HealthEquity

Cybersecurity Incident Response Plan

Original effective date:	12/4/2014
Date of last approval:	9/29/2025
Approved by:	Executive Sponsor
Business unit:	HealthEquity, Inc.
Owner:	Executive Sponsor
Executive sponsor:	CSO

TABLE OF CONTENTS

1 PURPOSE AND SCOPE 4

2 THIS OPERATIONAL PLAN VS. TECHNICAL INCIDENT RESPONSE PLANS 4

3 OVERVIEW AND FRAMEWORK 4

3.1 Cyber Incident Response Procedure Summary 6

3.2 CIRT Activation Process Flow Illustration 9

A. Incident or Breach Process 9

B. High-level Strategy and Intelligence Lifecycle 11

3.3 The Three Pillars of Incident Response and NIST 800-61 12

3.4 Related Documents 12

4 ROLES AND RESPONSIBILITIES 12

4.1 Cyber Defense Operations Center (CDOC) 12

4.2 Cyber Incident Response Team (CIRT) 13

4.3 CORE Cyber Incident Response Team (CORE-CIRT) 14

4.4 Incident Management Team 14

A. Incident Commander / Crisis Leader 14

B. Deputy Incident Commander/Crisis Leader 15

C. Scribe 15

D. Business Resilience 15

E. 3rd Party Risk Management (Cyber) 15

4.5 Crisis Communications Team (CCT) 15

4.6 Associate Vice President (AVP) of Cyber Defense 16

4.7 Chief Security Officer (CSO) 16

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

4.8 Senior Leadership Team (SLT) 16
4.9 Governance Risk and Compliance (GRC) 16
A. Regulatory & Legal Compliance 17
B. Risk Assessment & Impact Evaluation 17
C. Communication & Reporting 17
D. Audit & Post-Incident Review 17
4.10 Legal Team (Compliance, Privacy, Enterprise Risk, Impact Assessment) 17
A. Legal / Compliance 17
B. Privacy 18
C. Enterprise Risk Management 18
4.11 Trusted Partners 18
A. Outside Counsel 18
B. Insurer 18
C. Public Relations 19
D. Data Breach Notification Provider 19
E. MSSP and Forensics Analysts 19
F. Ransom Negotiator 19
4.12 Fraud Response Team 19
A. Fraud resulting from a cybersecurity deficiency 20
B. Fraud involving cyber indicators of compromise (IOCs) 20
C. Fraud incidents with potential systemic or large-scale impact 20
4.13 Third Party Risk Management Response Team 21
4.14 Privacy Response Team 22
5 PROCEDURES 22
5.1 Cybersecurity Incident Detection and Reporting 22
A. Detection 22
B. Detection by Team Members, Contractors, and Clients/Members/Account Holders 23
5.2 Cybersecurity Incident Analysis and Incident Level 24
5.3 Initial Cybersecurity Incident Notification and Cadence 25
A. Notification and Engagement 25
B. Communications Coordination 26
C. Insider Threat Incident Notifications 27
5.4 CIRT Response and Recovery Management Activities 27
5.5 CIRT Succession of Command 28
5.6 Cybersecurity Incident Containment, Eradication, and Recovery 28

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

A. Containment 28
B. Evidence Collection and Preservation 29
C. Eradication and Recovery 30
5.7 Crisis Communications Team Engagement and Coordination 30
5.8 Trusted Partner Notifications and Regulatory Reporting 31
5.9 Post-Incident Root Cause Analysis and After-Action Report 31
A. Root Cause Analysis 31
B. Lessons Learned and the After-Action Report 32
C. Evidence Gathering and Handling 33
6 TRAINING AND EXERCISING THE PLAN 33
7 CIRP REVIEW 33
8 APPENDICES 34

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

1 PURPOSE AND SCOPE

The HealthEquity, Inc. (“Company”) *Cybersecurity Incident Response Plan* (“CIRP” or “Plan”) outlines the procedures and describes the roles and responsibilities of the Cybersecurity Incident Response Team (“CIRT”) intended to support codifies procedures for handling cybersecurity-related incidents.

The CIRP applies to all Company team members, including, but not limited to, full-time employees, part-time employees, trainees, volunteers, or other worker who is under the direct control of the Company (collectively “team members”), as well as Company contractors and vendors. The CIRP is for use by the Cyber Defense Organization (CDOC) and any member of the CIRT.

Cybersecurity incident response is an organized approach to address and manage activities upon detection, during, and after a cybersecurity incident, that could include a data breach. The goal of cybersecurity incident response is to handle the situation in an organized and effective manner that limits damage to the Company and reduces recovery time, cost, and reputational harm. The CIRP provides guidelines on what constitutes an incident and the process to be followed when a cybersecurity incident occurs.

2 THIS OPERATIONAL PLAN VS. TECHNICAL INCIDENT RESPONSE PLANS

This Plan focuses on organizing the holistic response to a major cyber incident leveraging our crisis management framework as well as best practices drawn from numerous cyber incidents and national standards. Our challenge is to meet the technical, regulatory, operational, reputational obligations in the defense and recovery of our systems as well as advise business and operational leaders of their actions so that the business can indicate and coordinate with its stakeholders.

For large scale incidents, the Company uses the Crisis Management Team as its overall incident response team while the highly technical requirements would have to be executed by our cyber incident responders in collaboration with our internal teams and partners in order to protect Company assets, systems, platforms, and network infrastructure. For a cyber incident specifically, simultaneously with the technical responders working rapidly to minimize the damage or investigate the compromise, the CMT is augmented with additional SMEs from across the business to manage the crisis and this is forms our Cyber Incident Response Team (CIRT). This operational plan’s focus is on the incident response work to protect the Company’s reputation by meeting our obligations to our members, clients, partners, and brokers to protect their information and ensure accurate and timely reporting during and after the incident resolution.

This Plan helps illustrate how this process scales as needed providing the Incident Commanders in our Security and Resilience Organization’s the flexibility to adapt the necessary team and approach to address the specific threat to the Company.

3 OVERVIEW AND FRAMEWORK

The Cyber Incident Response Annex outlines the procedures and responsibilities intended to guide the Company in the event of a potential or confirmed Priority 1 "Cyber Crisis" affecting

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

financial data, Company proprietary data, Protected Health Information (PHI under HIPAA), Non-public Personal Information (NPI under GLBA), Payment Card Industry (PCI) data, or other sensitive data.

Execution of this annex is the responsibility of the CIRT. The CIRT is a cross-functional specialized subset of the Crisis Management Team (CMT), combined with outside consultants, that is directly responsible for leading response and recovery activities for a cyber incident. Given the variation of complexity and potential for rapid escalation within a cyber or technology incident, several members of CIRT require early engagement to affirm response options, position resources, and prepare communication. These members comprise the CORE-CIRT, who are often alerted to lower-severity incidents with the potential for escalation without diverting the day-to-day activities of the broader CIRT.

The CIRT works closely with technical incident responders, Senior Leadership Team (SLT) and other experts to ensure a holistic response and mitigate additional risks. The CORE-CIRT will determine whether to activate the full CIRT, utilizing this annex (or portions thereof) based on the following:

- The number of affected members
- The number of impacted clients
- The nature of the cyber crisis (including the threat actor)
- The likelihood of media attention
- Any regulatory or compliance obligations
- As directed by Legal or designated leadership

This annex aligns with, and supplements protocols laid out in the Crisis Management Plan which are managed by the Business Resilience Team.

<u>Key Response Objectives include:</u>

- Provide CIRT members direction for all response and recovery activities.
- Minimize decision-making time in response to a cyber incident.
- Ensure stakeholder accountability by clarifying responsibilities.
- Support Compliance with regulatory and contractual notification obligations to affected parties and regulatory authorities.
- Provide clear lines of communication and quick dissemination of information to key internal and external stakeholders.
- Share only vetted, accurate information through appropriate channels.

The Cyber Incident Response Plan Annex will be updated and disseminated at least annually. The Chief Security Officer is the plan owner and is accountable for reviewing and updating the annex in coordination with the Business Resilience Program Director, who is responsible for maintaining, training, exercising, and ensuring dissemination to all CIRT/CMT members. This Plan Annex is distributed to CIRT members and is stored in Fusion Risk Management and with the CDOC.

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

3.1 Cyber Incident Response Procedure Summary

This summary provides a high-level overview of the Annex and initial CIRT actions, detailed below. Usage of the summary process portion is only meant as a quick reference in the event a member is not familiar with the CIRP or time is of the essence. The summary guidance is NOT meant to replace the information within this document, supersede the guidance and direction of legal counsel, or replace appropriate playbooks and tactical/ technical workflows that are specific to a department or response team. Individual teams should build their own tailored checklists or standard operating procedures to capture specific tasks that should be executed in their own area of responsibility.

This procedure guides a structured response by the CIRT to a Priority 1 or 2 cyber incident. This process does not outline the technical security actions, investigative steps, or data recovery procedures that may be needed during a Priority 1 or 2 cyber incident. The appropriate technical teams, which have representatives on the CIRT, will undertake those actions and procedures and document them in their own runbooks and standard operating documentation.

Alert and Activation. As outlined in the Crisis Management Plan (CMP), the Company uses an established severity and escalation process to enable the appropriate management Priority (P5-P1) of an incident and for cyber incidents when the CORE-CIRT or CIRT is activated. The Company has aligned all incident designations for ease of internal coordination using the P5-1 scale with P2 or P1 being Major Incidents and potential crises.

P5/4/3 Incidents	• These are the most common cyber incidents that occur during normal business within the cyber ecosystem. • The Security Organization leverages dozens of teams, industry and government information sharing partnerships, sensors, software, and machine learning to monitor, assess, investigate, and respond to these levels of incidents. • Normally, these levels of incidents are closed out within the Security Team and rarely become P2 incidents requiring further investigation and wider engagement of incident responders.
P2 Incident	• If the CDOC investigation and analysis identify a P2 incident, CDOC should convene the CORE-CIRT to ensure their awareness and expertise is ready and available to support a potential P1 or CIRT/CMT activation. • The CORE-CIRT will receive a briefing from the CDOC and CORE-CIRT members can review and consider the illustrative investigation questions as detailed in the **Appendix.** • The CORE-CIRT may assess that full activation of the CIRT is not needed and should set a cadence to evaluate new information that may cause an escalation to P1. The CORE-CIRT will continue to be briefed and remain engaged in the P2 response/investigation. • A SME Liaison from the CIRT should be assigned to the Crisis Communications Team to review and prepare draft communications (as needed). • *Should the investigation involve PII/PHI or other client/member specific data, the Privacy Officer will be added to the CORE-CIRT for review and triage. The CORE-CIRT will evaluate the incident for potential further activation of the CIRT.*

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

	• The Legal and Privacy Teams will (i) evaluate Securities and Exchange Commission (SEC) reporting and disclosure obligations according to materiality thresholds (including stockholder, stock exchange, and Form 8-K disclosures); (ii) determine the impact on immediate or pending trade executions for members of the CIRT or those who are aware of the incident; and (iii) decide whether to impose a blackout for members of the CIRT and others involved.[1] These actions can also be re-evaluated as the incident develops. • If CDOC confirms a loss of confidentiality, integrity, or availability of the data resulting in the recommendation to escalate to a P1 Incident or upon evaluation of the threat or impact based on our severity index in **Appendix**, it will alert the Crisis Leader to activate the complete CIRT under this Plan.
P1 Incident	• Use Everbridge to activate the CIRT and convene the initial briefing within 30 minutes of activation notification. See BR-001 Everbridge Conference Call. • See BR-002 Crisis Management Team (CMT) Activation and BR-003 CMT Meeting Roll Call and Checklist to prepare for initial CIRT activation meeting. • Once activated, the CIRT will meet regularly at a cadence determined in coordination with the Chief Security Officer and General Counsel or other SLT delegates to the CIRT. • The Crisis Leader will work with the CSO and CDOC to execute the initial briefing of the CMT and other SMEs as appropriate. If the incident then warrants, the team can be scaled down with a recognition that the CMT will be kept informed electronically and reconvened when needed. • Upon activation, the CIRT shall direct the Company's response actions and provide updates to SLT and the Crisis Communications Team as appropriate. • If operating under ACP, Legal will disseminate the ACP Procedures to the CIRT. The Scribe will update MSTeams and documentation accordingly.
Investigation and Remediation	• The CSO, AVP of Cyber Defense, or their designee shall set priorities for the investigation, response and remediation to guide the CIRT in its response and recovery work. The Incident Commander will manage the response to these priorities. • At the CSO, AVP of Cyber Defense, or their designee's direction, the CDOC team will investigate and remediate the incident as outlined in their procedures specific to the type of compromise. These tasks could include performing the necessary actions to prevent the incident from affecting additional Company resources including: ○ Identifying if other Company systems have been compromised, including incident communications (email/Teams). ○ Eliminate vulnerabilities that allowed the incident to occur. ○ Undo any undesired changes that resulted from the incident. ○ Determine the cause of the incident and update resources to prevent the incident from reoccurring. ○ Perform restoration procedures to return to normal operational state. ○ Perform necessary testing to ensure the correct functionality of the system. ○ Determine the need to collect and preserve evidence. • The CSO or designated member of the CDOC team will provide the CORE-CIRT or the activated CIRT with regular updates regarding critical details, including progress, impacts, and resource requirements. • The Crisis Leader, Technical IC, CSO, and AVP of Cyber Defense must define and manage the tempo for these regular updates to maintain situational awareness

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

	and the appropriate cadence to undertake necessary response activities without adversely impacting the technical investigative work. • At a minimum, an incident update must be provided daily during any CORE-CIRT/CIRT activation and in advance of any activation-related briefing to the SLT. • The Crisis Leader will work with the CSO, AVP of Cyber Defense, and assigned attorney to evaluate additional outside SME additions (Call Center support, Outside Counsel, MSSP, PR Firm) to the CIRT beyond those called for in this Plan. • If additional contracted resources are not already available, the Crisis Leader will coordinate with Procurement and Legal for the rapid acquisition of the requested additional support.
Communication Content, Strategy, Legal Review and Execution	• The Crisis Communications Team (CCT), a specialized group of CIRT members and SMEs, is responsible for all communications strategies and content related to the incident. A Crisis Communications Team Lead is designated specifically to ensure coordination of all development, modification, review, approval, and distribution of critical communication artifacts, media statements, talking points, or other messaging. The Crisis Communications Team members are embedded within the CMT. The CCT Lead or On-Call is also a member of the CORE-CIRT and is available to support incident response regardless of the severity level of incident. *Reminder that no one is approved to talk to the media unless designated as a spokesperson for that purpose. All Media/external requests for information should be directed to the CCT for management.* • The CCT will convene immediately upon the CIRT's activation to begin developing a communication strategy for the specific cyber incident. If necessary, they will leverage the appropriate pre-approved holding statement(s). • All communications will be developed and vetted by the CCT in accordance with our review process as established with the Legal/Compliance team. • A CDOC Liaison to the CCT should be designated to ensure that communications requests do not impede the incident response. To reduce communications briefing fatigue among those CIRT team members that may be needed as spokespersons or as Liaisons to the CCT, establish two teams: ○ TEAM ONE: composed of senior leadership, will address meeting requests from specific employers and partners, and ○ TEAM TWO: composed of other CIRT team members (i.e. Client Services), will address meeting requests from less critical partner and employer relationships. • The CCT Lead will provide regular communications updates during CIRT meetings and as needed as part of the Incident Commander’s core team and is responsible for managing the work of external PR consultants added to the CCT. • The CCT Lead will schedule an Internal CIRT member meeting before any more prominent conference calls to prepare the internal team, client-facing teams, or any spokespeople.

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

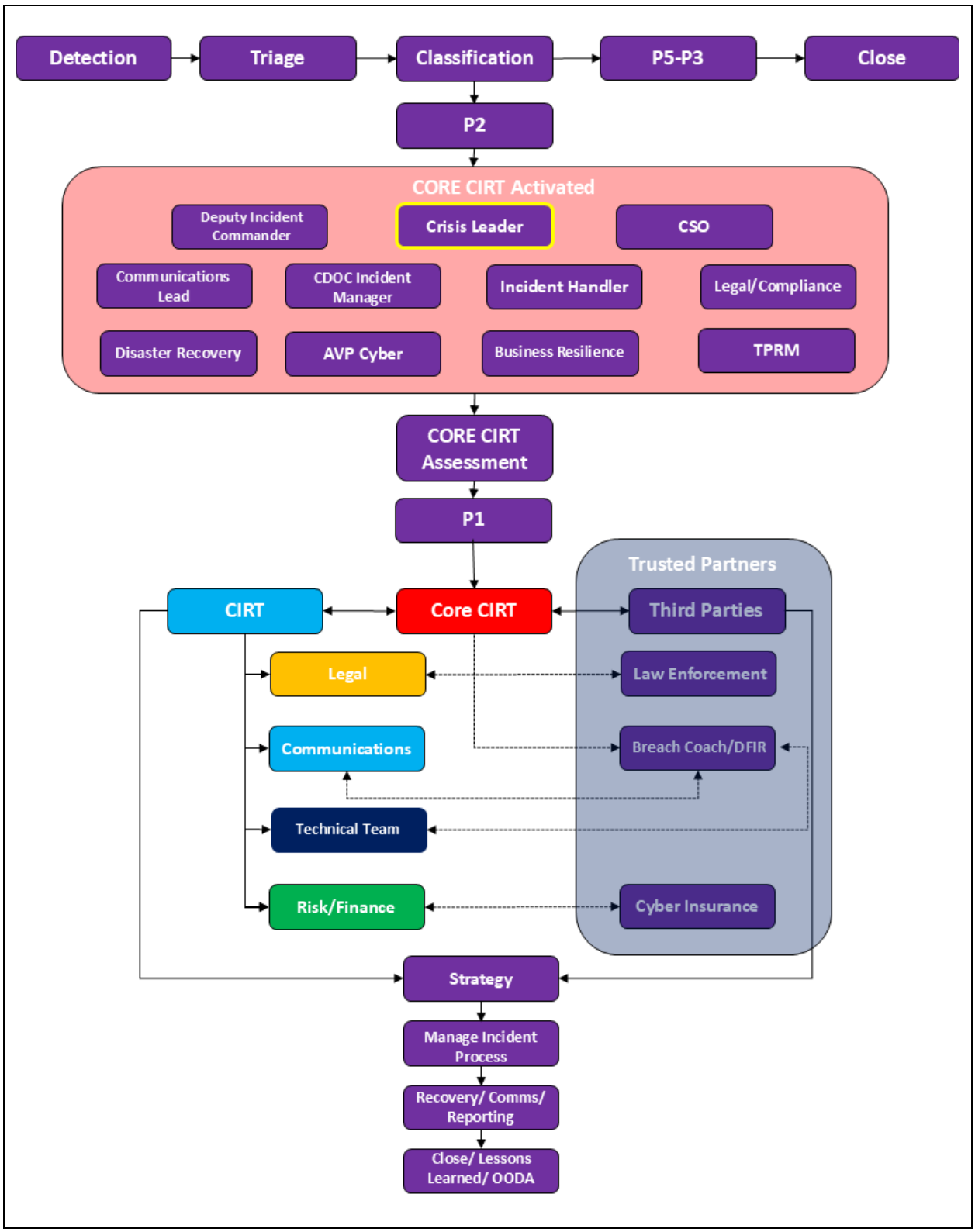
Incident Management	• Once activated, the CIRT will meet regularly at the direction of the Crisis Leader to develop, coordinate, and execute the Company's management of the cyber incident. In conjunction with the General Counsel or other SLT delegates to the CIRT, the Crisis Leader will be responsible for setting the cadence for briefing the SLT on the incident. • The Crisis Leader will designate a "Scribe" as well as a "Fusion Manager" to ensure documentation of the incident timeline as well as critical actions requiring completion. • The Scribe will ensure that all responders are documented, and appropriate ACP documentation is understood and access to incident management communications channels maintained. • The Fusion Manager will ensure access to relevant continuity documentation as well as support incident reporting, and any logistical needs. • The CIRT should plan for the incident to unfold over a prolonged period and may require additional team members to be assigned to the CIRT for specific tasks or functional coverage.
Deactivation	• Once activated, the CIRT may only be deactivated at the direction of the CSO, Incident Commander or their designee upon recommendation SLT. • The CIRT will not be deactivated until all material investigation, remediation, and communication activities are complete to standards and priorities agreed upon by compliance, regulatory, and contractual requirements. • A smaller team may need to be designated with a project manager to ensure that the remaining recovery and remediation activities are tracked and executed. • After the CIRT is deactivated, close out actions will transition to Compliance and Privacy and other Company teams for any additional follow-up items related to the cyber incident. CIRT members or their organizations may continue to be engaged as needed to manage communications and customer support.
Root Cause Analysis, Lessons Learned and the After-Action Report	• A Root Cause Analysis will be completed following the incident led by the CDOC or ITSM organization per our existing RCA processes. • Under the direction and oversight of the Chief Risk and Compliance Officer, the Resilience Program Director will organize and conduct the after-action review following the P1 incident. Participants should include the CIRT, SLT, the CDOC team and any other SMEs in separate discussions. • The after-action process will include reviewing the current Cyber Incident Response Plan Annex for lessons learned and capturing edits that should be made to mature the Annex and cyber incident training and processes further.

3.2 CIRT Activation Process Flow Illustration

A. Incident or Breach Process

The diagram below outlines the process in the event of an incident and/or breach:

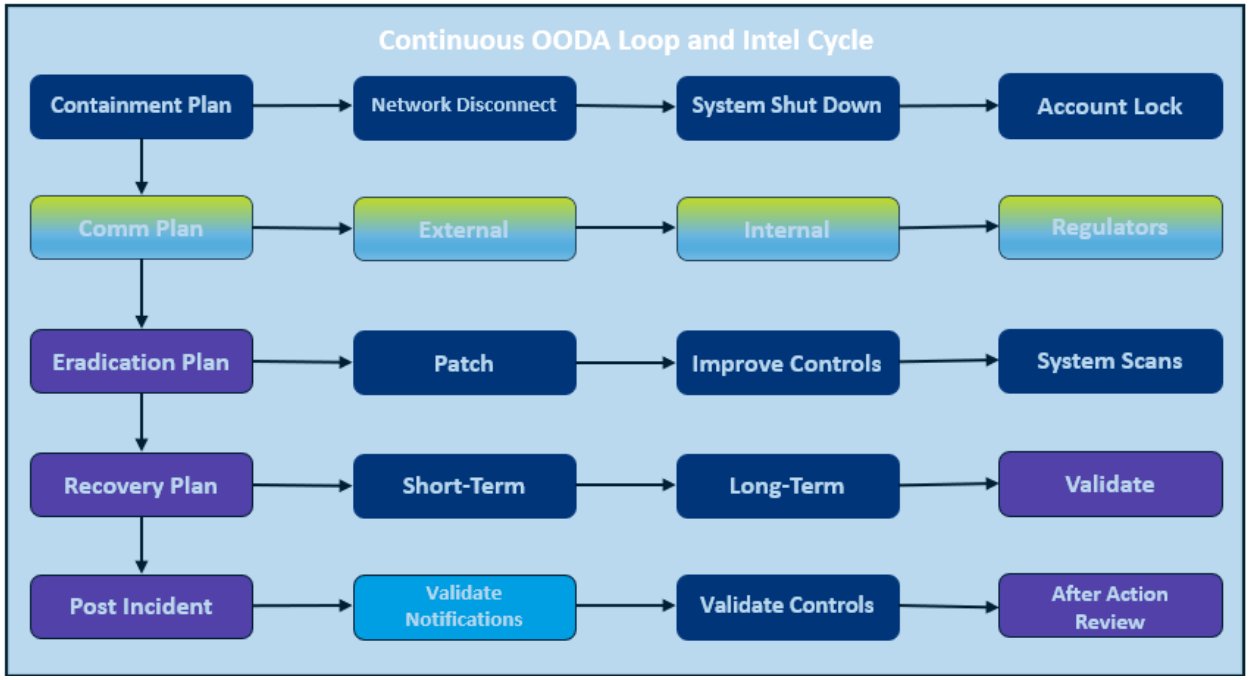
© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

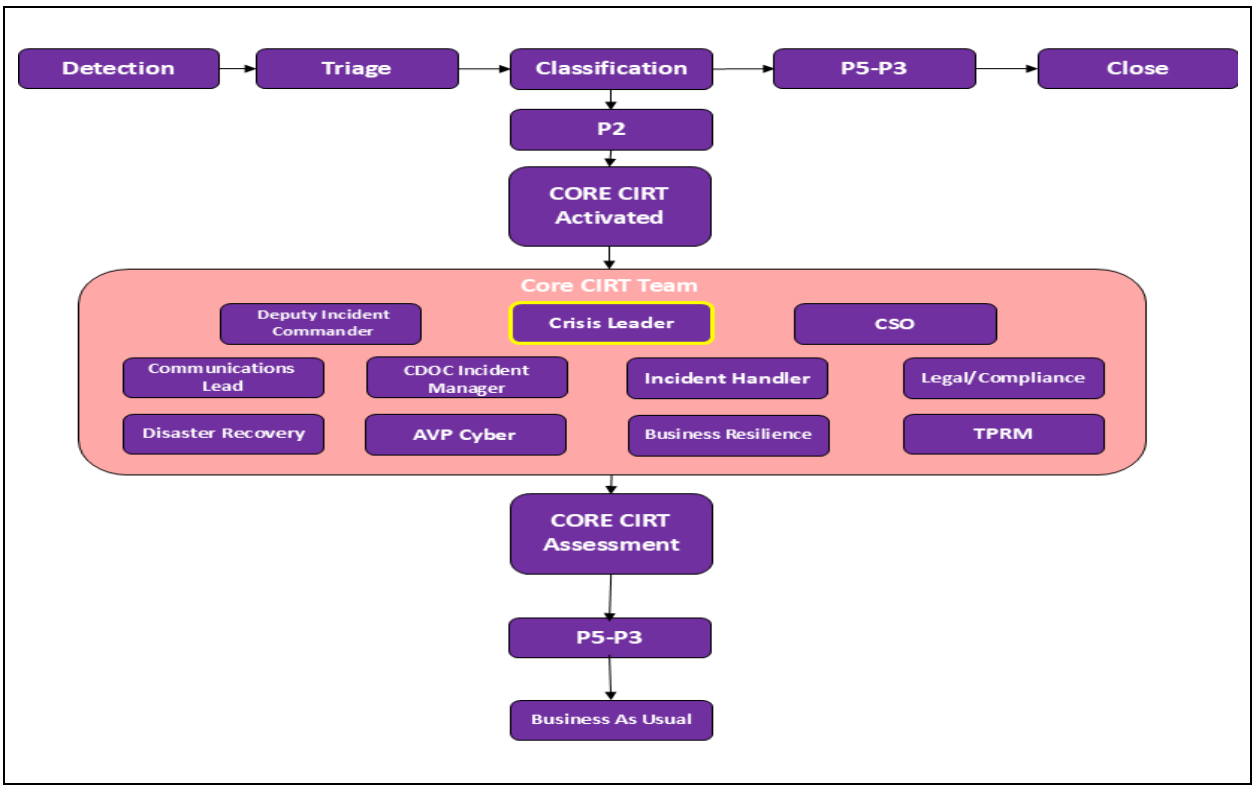


© 2025 HealthEquity, Inc. Proprietary and confidential, for internal use only.

B. High-level Strategy and Intelligence Lifecycle

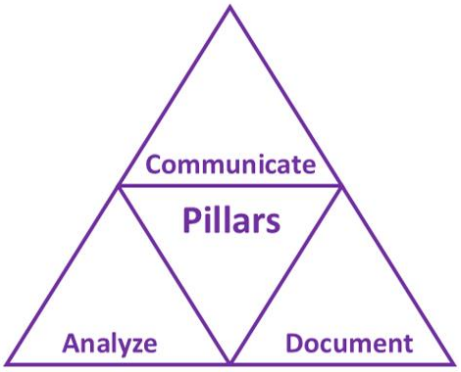
Below outlines the high-level strategy leveraging the OODA loop and intelligence lifecycle.





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

3.3 The Three Pillars of Incident Response and NIST 800-61



Incident Response is dynamic by nature but can be distilled down to three pillars: communicate, analyze and document. At a minimum, one of the three pillars should be conducted to ensure success. This by no means implies that only one pillar should be focused on for the duration of the incident response lifecycle, as all could be equally important at any given time. Alternatively, depending on the situation, one pillar may need additional focus like documentation towards the end of the incident.

The Company recognizes that the nature of our business, the clients and members we serve, as well as the data we protect, and use necessitates a range of information security tools, teams, and processes need to be used to execute an effective response. We endeavor to train our personnel to recognize the importance and interdependencies of these three pillars as well as the framework for incident management as laid out by the National Institute for Standards and Technology (NIST) Special Publication 800-61 which recognizes four main phases for the lifecycle of cybersecurity incident handling.

3.4 Related Documents

The following documents are referenced by or related to the CIRP Annex:

- See Appendix A (Security Events and Incident Definitions) for a complete CIRP definition list.
- Crisis Communication Plan managed by the Crisis Management Team
- Privacy Event Response Plan managed by the Privacy Team
- Defense Operations Team procedures managed by the Security Operations Team

4 ROLES AND RESPONSIBILITIES

The following section lays out in broad terms the types of tasks and activities various members of the CIRT will undertake when engaged in a P2/P1 incident or investigation. These activities are not meant to be exhaustive as individual teams will have their own tasks and requirements internally to execute, including critical business processes they manage.

4.1 Cyber Defense Operations Center (CDOC)

The Cyber Defense Operations Center (CDOC) is responsible for 24/7 monitoring of the organization's critical infrastructure, including servers, networks, databases, and cloud environments. The primary investigative and analytic element within the Security Department, the CDOC monitors and alerts the CIRT, CORE-CIRT, and the Extended CIRT when needed. The CDOC leads the investigation and contributes the assessment of the incident's potential impact while directing the steps needed to contain and remediate the threat.

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

The CDOC plays a central role in managing cybersecurity incidents. Its responsibilities include:

- Monitor environment to detect, analyze, and respond to cybersecurity incidents.
- Coordinating technical incident response to a cyber incident, including insider threats and significant fraudulent actions.
- Receiving and responding to reports of potential cybersecurity incidents.
- Directing the containment and eradication strategy for incidents.
- Coordinating with the Major Incident Management Team, IT and Product organizations to determine and execute containment, eradication, and recovery plans.
- Investigate the cause and impact of the security incident including interviewing team members or stakeholders to understand the incident.
- Briefing the CIRT and any other stakeholders on the incident, as directed.
- Support messaging development to ensure clear understanding of the incident.
- Prepare initial risk assessments, forensic analysis, and document a formal Incident Report including Root Cause Analysis (RCA), depending on the scale and type of incident.

4.2 Cyber Incident Response Team (CIRT)

The CIRT is comprised of the **CDOC**, **Crisis Management Team**, information security and other product **SMEs**, and outside trusted partners.

The CIRT is directly responsible for managing the Company's response and recovery from a P1 cyber or data incident. As a cross functional team, the CIRT is organized to manage the incident to prevent further loss of information, information assets, property, and customer confidence by providing a consistent approach to any event involving Company information systems, networks, or data. Specific platform and product subject matter experts (SMEs) relevant to cyber, data, or technical incident response may be added to the CIRT when needed.

If not assigned specific duties by this Plan, the Crisis Management Plan, or Crisis Communications Plan, the CIRT members should default to their functional expertise and core responsibilities as the critical expertise needed by the incident responders. Our CIRT is purposefully inclusive of numerous technical, operational, and supporting functions to ensure comprehensive and rapid access to the diversity of knowledge of the Company and its products, services, data, and platforms to ensure a robust response. CIRT team members are encouraged to develop their own operational checklists to support their participation in CIRT activations. Similar to the CMT, each function within the CIRT must have a primary member and a secondary, or back-up, member to ensure each functional capability is available and ready to support an incident, at any time.

Responsibilities of the CIRT include:

- Convene the appropriate subject-matter experts throughout the incident duration to effectively support the response and recovery.
- Lead specific workstreams as directed based on assigned timelines and cadence.
- Manage specific incident requirements assigned by the Incident Management Team.

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

- Identify and mobilize additional internal subject matter experts (e.g., product lead, R&D resourcing) that may be needed.
- Participate in any After-Action Review following recovery and report findings to management and to the appropriate authorities, as necessary.
- Collaborating with customer account managers or business units to address customer concerns related to cybersecurity incidents.
- Coordinating investigations across account, technical, and fraud teams when necessary.
- Offering internal guidance throughout the investigation on managing incident risk.

Team members must be able to reprioritize their daily responsibilities to respond to a cybersecurity incident. They must have the appropriate level of authority to make decisions regarding risk and security measures.

4.3 CORE Cyber Incident Response Team (CORE-CIRT)

This group is comprised of the following CIRT members: Crisis Leader, Deputy Incident Commander, CSO, AVP of Cyber Defense, Communications Lead On-Call, CDOC Incident Manager, Incident Handler, Legal/Compliance, Third-Party Risk Management, Disaster Recovery, and ERM/Business Resilience.

They are responsible for affirming the severity of the incident, preparing possible response options, positioning resources, and preparing communications for incidents, especially if there is no current solution, have the potential for rapid escalation or do not yet meet the threshold for activating the full CIRT. Additional SMEs can be added to these meetings at the direction of the CSO or CDOC. The CORE-CIRT will remain engaged as appropriate based on the nature of the P2 incident.

4.4 Incident Management Team

The Incident Management Team includes: IC/Crisis Leader; Deputy Incident Commander (if designated, Scribe, Business Resilience, CDOC Liaison, Third Party Risk Management (Cyber), Crisis Communications Lead, and the assigned Company Attorney.

A. <u>Incident Commander / Crisis Leader</u>

- The Incident Commander/Crisis Leader is a pre-designated individual who is responsible for the overall leadership of the CIRT throughout a P1 or P2 Cyber incident. The Incident Commander/Crisis Leader is further responsible for communicating relevant information to SLT and, as appropriate, CIRT throughout the duration of the incident. They will establish the CIRT meeting cadence, lead the CIRT meetings, and ensure the action items are executed and tracked.
- During a P2 incident, the Incident Commander will work with the CSO and CDOC to ensure appropriate awareness within the organization, as well as engagement of resources by the CORE-CIRT and other subject matter experts and third-party resources.

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

B. Deputy Incident Commander/Crisis Leader

- The Deputy Incident Commander is designated to be responsible for the governance of all crisis and incident response processes in support of the Incident Commander.
- The Deputy Incident Leader provides additional support by managing the Incident Support Staff; crisis management procedures and materials; and ensures proper situational awareness of activities, decisions and incident details.

C. Scribe

- The Scribe will be designated to assist with documenting actions taken in MS Teams chat/ Incident Ticket and other forums the CORE-CIRT / CIRT may use. They will also assist in capturing lessons learned items.
- Use of Co-Pilot or other transcription services during incidents should be approved by assigned attorney before utilized so as to ensure safe use of the AI tools, especially when referencing confidential company security information and procedures. These transcripts will then need to be retained/destroyed as directed by assigned attorney and the Record Retention Policy.

D. Business Resilience

- In support of the Scribe and other continuity requests, the Business Resilience representative uses Fusion to assist in identifying interdependencies that may be managed by critical process owners and identify plans that may need to be activated to ensure operational continuity.

E. 3rd Party Risk Management (Cyber)

- A representative of the TPRM (cyber) team may be designated to support any vendor specific risk or insights that may be necessary to inform the response impacting partners or impacting the Company from the partner.

4.5 Crisis Communications Team (CCT)

This is a specialized group comprised of CMT members and SMEs, including Communications, Service Recovery, Client/Member/Partner/Broker relations, Legal, Compliance, and outside consultants, responsible for messaging strategy and content related to the incident. To provide immediate communications expertise to an escalating incident or a declared crisis (P1), a Communications On-Call procedure has been established. A member of the Communication Team will be designated as the On-Call with the responsibility to support and triage, if necessary, incidents 24/7. In addition, this person is the Communications representative to the CORE-CIRT group and will assume those responsibilities as required. The Communications On-Call can be contacted by the CDOC through PagerDuty for automated notification or contacted directly.

Over the life of the incident, the Crisis Communications Team will:

- Lead and advise the Senior Leadership Team on key strategic messaging decisions.

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

- Develop, coordinate approvals, and disseminate approved internal and external communications
- Develop and execute an incident response communication strategy for all Company stakeholders and coordinate with approved reviewers and trusted partners, for approval before distribution.
- Monitor media coverage and distribute as needed.
- Participate in all CORE-CIRT and CIRT activities.

4.6 Associate Vice President (AVP) of Cyber Defense

The AVP of Cyber Defense serves as the CSO's principal support and trusted technical advisor, providing leadership and guidance to the CDOC, Threat and Risk Intelligence, and other cyber defense functions. This role is not part of the incident commander succession plan and does not assume direct incident commander responsibilities. Under the direction of the CSO, the AVP of Cyber Defense may act as the CSO's delegate for specific duties, including executive-level communications and representation in CIRT activities. The AVP provides strategic direction, operational leadership, and subject matter expertise to ensure effective detection, analysis, and mitigation of cyber threats, and supports the CSO in decision-making and oversight during incidents.

4.7 Chief Security Officer (CSO)

The CSO is responsible for all Information Security and Physical Security capabilities, including the Cyber Defense Operations Center (CDOC), Security Engineering, Threat and Risk Intelligence, Security Operations, and related teams. The CSO is a member of the Senior Leadership Team and serves as the primary advisor to the Executive Leadership Team on cybersecurity and physical security matters, including significant cyber incidents. The CSO provides strategic oversight for the Cyber Incident Response Team (CIRT), shaping its structure, preparedness, and overall response posture, and acts as the executive leader for incident-related decision-making

4.8 Senior Leadership Team (SLT)

The SLT plays a crucial role in any major cyber incident by setting strategic priorities, providing financial, personnel or other resources, and ensuring unity of effort across the SLT membership and the business. Additional actions could include approving or consulting on response strategies, acting as spokespersons for the corporation, as well as supporting the overall communications development and implementation with clients, members, the media and regulators (if directed).

4.9 Governance Risk and Compliance (GRC)

The GRC team is plays a critical supporting role that ensures the response is aligned with regulatory, legal, and organizational requirements. While they are typically not on the technical front lines, their work is essential for ensuring the response is defensible, coordinated, and compliant.

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

A. Regulatory & Legal Compliance

- Identify and interpret regulatory obligations related to breach reporting and data handling (e.g., breach notification laws).
- Ensure timely notification to regulatory bodies (e.g., within 72 hours for GDPR).
- Coordinate with legal teams to manage exposure and risk from a compliance perspective.

B. Risk Assessment & Impact Evaluation

- Collaborate with security and technical teams to evaluate the business risk and compliance impact of the incident.
- Help prioritize response actions based on the risk appetite and tolerance of the organization.
- Assess third-party/vendor risks if they're involved in the incident.

C. Communication & Reporting

- Ensure incident-related communications (internal and external) are accurate, complete, and compliant with disclosure requirements.
- Assist in drafting or reviewing communications to regulators, customers, and stakeholders.

D. Audit & Post-Incident Review

- Participate in the post-incident review and contribute to the lessons learned process.
- Ensure that findings are documented and used to update risk registers, controls, and policies.
- Facilitate or prepare for external audits related to the incident.

4.10 Legal Team (Compliance, Privacy, Enterprise Risk, Impact Assessment)

The assigned attorney provides legal guidance throughout the investigation or incident. This includes advising on legal and contractual obligations, potential liabilities, and public disclosure requirements (i.e. Form 8-K). They review and approve communications to stakeholders, regulators, and impacted parties, and guide the business on appropriate remedial actions. Additionally, they manage key outside partners including computer forensics, interactions with law enforcement and regulators, and outside counsel when needed. The Legal Team will also advise on whether the response will be conducted under ACP.

A. Legal / Compliance

- Advise on the wider regulatory impact of a data incident or breach.
- Support the Crisis Communications Team and perform risk analysis as required.

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

B. Privacy

- Review CDOC analysis, including impact assessments, to determine if a privacy incident occurred.
- Determine what laws and notification requirements apply to the privacy incident.
- Provide guidance internally throughout the investigation on issues relating to privacy of customer and account holder data.
- Support the Crisis Communications Team and Insurance claim requests.
- See also Privacy Event Response Plan.

C. Enterprise Risk Management

- Lead the Impact Assessment Team supported by a cross-functional team of data analysts from across the enterprise who help determine the identities of member and clients effected and the type of information disclosed as well as overall impact on the Company.
- Perform additional risk analysis as required.
- Notify and manage communications with the insurance provider regarding a claim.

4.11 Trusted Partners

During a cyber incident, the Company uses several trusted (external) partners that we may activate to support our investigation or incident response. Contact information for trusted partners is maintained in Fusion as a Roster, attached to this Plan annex. During a cyber incident, members of the CIRT, CMT, and SLT may involve trusted partners to bring specific expertise to the Company's management of the incident.

Trusted Partners for a cyber incident could include:

A. Outside Counsel

They will assist the legal department for the specific purpose of providing guidance for the Company's response and recovery efforts and steps to protect against litigation. Activation of outside counsel will be a collaborative decision made by the CSO, and Legal Department during the initial CORE-CIRT engagement. They will review and advise on all internal and external communications. Provide counsel on compliance requirements and regulations, including notification requirements under state and federal law.

B. Insurer

Our outside insurers may participate in the organization's investigation, response, and recovery efforts. In some circumstances, the insurer may also provide access to outside resources with experience in cyber incidents that can further assist the CIRT. Certain documentation, investigative data, or other details may be requested and provided to the insurer during the incident in order to access certain resources. Activating the insurer

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

during a cyber incident will be a collaborative decision made by the CRCO and Legal, with notification to the insurer broker made by Legal.

C. Public Relations

PR and crisis communications firms may assist the Company by supporting the available Corporate Communications resources through staff augmentation, strategy development, and subject matter expertise in cybersecurity and media affairs. Activating outside public relations and crisis communications resources will be a collaborative decision made by the CIRT Incident Lead, Chief Customer Officer, and the Crisis Communications Team during the initial response led by the CIRT.

D. Data Breach Notification Provider

Our response includes properly notifying those impacted by the disclosure of PII, PHI, or other sensitive data and supporting them after the incident resolves. The provider is an outside organization that assists the Company by providing trained and ready outside resources to fulfill this need and brings expertise from previously handled incidents with other organizations. The provider manages an inbound call center to take questions from impacted members or clients and attempt to answer those questions through documentation and capture information to triage escalations for resolution by the Company. They will assist in developing notification materials for dissemination, including Breach Notification Letters, Factual incident narratives and call center FAQs and scripts.

E. MSSP and Forensics Analysts

Digital forensics firms have been retained to support the CDOC and any investigative or incident response requirements. While the Security Team may elect to use existing in house or already engaged forensics SMEs, if additional support is required, and in some cases will be required for insurance purposes, the assigned attorney can engage outside counsel to initiate additional MSSP or forensic personnel.

F. Ransom Negotiator

If a ransom demand is received or ransomware discovered, a ransom negotiator has been retained through our outside counsel. Accessing the ransom negotiator requires engagement of outside counsel and invocation of ACP through the Legal Department.

4.12 Fraud Response Team

The Fraud Response Team is responsible for monitoring, investigating, and responding to fraud-related activity impacting members, clients, or partners. This includes detection of suspicious transactions, account misuse, and other activities intended to cause financial harm.

The majority of fraud incidents are managed and resolved within the Fraud Response Team without requiring engagement from the full CIRT. However, the Fraud Response Team will coordinate with the CDOC in the following scenarios:

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

A. Fraud resulting from a cybersecurity deficiency

- When fraud is committed as a direct result of a vulnerability or weakness in Company systems (e.g., credential stuffing, API exploit, malware infection).
- CDOC will lead technical containment and remediation to remove the ability to exploit.
- Fraud Team will identify impacted members, conduct notifications if needed, and ensure members are made whole.

B. Fraud involving cyber indicators of compromise (IOCs)

- When fraud patterns are linked to confirmed cyber-IOCs, Fraud will engage CDOC to coordinate technical investigation and controls.

C. Fraud incidents with potential systemic or large-scale impact

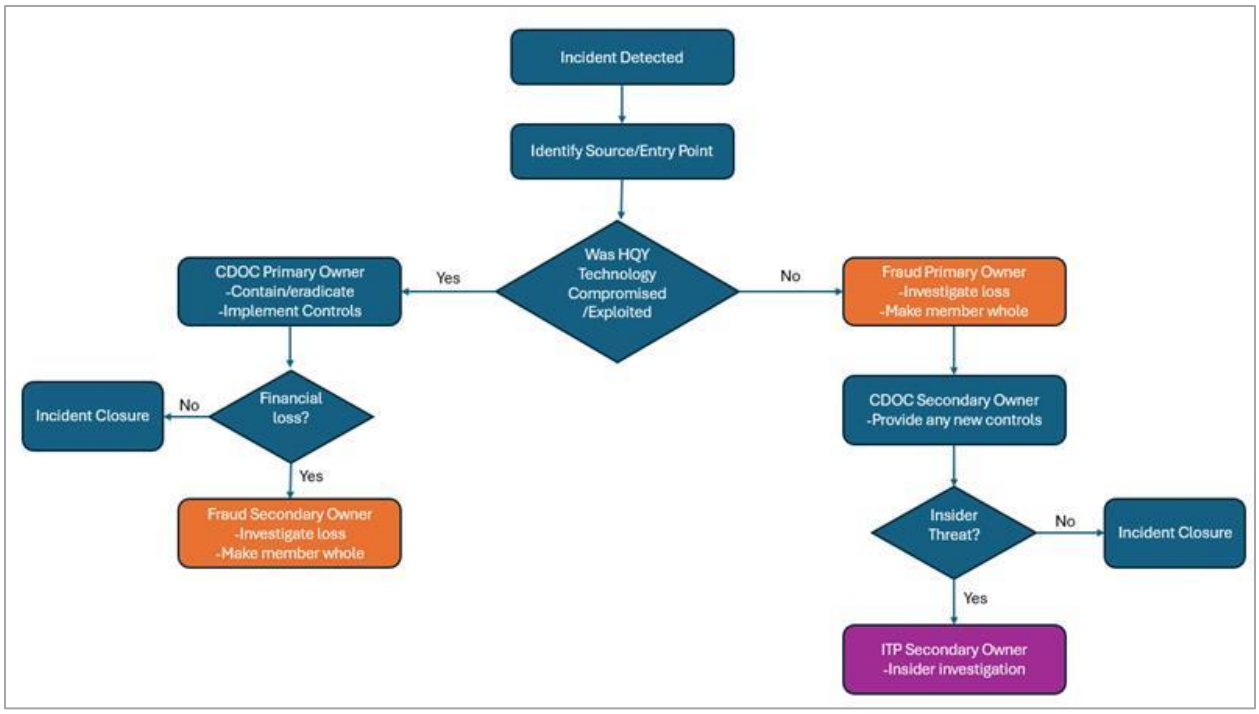
- Any fraud case that could escalate beyond Fraud Team capabilities or affect critical business operations must be escalated to CIRT-Core in accordance with Section 3.2 – Engagement Process for CORE-CIRT and CIRT in P1 or P2 incidents.

Scenario	CDOC Primary	Fraud Primary	Shared
Credential stuffing, API exploit, malware on Company infrastructure	✅	—	✅
Member socially engineered (no Company tech exploited)	—	✅	—
Generic fraud (e.g., card fraud, ID theft unrelated to the Company)	—	✅	—
Insider threat with fraudulent activity	✅	—	✅

In all shared or escalated incidents:

- Fraud is responsible for member-side investigation, loss calculation, and financial recovery actions.
- CDOC is responsible for technical investigation, containment, and preventive / detective control deployment.
- Both teams collaborate on member impact reporting and post-incident lessons learned.

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



4.13 Third Party Risk Management Response Team

The Third-Party Risk (TPR) Incident Responders are responsible for monitoring and managing security incidents involving partners, clients, and vendors. This includes evaluating potential compromise of third parties, assessing business impact, and coordinating response actions to protect the Company from downstream risk.

The Third-Party Risk Management team works in close collaboration with the CDOC to identify and investigate potential compromises of critical third parties. Both teams actively monitor threat intelligence feeds, telemetry, and alerts for signs that a partner, client, or vendor may be compromised.

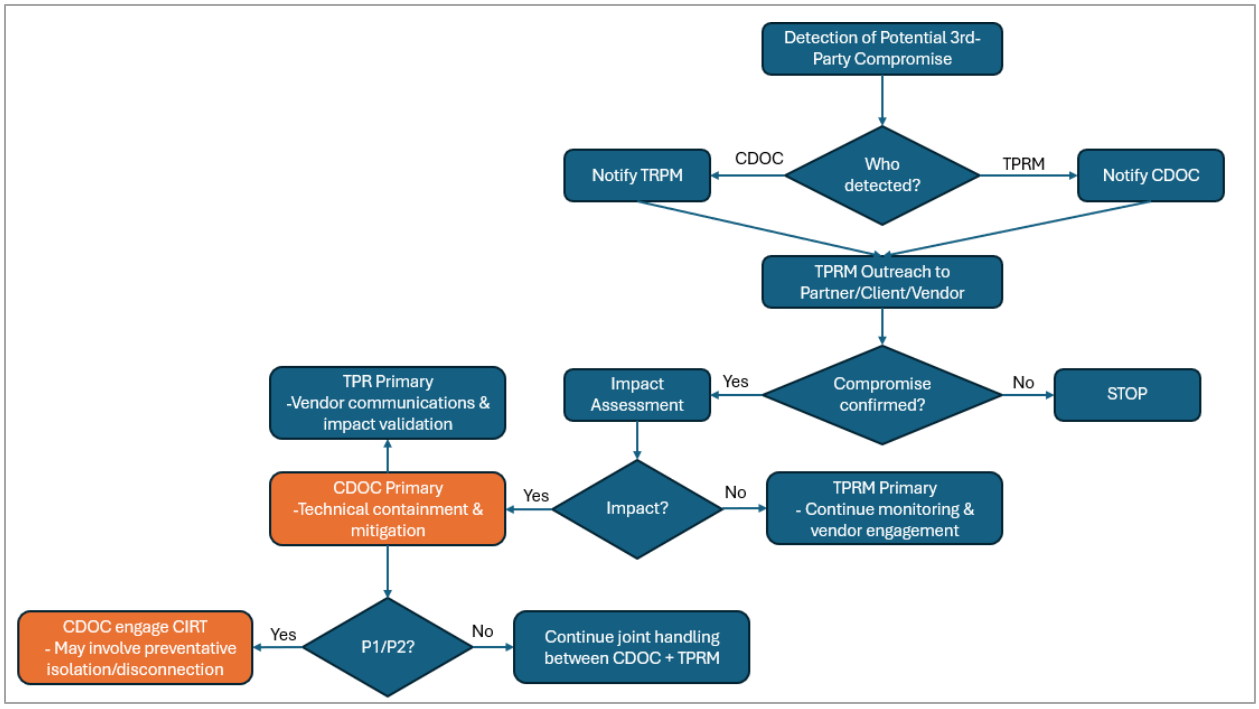
Most incidents involving potential third-party compromise are handled jointly by CDOC and Third-Party Risk without requiring engagement from the full CIRT.

In these cases:

- Third-Party Risk leads external communications with the affected partner/client/vendor.
- CDOC leads technical containment and threat hunting within Company systems.
- Both teams jointly brief CORE-CIRT on incident details, business impact, and recommended actions.

TPRM response plan is documented HERE.

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



4.14 Privacy Response Team

During a cyber incident involving personal or sensitive information, the Privacy Team is responsible for ensuring compliance with all applicable privacy, data protection, and breach notification requirements. They work closely with the Incident Response Team to determine whether personal data, protected health information (PHI), or other regulated information was accessed, exfiltrated, altered, or destroyed, and to provide guidance on containing the incident and minimizing further exposure. The team identifies relevant breach notification laws and regulatory obligations based on the type of data, jurisdictions, and impacted individuals, and coordinates with Legal and Communications to develop and execute notification plans for affected individuals, regulators, and other stakeholders.

When third parties, vendors, or business partners are involved, they act as a liaison to facilitate appropriate information sharing and coordinated response efforts. Following incident resolution, the Privacy Team participates in post-incident reviews to evaluate the effectiveness of privacy-related actions taken during the response and to recommend improvements to processes, policies, and training.

5 PROCEDURES

5.1 Cybersecurity Incident Detection and Reporting

A. Detection

The CDOC analysts lead incident detection and response efforts, leveraging the Security Information and Event Management (SIEM) platform, threat intelligence sources, and

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

behavior analytics to identify anomalous activity and potential cybersecurity incidents. The Advanced Threat Response (ATR) team works alongside the Cyber Defense Engineering (CDE) team as the primary escalation group for high-severity or complex cases, including those involving advanced persistent threats, zero-day exploits, or cross-domain attacks. Together, ATR and CDE direct eradication and cleanup activities to remove threats and restore normal operations.

Other internal IT support teams provide assistance as needed, helping to investigate abnormal system behavior or technical indicators of compromise across various assets, in alignment with Cyber Defense–led response plans. Cyber Defense teams continuously monitor the Company's environment and perimeter to detect and respond to threats to the confidentiality, availability, and integrity of our data, systems, and products.

OPERATIONAL NOTE: As of 01/01/2026, monitoring of critical system event logs will no longer be outsourced. The third-party Managed Security Services Provider (MSSP) will be decommissioned, and full responsibility for event monitoring and alert triage will reside with the internal CDOC team.

Cybersecurity incidents detected by the CDOC generally fall into the following categories:

- malware and ransomware
- unauthorized access or policy violations
- phishing and social engineering
- data loss or exfiltration
- web application attacks and cloud misuse
- insider threats
- and physical security incidents.

For definitions and response guidance, refer to **Appendix A – Security Events and Incident Definitions.**

B. Detection by Team Members, Contractors, and Clients/Members/Account Holders

Cybersecurity incidents may also be identified by team members, contractors, or our clients and member account holders. These individuals often encounter or experience incidents firsthand and play a crucial role in early detection. Commonly reported incidents include breach or suspected exposure of personally identifiable information (PII), suspected malware infections, phishing attempts or suspicious communications, improper system use or policy violations, unauthorized physical access, and issues involving third-party service providers.

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

All personnel are encouraged to report any suspicious activity immediately via approved reporting channels (e.g., ServiceNow, security email alias, or Member Services hotline). Those contact numbers include:

- For HealthEquity Team members or Contractors: Call: 480-781-4437 or email: infosec@healthequity.com
- For clients and member account holders: email: infosec@healthequity.com

5.2 Cybersecurity Incident Analysis and Incident Level

The Cyber Defense Operations Team (CDOC) is responsible for conducting detailed analysis of reported or discovered cybersecurity incidents using available data, tools, and threat intelligence to determine incident severity, priority, and potential impact. Analysts may reclassify the initial priority of an incident based on the findings of their investigation, in alignment with operational response standards and business impact.

CDOC operates 24/7 and is the primary team responsible for monitoring the Security Information and Event Management (SIEM) platform, as well as other detection and enrichment tools. These platforms provide telemetry and context that help assess the depth and breadth of malicious activity, identify affected systems, and inform containment and mitigation strategies.

For high-severity or complex incidents, the Advanced Threat Response (ATR) team provides specialized support. This includes deeper technical investigation, malware reverse engineering, adversary emulation, and guidance on containment and recovery in coordination with stakeholders.

CDOC analysts use various cybersecurity threat intelligence sources and information-sharing communities to supplement investigations. These sources provide insights such as malware behavior patterns, common lateral movement techniques, or indicators of compromise (IOCs) related to active threat campaigns.

All confirmed incidents must be documented in the CDOC SOAR Solution . Documentation must be factual, concise, and free of speculation or opinion. SNOW is also the source of record for all procedural documentation, including applicable Standard Operating Procedures (SOPs) and analysis workflows.

For specific analysis procedures related to individual incident types, refer to the relevant section under the “Analysis” portion of this document or the SOPs available within ServiceNow.

Note: HealthEquity will migrate incident documentation, workflow automation, and certain response playbooks from ServiceNow to CDOC SOAR Solution no later than January 1, 2026. SOPs and KB articles will be updated to reflect the new platform. Until the migration is complete, ServiceNow remains the official system of record.

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

5.3 Initial Cybersecurity Incident Notification and Cadence

When the CDOC verifies that a security incident meets the criteria for P2, immediate notification actions are required. CDOC's primary objective at this stage is to engage the CORE-CIRT in accordance with Section 3.2 – Engagement Process for CIRT-Core and CIRT in P1 or P2 incidents.

A. Notification and Engagement

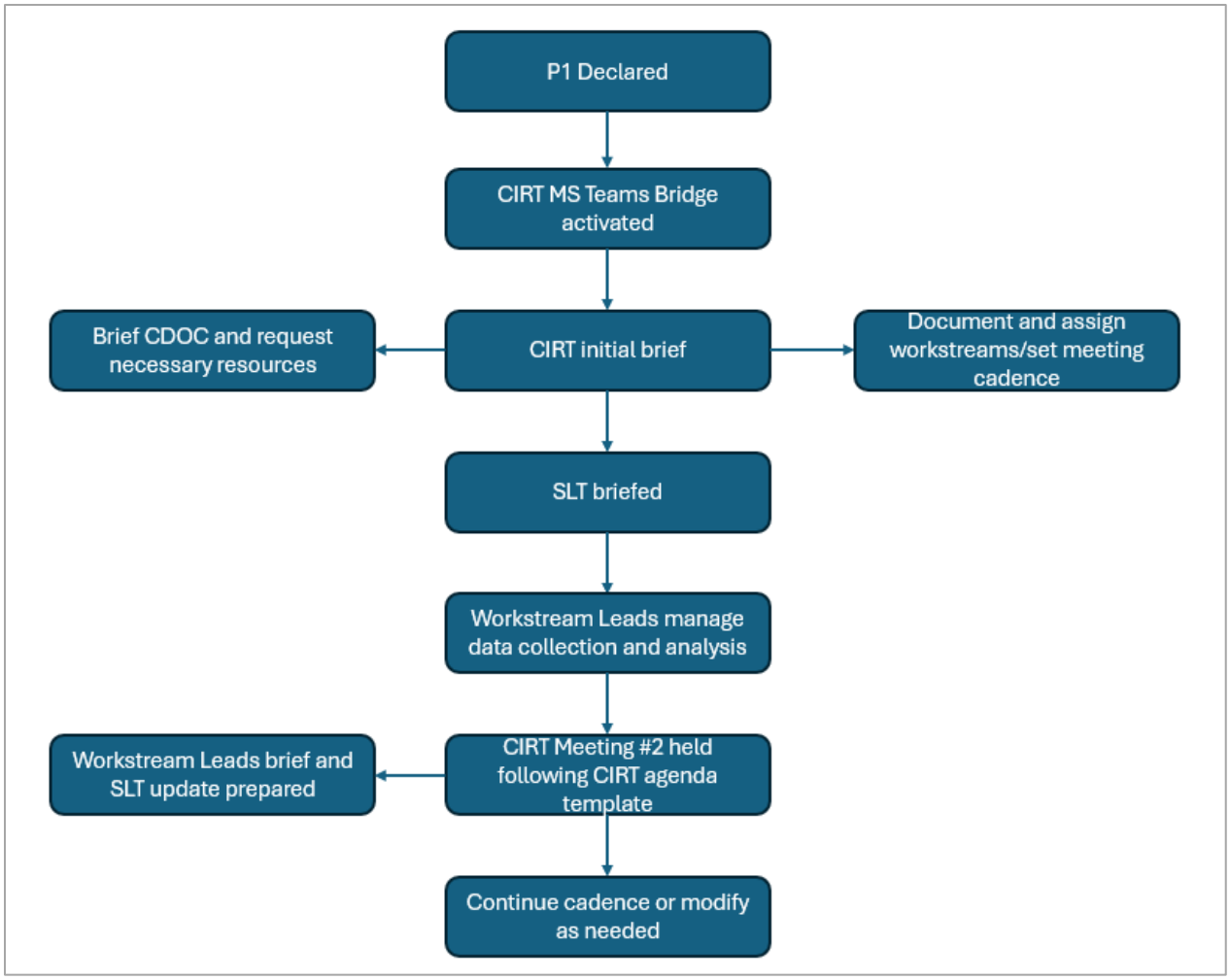
When the Cyber Defense Operations Center (CDOC) verifies that a security incident meets the criteria for a high priority incident, immediate notification actions are required. The CDOC's primary objective at this stage is to engage the CIRT-Core group in accordance with Section 3.2 – Engagement Process for CIRT-Core and CIRT in P1 or P2 incidents.

Once Activated:

- The CIRT will convene at a cadence set in coordination with the CSO and General Counsel, or other SLT delegates to the CIRT.
- The Crisis Leader, in collaboration with the CSO and CDOC, will deliver the initial briefing to the Crisis Management Team (CMT) and other SMEs as needed.
- The CIRT will direct response actions and provide timely updates to the SLT and the Crisis Communications Team.
- If operating under the ACP, Legal will distribute the ACP Procedures to the CIRT, and the Scribe will update MS Teams and maintain all related documentation.

[See diagram on next page.]

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



B. Communications Coordination

Following CIRT-Core engagement, the **Communications Team** is responsible for briefing the SLT on the status of the cybersecurity incident response according to the following cadence:

- **P1 Incident:** The SLT will be briefed within **30** minutes following the completion of the CORE-CIRT assessment.
- **P2 Incident:** The SLT will be briefed within **3** hours following the completion of the CORE-CIRT assessment.

The Communications Team maintains templates for SLT messaging. The CDOC maintains documented processes that outline:

- A checklist of technical and incident details for the initial CIRT-Core meeting are available in section 1 of the communications plan SOP. Link Here

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

- A checklist of technical updates needed to support the Crisis Communications Team in preparing all subsequent SLT communication are available in section 2 the communications plan SOP. Link Here

All technical updates provided to Communications should be factual, timely, and free of speculation.

C. Insider Threat Incident Notifications

It is possible that a cyber incident involves an insider threat. The CDOC will leverage the confidential process for managing an insider threat investigation. The scope for Insider threat incident management and communications should be limited due to their sensitive nature. The investigating team should keep only to those that need to know.

The likely team should only include the following people:

- Cyber Defense (Spencer McGalliard, Melissa Householder)
- Legal Team (Karen Clemes)
- Physical Security (Todd Palmer)
- Relevant People Business Partner
- insiderthreat@healthequity.com
- Relevant internal IT SMEs
- Outside Counsel if needed
- CSO (Sunil Seshadri)

5.4 CIRT Response and Recovery Management Activities

The procedure for CIRT activation and management of incident response and recovery for processes, products, and services—as outlined in Section 2—is not intended to be easy, fast, or simple. The CIRT is designed to scale its membership and resources to match the nature and scope of the incident. This structure ensures that:

- **Technical responders** can remain focused on containment, eradication, and recovery activities.
- **Business-facing teams** can concentrate on engaging and communicating with members, clients, partners, brokers, vendors, and other stakeholders.
- **Subject Matter Experts (SMEs)** from across the organization are available to execute their respective SOPs within the CIRT framework.

Depending on the incident, this may include execution of continuity plans, disaster recovery procedures, or data backup restoration.

Each CIRT member organization is responsible for **developing its own checklists** that identify the key questions, resources, data, and actions required to fulfill their role during the incident.

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

5.5 CIRT Succession of Command

Command and Control is a critical element of the incident response lifecycle. The following outlines the succession of command during an active incident:

- Director, CDOC
- SOC Manager
- ATR Incident Commander
- Designated Incident Commander

If the CSO requires a delegate for cadence calls or other executive-level coordination during an incident, the **AVP of Cyber Defense** will serve in that capacity.

5.6 Cybersecurity Incident Containment, Eradication, and Recovery

Once CDOC has verified an incident, it is vital to contain the incident as soon as possible to limit the potential impact. This requires close coordination between the CDOC, CIRT, and the ITSM. The CIRT will define the containment, eradication, and recovery strategies considering the business impact and legal, regulatory, and cyber insurance requirements. The CDOC will plan its containment, eradication, and recovery procedures based on those strategies to help coordinate its actions and increase responsiveness during a confirmed incident.

A. Containment

Containment procedures vary based on the type and severity of the incident. In many cases, multiple strategies may be available. The CIRT should consult **Appendix H** for incident-specific guidance and also consider the following questions when determining the most effective containment approach:

- What is the potential impact on affected resources?
- How important is preserving evidence in this case?
- Is it necessary to maintain network and service availability (e.g., connectivity, customer or account-holder services)?
- How much time and effort will be required to implement the chosen strategy?
- How effective is the strategy—will it partially or fully contain the incident?
- How long will the strategy remain effective—is it a temporary or permanent measure?
- Is there an existing disaster recovery plan or business continuity plan for any services that could be affected?

Containment strategies should be coordinated through the CIRT whenever possible. However, the **CDOC may take immediate containment actions without CIRT review** when needed to prevent the continuation of an active or ongoing threat to the company.

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

B. Evidence Collection and Preservation

Evidence collection is a critical component of the incident response process and must be performed in a manner that preserves integrity, supports investigative needs, and meets legal or regulatory requirements. The decision to collect and preserve evidence must be made early in the cybersecurity incident response timeline, as it will directly influence containment and eradication strategies.

Technical Evidence Collection

- From a technical perspective, all evidence is collected through standard Cyber Defense processes to ensure accuracy, consistency, and chain of custody. This evidence is documented and stored in Torq, which serves as the official ticketing and record-keeping platform for Cyber Defense activities.
- If evidence is also required for the **ACP** process, copies will be placed in the designated ACP SharePoint folder in addition to the CDOC SOAR Solution record. This ensures that ACP stakeholders have timely access to relevant materials while CDOC SOAR Solution remains the authoritative system of record for Cyber Defense evidence.

Key Considerations for Evidence Collection

- Preservation vs. Containment/Eradication – At times, these priorities may conflict. A risk-based approach should be taken, and guidance from Legal should be sought in such situations.
- Cyber Insurance Requirements – If a Cyber Insurance claim is initiated, evidence must be collected and preserved in accordance with the policy's requirements, and forensic analysis must be performed by approved third-party analysts.
- Law Enforcement Involvement – For incidents involving fraud, malicious intent, or potential criminal activity, evidence must be collected in line with CDOC forensics procedures to ensure chain of custody.
- Privacy Law Compliance – Certain laws require the company to prove that Personal Information (PII, PHI, NPI) was not compromised. If such information is potentially involved, evidence must be collected and preserved to support later analysis.

Until directed otherwise by the CIRT, evidence should be collected for all P1 and P2 incidents.

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

C. Eradication and Recovery

After an incident has been contained, the Cyber Defense and IT Incident Management Teams should begin **eradication** and **recovery** procedures. These phases often overlap and may involve coordinated actions to return systems to a normal, secure state.

During eradication and recovery, the following actions should be considered:

- Prevent attackers from relaunching the same attack (e.g., remove malicious code, disable compromised accounts).
- Remove residual artifacts left by the incident (e.g., unnecessary or suspicious files).
- Restore systems from clean backups or verified build images.
- Strengthen security controls across the organization to prevent recurrence.

The company has established an **Impact Assessment Team** to work alongside the CIRT, CDOC, and other responding teams to determine the incident's effect on members, clients, partners, and brokers. When an incident impacts the confidentiality, integrity, or availability of data, the CDOC Liaison and other technical experts must coordinate early with the Crisis Communications Team (CCT) to align on impact details, support communication planning, and initiate appropriate incident messaging.

5.7 Crisis Communications Team Engagement and Coordination

All communications are coordinated through the CCT Lead and the Crisis Communications Team (CCT) in accordance with the company's Crisis Communications Plan. The CCT is a cross-functional group of communications professionals and supporting SMEs who rapidly design, review, and distribute key communications artifacts, talking points, and messages. These materials are used both for communicating with stakeholders and for ensuring access to the most recent and accurate information during incident response and recovery.

The communications review process is designed to expedite approval of communications, even when operating under the Attorney Client Privilege (ACP). The CCT is part of the CIRT and serves as an enterprise resource to support escalating incidents as needed. The CCT Lead—or the on-call designee—is a standing member of the CORE-CIRT.

When additional analysis or messaging is required for an investigation or other incident type, the CDOC should engage the CORE-CIRT to access the right partners for communications development, review, and dissemination. For example, the Internal Communications team—part of the CCT—can produce team member messaging through the CCT in alignment with the security and compliance requirements of the incident.

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

5.8 Trusted Partner Notifications and Regulatory Reporting

The Company has established a **CORE-CIRT** to streamline the rapid inclusion of Company liaisons to Trusted Partners in the incident assessment process. This structure enables Legal, Compliance, Privacy, Risk Management, and Communications leaders to quickly determine whether legally required notifications must be issued to customers, individuals, law enforcement, shareholders, state and federal regulators, or the media.

A risk analysis will be conducted following the procedures outlined in the Privacy Event Response Plan. If it is determined that notification to any regulatory entity is required, Legal will conduct a final review of all notification materials and determine the timing of their release. Contact information for third-party legal entities is documented in the **SO-078 Third-Party** directory.

The Legal and Privacy Teams are responsible for:

- Evaluating Securities and Exchange Commission (SEC) reporting and disclosure obligations according to materiality thresholds, including shareholder communications, stock exchange requirements, and Form 8-K disclosures.
- Evaluating notification requirements as dictated by Health and Human Services (HHS) and/ or state regulations.
- Assessing the impact of the incident on immediate or pending trade executions for members of the CIRT or individuals aware of the incident.
- Deciding whether to impose a trading blackout for CIRT members and others involved.

When required, **Payment Card Industry (PCI)** reporting will follow cardholder response procedures led by the Privacy and Legal teams. This includes compliance with the latest VISA Compromise requirements and associated reporting contacts, as outlined in: "VISA: What to do if compromised."

5.9 Post-Incident Root Cause Analysis and After-Action Report

To continue to improve our incident response, the CDOC, in partnership with the Incident Commander, Business Resilience Team and responding organizations, will participate in two process improvement activities: the Root Cause Analysis (RCA) and the After-Action Report (AAR).

A. Root Cause Analysis

Root Cause Analysis is an interactive, investigative process performed either during an active incident or immediately after incident closure. The goal is to determine **not only what happened and how it happened, but why it happened**, so that effective corrective measures can be implemented to prevent recurrence.

For cyber incidents, RCA is led by the **CDOC** and documented in the **Final Incident Report**. This report, along with supporting RCA materials, is stored in Loop as the official record.

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

Process Overview:

1. **Conduct RCA** – Performed by CDOC in collaboration with relevant SMEs; may begin while the incident is still active if conditions allow.
2. **Document Findings** – All findings are recorded in the CDOC Final Incident Report in Loop, including recommendations and a priority ranking for remediation.
3. **GRC Ingestion** – Any findings that cannot be resolved during the incident are entered into the Governance, Risk, and Compliance (GRC) lifecycle for further tracking, analysis, and mitigation.
4. **Escalation** – Each escalated finding is assigned a ticket for remediation tracking.
5. **Leadership Communication** – RCA outcomes and action items are communicated to senior leadership to ensure awareness, risk acknowledgement, and alignment on next steps.

B. Lessons Learned and the After-Action Report

The **Business Resilience Team** will organize a "lessons learned" meeting after a major cybersecurity incident, and for minor incidents when requested. This meeting is designed to improve security measures and enhance the incident-handling process. It should be held several days after the incident concludes and after at least a draft Root Cause Analysis (RCA) has been generated.

To capture key takeaways and reduce the risk of recurrence, the CDOC, in coordination with the Business Resilience Team, will generate the After-Action Review (AAR). The CIRT members and CDOC must maintain detailed, factual records of all actions taken during the incident. Each CIRT member involved in the incident must document their actions—especially when operating under ACP.

Questions to address during the AAR meeting include:

- What did the responding teams and management do well during the incident?
- Were documented procedures followed, and were they adequate?
- What information could have been provided sooner to improve or expedite remediation?
- Were there any steps or actions that slowed recovery?
- What corrective actions could prevent similar incidents in the future?
- What could be done differently next time a similar incident occurs?
- What additional tools, personnel, or resources are needed to detect, analyze, and mitigate future incidents?

Follow-up Actions: All lessons learned requiring formal follow-up will be logged and tracked in the Enterprise Risk Management system of record for risk events. Each follow-up entry will include a completion date, a management owner, and an executive owner.

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

Audit Oversight: Internal Audit Services may review the completeness and effectiveness of remediation activities on an ad hoc basis or as part of the annual audit plan.

System of Record Linkage: The system of record identifier (e.g., ticket number) for the incident must be linked to the AAR and RCA to ensure traceability between the report and associated risk management or remediation activities.

C. Evidence Gathering and Handling

In certain incidents, evidence must be collected for potential legal proceedings and preserved in compliance with applicable laws and regulations. The **Legal Department** must be consulted to determine the appropriate procedures for collecting, storing, and handling evidence to ensure it remains admissible in court.

When evidence is collected at the direction of counsel, the required **chain of custody procedures** will be communicated to incident responders. Legal has reviewed and approved **CDOC's chain of custody processes** to ensure they meet evidentiary integrity requirements. All evidence gathered through technical means will follow **standard Cyber Defense evidence collection processes** and be recorded in **CDOC SOAR Solution** as the system of record. If the evidence is also needed for an **ACP** process, a copy will be stored in the designated ACP SharePoint folder.

All personnel involved in evidence gathering or handling must follow the instructions of Legal. Questions should be directed to the Legal Department or the Incident Commander.

Note for Incident Responders: Evidence should be acquired as early as possible in the incident lifecycle, before changes are made for containment or eradication. This is critical for forensic investigations—system images, logs, and other data are most valuable when captured in their original state. Once an incident is confirmed, the responsible CIRT team member must coordinate with Legal to ensure proper handling and documentation of all forensic evidence.

6 TRAINING AND EXERCISING THE PLAN

The CIRP is tested periodically—at least once per year—to ensure team members understand their roles and responsibilities and that the plan remains accurate for the current environment.

In coordination with the Resilience Program, an annual tabletop exercise will be conducted with the Crisis Management Team, including members of the Senior Leadership Team.

7 CIRP REVIEW

The owner will review this Plan annually per the Business Resilience Policy.

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

8 APPENDICES

Appendix A – Cybersecurity Events and Incident Descriptions
Appendix B – Security Incident Preparation
Appendix C – Key Outside Resource Contact List
Appendix D – Operating Level Agreements (“OLA”)
Appendix E – Analysis and Definition of Severity Levels and Impact
Appendix F – Cyber SME Support to External Communications Activities
Appendix G – Incident Management Instructions for Operating Under Attorney-Client Privilege
Appendix H – Illustrative Incident Inquiry Questions
Appendix I – Cyber Incident Responder Roster
Appendix J – Data Loss Prevention Incident Severity Escalation

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

Appendix A
Cybersecurity Events and Incident Descriptions

Security Event	NIST 800-61 defines a security event as any observable activity on a system, network, or application. Thousands of security events occur daily and are part of normal operational activity. The following are examples of security events: • A web server receives an http request. • A user remotely logs on to the network using a VPN (Virtual Private Network) connection. • A firewall blocks a connection attempt from an unknown host. • A server restarts. • A user connects to a network share. • A user authenticates to connect to an FTP (File Transfer Protocol) server. • A user sends an e-mail. • A user's badge is denied at the entrance of a data center.
Security Alert	A security alert is a security event(s) with a potentially negative effect that requires investigation. Security alerts tell us of the possibility that a security incident has occurred, is occurring, or may occur in the future. The following are examples of security alerts: • A team member is sent a phishing email. • Malware is detected on a device. • A new domain admin account has been created. • An unusually high spike in data sent or received in any system. • A team member logs into their account from a suspicious location never used before.
Security Incidents	A security incident is generally defined as any attempted or successful unauthorized access, use, disclosure, modification, or destruction of data or interference with system operations in an information system. For example, a team member sending an unencrypted email containing personally identifiable information is a security incident.
Security Incident Categories	Most security incidents fall into one of the following six categories: • Denial of Service • Malicious Code • Unauthorized Access • Inappropriate Use/Policy Violation • Physical Security Breach • Breach of Personally Identifiable Information
Denial of Service / Distributed Denial of Service	A denial of service (DoS) is defined as an action that prevents or impairs the legitimate use of information systems by exhausting computing resources. DoS incidents often involve consuming resources such as central processing units (CPUs), memory bandwidth, or disk space. They can affect the performance and availability of networks, systems, or applications.

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

	A distributed denial of service (DDoS) is defined as a DoS that is performed by a large volume of attacking hosts, all coordinating to bring down one or more systems. DDoS has become a widespread threat to organizations because an attack leveraging a multitude of compromised machines is more difficult to prevent, track, and remediate than an attack from a single machine. DoS and DDoS attacks are dangerous because they jeopardize the availability of resources to authorized users and can hinder resources from functioning efficiently or at all. The lack of access to computing and network services can significantly disrupt a business and cause major financial loss. Some examples of DoS and DDoS attacks are: • Generating enormous amounts of traffic to exhaust all available network bandwidth • Initiating large numbers of incomplete connection requests to prevent new connections from being formed • Sending crafted TCP/IP packets to a server to crash its operating system • Overwhelming a server with requests for encrypted replies to consume all CPU (central processing unit) resources • Creating many large files on a server to consume all available disk space • Directing hundreds of externally compromised workstations to flood an organization's network with ping requests A DoS can also be caused unintentionally. For example, a sudden spike in a website's popularity can attract an unprecedented amount of traffic that exhausts all network bandwidth and causes the site to fail.
Malicious Code	Malicious code, often referred to as malware, is software that is secretly inserted into a program with the intent to infiltrate a computer system without the owner's permission or knowledge. Malware attacks attempt to compromise the confidentiality, integrity, and availability of the victim's data, applications, or operating system. Once a system is infected with malware, it can experience a wide variety of undesired effects, including data loss, decreased performance, or complete loss of functionality. Infected machines can also be used as intermediate systems in attacks against other systems. The following table describes the three main forms of malicious code. 1. Viruses. A virus is a form of malicious code that must insert itself into a host program and can only propagate when the infected program is run. Viruses are designed to replicate on their own and spread by infecting other files, programs, and computers exposed to currently infected entities. Viruses typically do damage by corrupting a system and its data or merely by playing annoying tricks on the users. Examples include: • A file infector virus that resides in memory infects every new program that is executed • A boot sector virus is executed every time a system is booted and prevents a computer from starting

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

	• A macro virus attaches itself to a word processing file template and infects every document that is created or opened 2. Worms. A worm is a complex, self-contained, self-replicating program that can spread and execute itself without any action from the user. Worms typically do damage by wasting system and network resources, but some worms damage systems by installing backdoors or performing DDoS attacks against other hosts. Examples include: • A network service worm uses the currently infected system to scan the network for vulnerabilities and infect connected machines • A mass-mailing worm searches the contact list of the currently infected host and distributes itself to all identified email addresses 3. Trojan Horses. A Trojan Horse is a non-replicating program that masks itself as legitimate but has a hidden malicious purpose. Some Trojan Horses replace existing files, while others are hosted within independent files. Trojan Horses sometimes continue to perform the function of the original program while performing additional malicious functions, while others entirely replace the original program's function. Examples include: • A program that overwrites the system hard drive and installs a backdoor disguised as a movie file • A login program is modified to collect usernames and passwords • A process listing program is tampered with to hide malicious processes Once a system is infected with malicious code, several types of attacker tools may be planted on the system to allow unauthorized access or launch additional attacks. Examples include: • Ransomware: a program designed to block access to a computer system until a sum of money is paid. • Backdoor: a program that listens or commands on a network port and allows a remote intruder some degree of control over the compromised system • Keylogger: a program that monitors and records keyboard input, which can include usernames, passwords, and financial information • Rootkit: a collection of files that is installed on a compromised system to modify the standard functionality of the system and hide the existence of malware on the system • Web browser plug-in: a plug-in that is loaded automatically when a web browser is started and monitors web activity on a compromised system • Email generating programs: a program that can be used to create and send out large quantities of email containing malware, spyware, spam, or other unwanted content without the user's knowledge
Unauthorized Access / Physical Security Breach	Unauthorized access occurs when a user gains access to a resource he/she was not intended to have. Unauthorized access is usually achieved by exploiting weaknesses in an operating system, acquiring account credentials, or tricking people into divulging confidential information (social engineering). Once unauthorized access to a resource is obtained, an attacker can view sensitive data, modify the resource, and perform other actions that an intended user could perform. Examples include: • Cracking passwords with a brute-force dictionary attack

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

	• An intruder enters the facility through a backdoor with a broken lock and commandeers a workstation that was left unattended and unlocked • A man dressed as a construction worker convinces the front desk to let him into the facility and launches an attack on company associates
Breach of Personally Identifiable Information (PII)	A breach is defined as impermissible acquisition, access, use, or disclosure that compromises the confidentiality, integrity, or privacy of PII such that the use or disclosure poses a risk of financial, reputational, or other harm to the affected party. Examples include: • Stolen or lost laptop containing unsecured protected health information • Papers containing PII found in open work areas, printers, etc. • Misdirected email listing HDHP enrollees to an external group list • Lost flash-drive containing a database of account holders • A team member accessing adjudicated claims for information on friends or family members out of curiosity/without a business-related purpose • Account record copies in response to an account holder's request lost in the mailing process and never received • Misdirected fax of account holder records to the wrong fax number
Third Party Risk Management (TPRM) Response Team Incident Scenarios	High-severity incidents P2 or higher require CORE-CIRT engagement in the following situations: • Operationally Significant Preventative Actions - Proactive measures are required to prevent infection or compromise via a third party. Example: Isolation or disconnection of systems integrated with a compromised vendor. • Third-Party Breach with Company Impact - A third-party compromise directly causes a privacy or cybersecurity incident at the Company. Example: Confirmed exfiltration of Company data, malware propagation via integrated systems, or compromise of vendor privileged access into Company environments. • Regulatory & Compliance Risk -Vendor actions or failures trigger immediate regulatory exposure or breach notification obligations. Example: Mishandling of PHI requiring HIPAA reporting within 72 hours. • Member or Public Trust Impact - The incident causes widespread member impact, brand damage, or negative media coverage. Example: Compromised vendor email system used to send phishing messages to members. • Uncooperative or Ineffective Vendor Response - Vendor fails to respond promptly, share critical details, or take timely mitigation actions. Example: Vendor ignores data requests during an active investigation. • Supply Chain Risk - An upstream provider (fourth party) breach directly affects Company systems, data, or operations. Example: SaaS vendor's hosting provider is compromised, disrupting Company services.
Fraud Response Team Incident Scenarios	• Credential Stuffing – Automated use of stolen username and password combinations from other breaches to gain unauthorized access to member or employee accounts. • API Exploit – Exploitation of vulnerabilities or misconfigurations in application programming interfaces (APIs) to access, manipulate, or exfiltrate data without authorization. • Malware on Company Infrastructure – Deployment of malicious software (e.g., ransomware, remote access trojans) on systems to disrupt operations, steal data, or enable further attacks.

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

	• Member Socially Engineered (No Company Tech Exploited) – Fraud in which members are tricked into sharing sensitive information or performing harmful actions through phishing, phone scams, or other manipulation tactics, without direct compromise of Company systems. • Generic Fraud (e.g., Card Fraud, ID Theft Unrelated to the Company) – Fraudulent activity involving stolen payment information, identity documents, or personal data obtained from sources outside of Company systems or infrastructure. • Insider Threat with Fraudulent Activity – Malicious or negligent actions by employees, contractors, or other insiders to misuse access for personal gain, commit fraud, or aid external attackers.

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

Appendix B
Security Incident Preparation

Cybersecurity Incident Response Team Tools and Resources

The table below lists common resources/tools that Detection and Response has in place.

Communications and Facilities	
Contact Information	Each CIRT team member should have emergency contact information for all other CIRT team members, including backups and executive leaders.
On-call Information	CIRT should have access to on-call information for all other relevant departments within the Company. CDOC is available 24/7 through PagerDuty for any potential security issues.
Incident Reporting Mechanisms	The infosec mailbox, SIEM, and CDOC will be the initial contact points for reporting security incidents. ServiceNow will generate tickets and store information about the incident.
War Room	The CIRT has a dedicated conference room in the SOC that can be used as a war room.
Secure Storage Facility	CIRT should identify a secure storage facility to store sensitive evidence and materials.
Conference Bridge Facilities	CIRT should have access to conference bridge facilities for internal and ongoing CIRT team meetings.
Incident Analysis Hardware and Software	
Laptops	CIRT must have easily portable workstations for analyzing data, sniffing packets, and drafting reports.
Blank Media	Flash drives and hard drives must be available as potential storage devices for sensitive information.
Packet Sniffers and Protocol Analyzers	These technologies should be available for Detection and Response to capture and analyze network traffic.
Security Event Logs	The Company leverages a Security Information and Event Management (SIEM) system to collect, protect, and analyze security event logs from critical systems. These logs are available to the CIRT to support research and analysis to identify the scope of an ongoing incident and determine the root cause of the incident. The Company's SOC MSSP is an additional resource available to the CIRT to support incident research and analysis.
Evidence Gathering Accessories	Hard-bound notebooks, digital cameras, audio recorders, chain of custody forms, evidence storage bags and tags, and evidence tape should all be available to CIRT.

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

Appendix C
Key Outside Resource Contact List

The table below includes the name and contact information of Operations Partners who collect, process, store, transmit, or otherwise have access to members, team members, and other PII.

Operations Partner Name	Business Owner / Service / Product	Contact Information
Experian Note: Experian purchased AllClearID	Business Owner: Legal Team Service: Data Breach Protection Services	Allen Burzen Senior Director, Data Breach Resolution Email: Allen.Burzen@experian.com Michael Morelli Director of Business Development Data Breach Resolution Direct: 714-227-2204 Email: Michael.morelli@experian.com
Lowenstein Sandler LLP If outside counsel engagement is required for incident response, internal counsel must initiate the engagement.	Business Owner: Legal & Privacy Teams Service: Legal Advice	Amy S. Mushahwar Partner Chair, Data, Privacy & Cybersecurity Lowenstein Sandler LLP 202-753-3825 AMushahwar@lowenstein.com
Greenberg Traurig, LLP If outside counsel engagement is required for incident response, internal counsel must initiate the engagement.	Business Owner: Legal Team Service: Outside Counsel Privacy and Security experts	Jena Valdetero (Pronounced “Gina”) 77 West Wacker Drive Suite 3100 Chicago, IL 60601 Desk:312- 456 -1025 Cell:202-431-0288 valdeteroj@gtlaw.com www.gtlaw.com
Alvarez & Marsal www.alvarezandmarsal.com (Technical)	Business Owner: Legal Team Service: Cyber Risk & Incident Response Investigations	Rocco Grillo, CISSP Managing Director Global Cyber Risk & Incident Response Investigations Alvarez & Marsal 600 Madison Avenue, 8th Floor New York, NY 10022 Mobile: +1 917 693 9700 rgrillo@alvarezandmarsal.com CyberResponse@alvarezandmarsal.com
Diversified Insurance Group	Business Owner: Matt Fleming; Felix Antwi Service: Insurance Broker	John Campos 801.325.5006 jcampos@digrisk.com

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

Unit 42	Business Owner: Incident Commander, Alvarez & Marshal Service: Support for Incident containment and recovery	unit42-investigations@paloaltonetworks.com +1.866.486.4842 (1.866.4.UNIT42) Emergency IR cen22-0767r-ir@paloaltonetworks.com Non-emergency cen22-0767r-non-urgent@paloaltonetworks.com
DHS Utah State Fusion Center	Business Owner: CDOC	
DHS Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency (CISA)	Business Owner: CDOC	801-965-3838, for SIAC (Statewide Information and Analysis Center) This is their number for a business to report a Cyber Crime.
FBI (Federal Bureau of Investigation)	Business Owner: Todd Palmer	801-579-6000
FBI (Federal Bureau of Investigation) CyberCrime Task Force	Business Owner: Melissa Householder, CDOC; Todd Palmer	801-579-1400
US Secret Service	Business Owner: Todd Palmer	801-524-5910
US Postal Inspector	Business Owner: Todd Palmer	877-876-2455
Infragard – Utah Chapter	Business Owner: Todd Palmer	https://www.fbi.gov/contact-us/field-offices/saltlakecity
US CERT		https://www.us-cert.gov/
National Cyber-Forensics and Training Alliance		https://www.ncfta.net/
Internet Crime Complaint Center		https://IC3.gov/
Financial Services Information Sharing & Analysis Center		
Health Care Information Sharing & Analysis Center		

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

Appendix D

Operating Level Agreements (OLA)

Security Incident Escalation Procedures

The following OLA timelines for acknowledging the incident following notification have been established:

Criteria	Timing
Acknowledge receipt of incident (after reviewing): P1 P2 P3 P4	30 minutes 1 hour 1 business day 5 business days
Notification to CIRT – P-1	30 minutes
Notification to CORE-CIRT – P-2	1 hour
Status Updates for P-1 and P-2	IC will set tempo for status updates based on the nature of the event, but at least daily

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

Appendix E
Analysis and Definition of Severity Levels and Impact

During the analysis, and after confirmation that a cybersecurity incident has occurred, the CIRT member must determine how many assets of each type are compromised or negatively affected and to what degree each asset is affected. With multiple asset types, the combination of asset criticality and quantity will be examined. The combination that results in the highest criticality rating while accurately describing the incident will be used. Alternatively, the ratings can be tracked separately; this adds detail to information about the incident at the cost of added complexity. Example: In a phishing attack, one must count the number of users who divulged or may have divulged their credentials.

Impact and Severity

Impact (or "breadth" or "degree of severity") can be rated as follows.

Impact	Definition
1	• Hardware: 1,000 or more devices affected. • Software: 1,000 licenses or more affected or inherent in a tool used by at least 1,000 users. • Privacy Records: 500 records impacted. • Fraud impact: 300 members or more. • Services/capabilities: Capability was destroyed; a complete rebuild is needed. • Financial: $100,000 or more in estimated cost/fraud loss exposure. • Data Protection Volume: Public disclosure of any Highly Restricted or Restricted data. • Insider: Confirmed malicious insider activity or confirmed exfiltration from critical code base (Classic, V5, Complink), sensitive production systems, etc. • Malware: A server has been compromised, or a system with sensitive data has been compromised and is successfully beaconing with high-severity malware (i.e., ransomware, keylogger, cobalt strike, etc.). • Third Party: Identified impact to the Company involving a Tier 1 or Tier 2 Partner/Vendor.
2	• Hardware: 100 to 999 devices affected. • Software: 100 to 999 licenses affected or inherent in a tool used by 100 to 999 users. • Privacy Records: 100 to 499 records impacted. • Fraud impact: 100 to 299 members. • Services/capabilities: Capability was destroyed; we will need to restore it from backup or reinstallation. • Financial: $50,000 to $99,999 in estimated cost. • Data Protection Volume: Unauthorized disclosure or confirmed access to 50+ Restricted Data files or 1+ Highly Restricted files. • Insider: Strong indicators of malicious insider activity with partial or attempted data exfiltration. • Malware: A system with sensitive data has been compromised and is attempting to beacon with high-severity malware (i.e., ransomware, keylogger, cobalt strike, etc.) • Third Party: Likely impact imminent involving a Tier 1 or Tier 2 Partner/ Vendor or Identified impact to the Company involving a Tier 3 or Tier 4 Partner/Vendor

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

3	• Hardware: 10 to 99 devices affected. • Software: 10 to 99 licenses affected or inherent in a tool used by 10 to 99 users • Privacy Records: 10 to 99 impacted. • Fraud impact: 10 to 99 members. • Services/capabilities: Capability is temporarily down; it will be restored with minimal response. • Financial: $10,000 to $49,999 in estimated cost. • Data Protection Volume: Unauthorized disclosure or confirmed access to 5-49 Restricted Data files or any Proprietary Data with business-critical impact. • Insider: Suspicious insider activity with potential for data misuse; investigation warranted. • Malware: A system has been compromised and is attempting to beacon with high-severity malware (i.e., ransomware, keylogger, cobalt strike, etc.), or a system is compromised and successfully beaconing with lower-impact malware. • Third Party: Likely impact imminent involving an impact to the Company involving a Tier 3 or Tier 4 Partner/Vendor or Identified impact to a 1 or Tier 2 Partner/Vendor without impact to the Company
4	• Hardware: 1 to 9 devices affected. • Software: 1 to 9 licenses affected or inherent in a tool used by 1 to 9 users. • Privacy Records: 1 to 9 records impacted. • Fraud impact: 1 to 9 members. • Services/capabilities: Capability mildly disrupted but continuous. • Financial: $1,000 to $9,999 in estimated cost. • Data Protection Volume: Unauthorized disclosure or confirmed access to 1-4 Restricted Data files or limited Proprietary Data without critical business impact. • Insider: Low-confidence insider concern based on unusual but explainable activity. • Malware: A system has been compromised and is attempting to beacon with lower-impact malware. • Third Party: A Tier 3 or Tier 4 partner/vendor has experienced a compromise with no confirmed impact to systems or data.
5	• Hardware: 0 devices affected. • Software: 0 licenses affected. • Privacy Records: 0 records impacted. • Fraud impact: 0 members. • Services/capabilities: There is no disruption. • Financial: $0 - $1,000 in estimated cost. • Data Protection Volume: No confirmed data disclosure; only blocked or quarantined incidents. • Insider: No insider threat indicators; activity blocked or contained by controls. • Malware: Malware is prevented by compensating controls. • Third Party: A non-Company-affiliated third party has been identified as compromised, with associated indicators of compromise (IOCs) provided for awareness and potential threat hunting.

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

Severity	Definition
P1	Catastrophic impact to Company services, reputation, and/or infrastructure. Incidents under this classification involve the potential breach of Restricted Data. This requires immediate attention, including the engagement of the Senior Leadership Team, SMEs (Subject Matter Experts), and possible outside counsel. Possible examples: Breach of an asset/system that contains restricted data, severe impact on the Company's service to partners, severe harm to the Company's brand perception, successful unauthorized access to the system hosting restricted data.
P2	Serious attempts or actual impacts on the Company's infrastructure as they pertain to service availability, data integrity, or data breach. Incidents categorized under this severity will include Company systems of moderate criticality and present vulnerabilities likely to be exploited. Persistent P-3 attacks may be categorized as P-2. Possible examples: A denial-of-service attempt, Buffer/stack overflow, multi-pronged attack, or virus infection of a critical asset. High-priority Vulnerability Exposure investigations identify a Zero-Day vulnerability that affects the Company impacting externally facing devices.
P3	A single, recorded instance of an attempt to gain unauthorized access or a single attempt to obtain unauthorized data from a single asset. A persistent and repeated P-4 incident will be rated as a P-3. Possible examples: A computer infection on a single, non-critical asset, unauthorized vulnerability scan yielding valuable results. High-priority Vulnerability Exposure investigations identify a Zero-Day vulnerability that affects the Company, regardless of whether it is internal or external.
P4	A single instance of potential or actual investigative/unfriendly conduct on Company systems. Possible examples: persistent port scan, unexpected, pegged performance on non-critical assets, and observation of potential malicious user activity.
P5	Any event where the Security Operations team has done work but is not a Security Incident. Possible examples: The People Team/ Legal seeks a non-security internal investigation. A preventative control/ policy violation has stopped a security incident.

Incident Level Matrix

The table below is intended to assist the Security team in calculating the criticality of each cybersecurity incident based on asset criticality and quantity ratings.

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

Quantity

Asset Criticality		None	Low	Medium	High	Critical
		5	4	3	2	1
Critical	1	5	4	3	2	1
High	2	10	8	6	4	2
Medium	3	15	12	9	6	3
Low	4	20	16	12	8	4

Each incident should be rated based on asset criticality and the quantity of the incident. Multiply the criticality rating of the asset by the quantity rating of the incident to obtain the overall incident criticality rating.

Each incident should be rated based on asset criticality and the quantity of the incident. Multiply the criticality rating of the asset by the quantity rating of the incident to obtain the overall incident criticality rating.

The current distribution of criticality is as follows:

16-20	P-5
12-16	P-4
6-11	P-3
3-5	P-2
1-2	P-1

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

Appendix F

Cyber SME Support to External Communications Activities

1. *Designate a Liaison to Crisis Communications Team:* Cyber Security SMEs will be in high demand during an incident to support the Company and outside counsel (if needed) in the development of specific messaging and communications materials. Designate at least one SME to support developing materials with the Communications team.

2. *Cyber Liaison Responsibilities:* During an incident, it is important that the Company communicates with our partners in a controlled manner about the updates of the incident. The Liaison ensures that accurate technical information is translated appropriately to explain actions without threatening the response or communicating privileged security details. The Liaison:
    - will coordinate with Crisis Communications Team Lead
    - will maintain and share updates on the technical response
    - is not a spokesperson for the Company but instead a collaborator with the Company's Compliance, Privacy, Legal, and communications team members.

3. *Shift Support (if needed) for Incident Duration:* The Security team will provide and rotate Cyber Liaison responsibilities to the Crisis Communications team based on the severity and duration of the incident. Communications support may last much longer than the actual incident response itself due to messaging and engagement with Clients/Members/Partners as services are recovered.

4. *Support to Contractual Client/Partner/Broker Notifications:* The Cyber Laision, or other designated Security leader will collaborate with the Company's wider Crisis Communications team to ensure contractual obligations regarding notification are met. In the weeks following the incident, the Crisis Communications Team Lead will work with the Liaison to cover scheduled times in which the select cyber CIRT team members will support client/partner engagement. The Crisis Communications Team Lead will direct the schedule and participation needs for notification briefings in coordination with Legal Department as appropriate.

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

Appendix G

Attorney-Client Privilege (ACP)

In today's dynamic risk environment, it is highly likely that the Company's incident management efforts will, at times, require the incident response team to operate under attorney-client privilege ("ACP") and at the direction of counsel. The necessity to operate under ACP should not slow the incident response work and is an additional tool to assist the Company's incident responders in protecting the Company's legal rights in the event of an investigation or legal action resulting from the incident.

This process should be applied to any incident response activity where the Legal Department has determined ACP is to be invoked. This document briefly:

- outlines the responsibilities of incident managers and incident responders operating under attorney-client privilege
- describes the attorney-client privilege and the importance of properly protecting communications and work product (i.e., analyses, strategy discussions, etc.),
- provides directions on how to label and handle email communications and documents relating to this investigation going forward, and
- reminds everyone involved that they must be vigilant about protecting the confidentiality of all aspects of this matter

Definition of Attorney-Client Privilege (ACP)

The attorney-client privilege or lawyer-client privilege is a "client's right privilege to refuse to disclose and to prevent any other person from disclosing confidential communications between the client and the attorney." Generally, the "client" is HealthEquity, Inc., who might be represented by members of the Incident Response Team (IRT), and any others brought into the incident response or project team.

ACP prohibits a court or other government tribunal from compelling the revelation of confidential communications between an attorney and a client if the subject of the communication concerns the professional relationship between the attorney and the client. For the Company, the client is the corporation, and ACP covers communication between the lawyer and a high-ranking corporate official(s) or those acting on behalf of that official. In addition to ACP, the "attorney work product" concept means that material prepared by a lawyer for litigation or in anticipation of litigation (including mental impressions or opinions) is generally immune from discovery or other compelled disclosure.

What is NOT Attorney-Client Privileged?

Communications with non-clients (partners, employers, regulators, etc.) are not privileged so be careful what you say. Likewise, internal communications shared beyond the IRT might not be privileged. Any questions about whether to share information should be directed to the lead attorney for the incident.

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

Declaring an Incident to be under ACP

ACP will be invoked when the CIRT determines that it is reasonably likely that the Company may face litigation or regulatory action due to the incident. Declaring an incident will be managed under ACP does not preclude the group from including whomever the Incident Commander, with advice of Legal Department, recommends be included in the response.

The following is an illustrative list of when ACP could be invoked:

- Personal information may have been accessed for over 5,000 individuals (which may trigger large-scale individual notification and/or regulator notification).
- The incident is assessed as a P1 or P2 on the severity matrix in the IRP.
- A client or partner threatens a breach of contract or other claim resulting from the incident.
- The CIRT believes that there is a likelihood that litigation or regulatory action may result, considering the following factors:
    a) the number of records implicated
    b) the sensitivity of the data compromised
    c) the likely unauthorized use of, or access to, the compromised data
    d) the likelihood of harm to individuals
    e) the novelty of the method used to access the data
    f) the business disruption resulting from the incident
    g) the company's culpability in failing to detect or prevent the data incident, or gaps in its information security practices
    h) the amount of press or social media attention resulting, or that may result, from the data breach
    i) whether the Company issued potentially false or misleading statements regarding its information security and cyber security risks
    j) the Company's failure to timely notify affected individuals and other stakeholders (e.g., HIPAA covered entities) under relevant federal or state laws

Once an incident is declared to be operating under ACP, the following process:

1. Incident Commander (IC) will gather Key personnel from Legal Department and IRT to present an incident summary and advise the Legal Department on the likelihood of litigation/regulatory or reportable incident.
    - If not moving under ACP, the Legal Department will participate in the IRT and re-evaluate the decision as the incident progresses.
    - If moving under ACP, the IC will ensure every IR meeting begins with an oral reading of ACP Work Product Handling Instructions. See below "Protecting the Privilege"
2. The IC will inform the Crisis Communications Team Lead to ensure all future communications materials are given additional scrutiny through the formal review process, that includes the assigned attorney.
3. The IC shall instruct the Scribe to maintain a list of incident participants for future reference by the Legal Department. Any requests for additional incident responders to join the effort shall be shared with the assigned attorney and Scribe prior to participating in any incident response work.
    - No one can be brought into an ACP investigation who is not an employee of the Company, or who is not a member of consulting firms/service providers with whom the Company

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

has a current contract, without first going through the assigned attorney for the investigation.

4. Although the incident proceeds at the direction of counsel and artifacts become Attorney Work Product, day-to-day management of the incident does not transition to Legal from the existing Incident Commander. However, the Incident Commander works closely with the incident's assigned attorney to participate in any or all IR meetings going forward.
5. The Company's Crisis Leader may also be added to the Incident Response to support the IC if requested or should the ACP investigation be assessed as possibility of escalating to a P1.
6. The Legal Department will set up an ACP SharePoint site and folder structure for data management of the incident. The Legal Department will provide access to this SharePoint site to all ACP Incident Responders.
    - Rather than sending sensitive documents as email attachments, place the documents in the project SharePoint folders and alert project team members via email that the materials are available.
    - Keep attachments to a minimum, especially if the attachment contains sensitive information.
7. The Incident Commander will ensure a MSTeams site is built to ensure all ACP chats are managed within a specific chat environment.
8. The Legal Department is responsible for advising the IC of any changes to ACP handling instructions during the incident.
9. Questions or concerns about these instructions or operating under ACP can be directed to the lead attorney for the ACP incident, or the General Counsel.

Special Note: Though rare, there are times when elements of an investigation, or incident, will be managed under ACP guidelines, while the rest of the incident response will not be. The assigned attorney will provide counsel and direction should this hybrid approach be necessary. If the incident response team has any questions during the execution of their duties, they can always ask for guidance from the Legal Department.

Attorney Work Product

The "Attorney Work Product" is a rule that an opposing party generally may not discover or compel disclosure of written or oral materials prepared by or for an attorney during legal representation, especially in preparation for litigation. It is not meant to imply that the lawyers are doing all the work or to minimize anyone's efforts. ACP and the work product concept can be quite complex, and so it is important to follow the instructions provided by the Legal Team during an incident, including those documented here.

Protecting the Privilege – Instructions for Marking Written Documents and Communications

Please note that the instructions below are not intended to slow down any work or be burdensome. Rather, they primarily require proper labeling of written internal communications/documentation. It is critically important to discuss strategies and technical findings in a way that protects those discussions from potential disclosure in the event of litigation or other regulatory/legal scrutiny. This is primarily to protect the Company's legal rights, but also will protect anyone who is called to testify on this matter in the future.

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

Keep all communications about the incident (including technical findings, etc.) confidential and limited to those who are "under the ACP tent" and have a need to know. Any communications or disclosures to external parties, or even internal parties who have no need to know, can destroy the ACP status of that communication. Contact the Incident Commander or lead attorney with questions.

Therefore, please comply with the following instructions:

(1) **The subject field** of all communications (emails, chats, messaging, memos, meeting notices, etc.) regarding this investigation must be labeled as shown below:

ACP [insert project code name] – [add subject]
Example: ACP Swordfish – Task list update

(2) **The first line in the body of communications** should contain the phrase listed below. Please copy (cc) the lead attorney for the investigation on **all** such communications.

Privileged and Confidential | Attorney Work Product

(3) **All documents and reports produced** as part of this investigation should be marked as shown below.

Privileged and Confidential | Attorney Work Product | Prepared at the Direction of Counsel

These documents should be handled as highly confidential. That means they should be shared only on a “need to know basis” and should not be left open in workstations, or otherwise sent to systems external to the Company except to those firms and consultants with whom we have contracts in place for this matter.

(4) Information should be provided to internal employees and service provider technical support personnel only on a limited “need to know” basis to perform technical or administrative tasks, and they should be advised of these instructions.

(5) Communications with law enforcement, account holders, employers, health plans, or the public at large, are not privileged, and thus are discoverable in the event of later litigation activity. Accordingly, do not have any communications regarding the investigation without discussing with the assigned attorney first.

(6) Written communications between forensics/technical personnel should be labelled as described above so that they are protected as “attorney work product” performed “at the direction of counsel.” Any reporting of factual findings or strategic concerns or general security-related issues via email should be copied to the assigned attorney for the investigation.

(7) At the conclusion of an ACP incident, the assigned attorney will send instructions for the proper removal of incident related communications and materials from project team systems. The SharePoint will be the official repository for documentation.

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

Appendix H

Illustrative Incident Inquiry Questions

- What happened?
- Where and when did it happen?
- Who or what was affected?
- Who is involved?
- Who internally has been informed? What were they told?
- Was sensitive information misused or compromised?
- Has the vulnerability been closed?
- Do we know who was responsible for the incident?
- Who are the contacts to obtain additional information?
- What data is a risk / compromised / leaked?
- What is the extent of the data incident?
- How many records were or could be affected?
- What is in the records?
- What type of data is included?
- Do we need to inform members or clients at this time?
- When did we learn about the incident?
- What is the likely impact / known impact?
- Is there additional risk or exposure to the Company or members or clients?
- What is being done now to protect client and member data?
- What security systems were in place to protect this information?
- Were those systems functioning properly?
- Is this known yet outside of the Company?
- Have authorities been notified? If so, who was notified and what were they told?
- Has the compromise been contained? When was it contained?
- Could this have been prevented? Were there any warning signs or indicators?
- What steps are being taken now to avoid similar situations in the future?

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

Approval Certificate

Docusign Envelope ID: 79562561-FB30-41E8-8D65-984FD395B963

Cybersecurity Incident Response Plan

APPROVER

Title	Name	Signature	Date
CSO	Sunil Seshadri	Signed by:	09/29/2025

REVIEWERS

Title	Name	Signature	Date
CIO	Abhi Gite	Signed by: Abhi Gite	09/26/2025
SVP, Fraud & Product Security	Ajit Gaddam	Signed by: Ajit Gaddam	09/25/2025
VP, Head of Product Security	Neil Bahadur	Signed by:	09/25/2025
AVP, Cyber Defense & Eng	Spencer McGalliard	Signed by: Spencer McGalliard	09/19/2025
Dir, Business Resilience	Bridger McGaw	Signed by: Bridger McGaw	09/16/2025
Dir, Fraud Analytics and Ops	Kristi Gardner	Signed by: kristi Gardner	09/18/2025
Dir, Cyber Defense Operations	Melissa Householder	DocuSigned by: Melissa Householder	09/18/2025
Dir, Privacy	Justin Pingel	Signed by: Justin Pingel	09/18/2025
Dir, Security GRC	Kaushik Kiran	Signed by: kaushik kiran	09/18/2025
Sr Mgr, People Security	Todd Palmer	Signed by: Todd Palmer	09/18/2025
Mgr, Cyber Defense Operations	Jared Miller	DocuSigned by: Jared Miller	09/22/2025
AGC, Regulatory and Governance	Thor Larson	DocuSigned by: Thor Larson	09/19/2025

© 2025 HealthEquity, Inc. Proprietary and confidential.

APPROVED (as to form) DS TL DS FS