program. • Perform Operations Partner risk assessments as defined in the Operations Partner Risk Management Program. • Conduct compliance reviews, and monitoring and testing activities, to ensure that this Policy, various Privacy Standards, and related processes and procedures are implemented. Guide remediation efforts. • Engage internal or external compliance reviewers to assist with evaluations or assessments (when needed). • Investigate and manage privacy events, incidents, and breaches. • Fulfill privacy incident reporting obligations defined in revenue agreements. • Lead interactions with regulatory authorities in connection with privacy matters. • Report the status of activities under this Policy to the Audit and Risk Committee ("ARC") of the Board. Internal Audit • If directed by the Audit and Risk Committee of the Board ("ARC"), review this Policy and relevant Privacy Standards to determine whether they have been properly implemented. See Audit and Risk Committee Charter, Section 5.e. Legal • Help determine whether privacy laws and regulations apply to the Company. • Assist with Privacy Standard development and document Legal Standards. • Confirm breach determinations. • Assist with government and other investigations.
Public Policy and Government Affairs	• Ensure that data used in connection with the Public Policy and Government Affairs Program is de-identified and complies with this Policy or applicable Privacy Standard.
Business Leadership Team ("BLT")	• Partner with the Privacy Team to help implement this Policy and various Privacy Standards. • Train team members and enforce the Privacy Standard – Privacy and Security Sanctions Matrix.
Workforce	• Understand the Company's privacy obligations, promptly complete required privacy training, and comply with this Policy and Privacy Standards relevant to specific job functions. • Report privacy issues pursuant to Privacy Standard – Inquiry, Complaint, Incident, Breach.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

4 REQUIREMENTS

4.1 Compliance with Laws and Regulations

The Company recognizes the need to thoroughly understand and comply with applicable privacy laws and regulations, and quickly adapt as requirements change over time. This is a key component of Company strategy, value, and culture. The Senior Leadership Team and each member of the Workforce will strive to properly protect and manage Protected Information.

4.2 Standards

To implement this Policy, the Privacy Team will (i) create and maintain formal Privacy Standards that identify laws, regulations, rules, and best practices that apply to the Company and translate them into clear operating requirements; and (ii) develop formal procedures to implement this Policy and any Privacy Standards. Privacy Standards will be owned by the General Counsel and may be approved by the VP, Chief Risk and Compliance Officer.

In addition, when needed, the Legal Team may create formal Legal Standards in support of this Policy, which will be owned by the General Counsel and may be approved by an Associate General Counsel.

4.3 Safeguards for Protected Information

The Company must implement administrative, physical, and technical safeguards for Protected Information, as required by applicable regulations and best practices. Applicable regulations and frameworks include NIST Cybersecurity Framework, NIST Privacy Framework, the HIPAA Privacy and Security Rules, HITECH, GLBA Privacy and Security Rules, and other applicable security regulations.

Type	Description
Administrative Safeguards	The Company develops, implements, and enforces policies and procedures that Workforce members must comply with to protect information.
Physical Safeguards	The Company physically protects or prevents access to resources. For example: security guards, restricted areas, and ID badges.
Technical Safeguards	The Company deploys information technology safeguards, such as password and authentication schemes, encryption, and identity and access management.

4.4 Requirements for Access, Use, and Disclosure of Protected Information

Workforce Members must comply with applicable regulations, privacy and security policies and standards, and contractual obligations when accessing, using, or disclosing Protected Information. Although requirements differ based on the type of Protected Information (e.g., PHI, NPI, or PII), the requirements listed below apply to all types. Workforce Members who are storing Protected Information outside of systems of record are accountable for access, use and disclosure of that

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

information until it is deleted. Specific requirements are defined in the applicable Privacy Standards, including Consumer Privacy, GLBA, and HIPAA.

Requirement	Description
Authentication	The process of proving that an individual or entity is who they say they are prior to granting access or disclosing Protected Information.
Authorization	The consent by the individual to use or disclose Protected Information to another individual or entity for a purpose not otherwise permitted by applicable regulations. Note: HIPAA authorizations must be in writing and include all HIPAA authorization requirements.
Job-related Necessity	Access and use are restricted except as required to perform job-related duties.
Minimum Necessary	Workforce members may only access the Minimum Necessary Protected Information to perform a job-related duty. Minimum necessary means: • Protected Information may not be accessed, used, stored or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. • The Company is required to evaluate its practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of Protected Information. • That systems and processes are designed to be sufficiently flexible to accommodate the various circumstances Company may face.
Marketing	Marketing is a communication about a product or service encouraging the recipient to purchase or use the product or purchase. Protected Information must not be used for marketing purposes without approval from the Legal and Privacy Teams. Express authorization from the individual (an opt-in) or an opt-out may be legally required.
Sale	The Company does not sell Protected Information for any reason. Sale may include direct or indirect, monetary or non-monetary remuneration from or on behalf of the recipient. All suspected sales of Protected Information must be reported to the Privacy Team for review.
Inappropriate access	Inappropriate use, access, or disclosure of Protected Information is a violation of this Policy and may result in disciplinary action as defined in the Privacy Standard – Privacy and Security Sanctions Matrix.

4.5 Privacy Compliance Assessments

A. General/Periodic Assessments

The Privacy Team will perform or commission a risk analysis or assessment to evaluate compliance with new or amended legislation or regulations, contractual obligations, this Policy, applicable Privacy Standards, and related procedures. Assessments may be performed internally or by a third party. All audit findings will be documented and remediated by the appropriate business owners.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

B. New Product/System Privacy Impact Assessments

The Privacy Team must be engaged to perform an assessment whenever a new product or data processing system is proposed, or revisions are made to existing data practices. The business owner or sponsor of such new product or data processing system will complete a privacy assessment in accordance with the Privacy Standard - Privacy Impact Assessments.

The assessment will evaluate the following:

- How information will be collected, accessed, stored, protected, shared, retained, and destroyed;
- Appropriate documentation in data and system inventories;
- Controls for the entire information life cycle of the data;
- Appropriate contracts when data will be accessible or used by a third party;
- Administrative, physical, and technical controls;
- Designated leader responsible for protection of the information and compliance with applicable law, policy, and contract;
- Use of third-party devices and data storage; and
- Auditing and monitoring of access and data use.

The results of assessments will follow the process set forth in the Privacy Standard - Privacy Impact Assessments. Completed assessments and supporting material will be retained in accordance with the Record Retention Policy.

4.6 Security Risk Assessment and Risk Management

The Risk & Security Team will perform or commission an annual risk assessment (called risk analysis under the HIPAA Security Rule) to identify potential threats and vulnerabilities to the confidentiality, integrity, and availability of Protected Information and to develop strategies to mitigate risks efficiently and effectively. Assessments may be performed internally or by a third party. Assessments must include NIST, HIPAA Security, and GLBA Security, and other required security frameworks. All risks will be documented and remediated by the appropriate business owners.

4.7 Operations Partners

In accordance with the Operations Partner Risk Management Program, the Company will conduct appropriate due diligence reviews before and during the selection of third parties who have access or host Protected Information or process Protected Information on our behalf. Third parties must adhere to contractual terms and guidelines on data protection. The Company may disclose the minimum necessary Protected Information to Operations Partners[7] pursuant to a

[7] See Operations Partner Program.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

services agreement to assist with business operations. The services or subcontractor agreement must contain appropriate privacy and security provisions, including:

- Compliance with regulations, contractual requirements, this Policy, applicable Privacy Standards.
- Adherence to appropriate physical, administrative, and technical safeguards.
- Right to audit all Protected Information related activities in conjunction with the performance of services.
- Requirement that all inappropriate use or breach of Protected Information be reported.
- Full cooperation with the Company in its investigation of and response to security incidents.
- A business associate agreement, if applicable.

4.8 Privacy Risk Management

The Company uses the NIST Privacy Framework to help manage risk and fulfill privacy obligations.

4.9 Incident Management

Depending on the type of information, the violation, and the applicable regulations, the Company may be subject to government fines, penalties, and compliance plans for failure to protect Protected Information. Workforce members may be held liable as well. Certain breaches require media reporting and pose a substantial reputational, operational, financial, and legal risk to the Company.

A. Mandatory Issue Reporting

All Workforce members must report all potential or actual privacy incidents and issues to the Privacy Team using an approved method. Approved reporting procedures are defined on the Privacy Workvivo. The Company will not retaliate against an individual for reporting an incident or issue. Anonymous reporting is available via the Company hotline, refer to the Whistleblower Hotline Workvivo for information.

B. Breach Response

All issues will be fully investigated and assessed for reporting requirements under applicable federal and state regulations, including state security breach notification laws and FTC breach notification requirements.[8] The Privacy Team will coordinate all reporting requirements with the appropriate clients, plan sponsors, health plans, and teammates as outlined in Privacy Standard - Inquiry, Complaint, Incident, Breach; the Privacy Event Response Plan; Security Incident Response Plan; and applicable contracts. The Privacy Team will participate in all privacy and security desktop drills, including breach response.

[8] 16 C.F.R. § 314.4

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

C. Government Agency Investigations

Upon receiving a request for information from a government agency, the Privacy Team will notify the Legal Team immediately, determine whether Attorney Client Privilege is appropriate, and engage appropriately with the government agency. Please see the applicable Privacy Standards for more information about government agency oversight for specific types of Protected Information.

4.10 Training

The Privacy Team develops and delivers mandatory annual training. Training is mandatory for all Workforce members and must be completed within 30 days after initial access to Company information and systems and repeated annually. Training, in response to an incident, is required to help prevent the issue from recurring. Other ad hoc training, such as role-based or department-specific training, may also be required.

4.11 Reports

In accordance with Section 6.d (Oversight of Risk Management) of the Audit and Risk Committee Charter of the Board of Directors, the head of privacy will "regularly" provide reports to the Audit and Risk Committee ("Committee") of the Board and "at least once a year … shall submit [a report] to the Committee on activities undertaken during the year".

The annual report will summarize the following:

1. Important new legislative or regulatory developments and their impact to Company operations.
2. Significant privacy related initiatives and how they align with Company strategy.
3. Efforts to ensure the implementation of this Policy and important Privacy Standards (e.g., results of reviews and audits, training activities, etc.).
4. A summary of significant privacy events or incidents, and remediation efforts.

5 ENFORCEMENT / VIOLATION

Compliance with this Policy and related Privacy Standards are required. Noncompliance may result in disciplinary action as outlined in the Privacy Standard - Privacy and Security Sanctions Matrix. Any exceptions must be approved by the head of privacy and Executive Sponsor of this Policy, following processes defined by the Risk & Security Team (Enterprise Risk).

6 POLICY REVIEW

The policy owner will review this Policy annually.

© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

Approval Certificate

Docusign Envelope ID: 1555BB38-D5B8-4674-B9E9-50CFCD6FE9E1

Privacy Policy

APPROVER

Title	Name	Signature	Date
General Counsel	Del Ladd	DocuSigned by: Delano Ladd 7E91BB0AA624C2...	10/02/2025

REVIEWERS

Title	Name	Signature	Date
VP, Chief Risk & Compliance Officer	Matt Fleming	DocuSigned by: Matthew Fleming 08B012ADF8C24D9...	09/30/2025
Privacy Director	Justin Pingel	Signed by: Justin Pingel 78D038D395554FA...	09/03/2025
Sr Program Mgr, Data Privacy	Tina Bunn	Signed by: Tina Bunn B0F75A638D674DB...	09/04/2025

© 2025 HealthEquity, Inc. Proprietary and confidential.

APPROVED (as to form) DS TL DS FS