HEALTHeLINK™

Privacy and Security Policies and Procedures

Security Officer:	Chris Klimek
Privacy Officer:	Patti Burandt

Table of Contents

Privacy and Security Policies and Procedures

Privacy Policies and Procedures

Security Policies

HEALTHeLINK™

Privacy Policies and Procedures

Preamble

Privacy Policy and Procedure
Policy No. P00

1 Introduction

This document, in conjunction with the Privacy and Security Guidance for Qualified Entities and their Participants, provides information related to privacy and security for qualified entities participating in New York's Statewide Health Information Network, consistent with 10 N.Y.C.R.R. § 300.3(b)(1). This guidance ensures secure health information exchange through the Statewide Health Information Network for New York (SHIN-NY) that will improve health care delivery and health outcomes for all New Yorkers. The New York State Department of Health (NYS DOH), along with key stakeholders, participated in the development of this guidance, which is compliant with all applicable state and federal laws.

2 Scope

HEALTHeLINK Privacy Policies and Procedures are meant to communicate specific requirements for Participants.

3 Reference

Please refer to the current Statewide Health Information Network for New York (SHIN-NY) Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and other applicable laws.

Authorized User Access

Privacy Policy and Procedure
Policy No. P03

1 Policy Statement

Participants must comply with applicable law and HEALTHeLINK Policies and Procedures and promulgate the internal policies required for such compliance in order to provide essential privacy protections for patients. Authorized Users will be permitted access to patient Protected Health Information only for purposes consistent with a patient's Affirmative Consent or an exception.

2 Scope

This policy applies to all Participants that have registered with and are participating in HEALTHeLINK that may provide, make available or access health information through HEALTHeLINK. This policy also applies to all HEALTHeLINK personnel who access health information through HEALTHeLINK.

3 Procedure

3.1 Requirements for Participant's Authorized Users

At the time that a Participant identifies an Authorized User to HEALTHeLINK, the Participant must confirm to HEALTHeLINK, if requested, that the Authorized User:

A. Has completed training provided or approved by HEALTHeLINK;

B. Will be permitted to use HEALTHeLINK's Health Information Exchange (HIE) only as reasonably necessary for the performance of the Participant's activities as the participant type, as indicated on the Participant's Registration Application;

C. Has had his or her identity verified by the Participant;

D. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized User;

E. Has acknowledged that his or her failure to comply with HEALTHeLINK Policies and Procedures may result in the withdrawal of privileges to use the HIE and may constitute cause for disciplinary action by the Participant; and

F. Has complied with other requirements described in HEALTHeLINK Policies and Procedures and SHIN-NY Policy Guidance.

3.2 Requirements for HEALTHeLINK's Personnel

HEALTHeLINK will require that each person utilizing the HIE on behalf of HEALTHeLINK:

A. Has completed a training program provided or approved by HEALTHeLINK;

B. Has had his or her identity verified by HEALTHeLINK;

C. Will be permitted to use the HIE only as reasonably necessary for the performance of HEALTHeLINK's activities;

D. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized Users;

E. Has acknowledged that his or her failure to comply with HEALTHeLINK Policies and Procedures may result in the withdrawal of privileges to use the HIE and may constitute cause for disciplinary action by HEALTHeLINK;

F. Has complied with other requirements described in HEALTHeLINK Policies and Procedures and SHIN-NY Policy Guidance.

3.3 Community-Based Organizations Not Subject to HIPAA

A. HEALTHeLINK and Participant shall undertake reasonable efforts to limit the Protected Health Information Accessed by or Transmitted to a Community-Based Organization that is not a Covered Entity to the minimum amount necessary to accomplish the intended purpose of the Access or Transmittal, taking into account the nature of the Community-Based Organization Accessing the Protected Health Information or receiving the Transmittal, the reason(s) such organization has requested the Protected Health Information, and other relevant factors.

4 References

- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1).*

Patient Consent

Privacy Policy and Procedure
Policy No. P04

HEALTHeLINK™

1 Policy Statement

New York State law requires that hospitals, physicians and other health care providers, and payers obtain patient consent before disclosing Protected Health Information for non-emergency treatment. Therefore, affirmative consent must be obtained from the patient before Participants Access a patient's Protected Health Information.

2 Scope

This policy applies to all Participants that have registered with and are participating in HEALTHeLINK that may Transmit, make available or Access health information through HEALTHeLINK.

3 Procedure

3.1 Special Provisions Relating to Minors

A. On the minor individual's 18th birthday, when the minor becomes an adult, Participant access to the Protected Health Information will no longer be available until the individual executes his/her own Affirmative Consent.

B. A one-time Access may be granted to a Practitioner, or Authorized User under the supervision of a Practitioner, by a minor under the age of 18 who is receiving Minor Consented Services from that Practitioner and where the minor's Personal Representative has not previously provided consent or the minor's Personal Representative has denied Affirmative Consent, to allow Access by the Practitioner or Authorized User to the minor's clinical information. The minor's consent for such one-time Access will be on a NYS DOH approved minor consent form. This ability for one-time Access will be limited to those Practitioners or Authorized Users likely to deliver Minor Consented Services and who have received special training in the use of this one-time Access capability. HEALTHeLINK will perform an audit of all one-time Accesses.

3.2 Other Policies and Procedures Related to Consent

3.2.1 Consent Process

Unless an exception applies, a Participant will be unable to Access a patient's Protected Health Information through HEALTHeLINK until the individual patient has been given an opportunity to consent to the Access, in writing.

A. The Participant must document the patient's consent on the HEALTHeLINK Consent form and indicate the patient's consent in the HEALTHeLINK software.

B. The Participant will:

1. Forward a copy of the Consent to HEALTHeLINK within 3 business days of obtaining the Consent form; OR

2. Retain all patient consent forms and be able to produce the forms upon HEALTHeLINK request.

3.2.2 Consents Covering Multiple Participants

HEALTHeLINK's Affirmative Consent applies to more than one Participant.

3.2.3 Denial of Consent

Patients may deny consent to the Access or receipt of their health information by Participant(s) through HEALTHeLINK.

A. Patient denial of consent must be in writing on a HEALTHeLINK Consent form with one of the denial of consent options checked:
   1. "No, Except in an Emergency"; or
   2. "No, Even in an Emergency".

B. Providers/Payers must not condition treatment/coverage on the patient's willingness to consent to the Access of their Protected Health Information through HEALTHeLINK.

3.3 Patient Consent Transition Rules

3.3.1 Use of Approved Consents

HEALTHeLINK shall be required to utilize an Approved Consent with respect to all patients who consent to the exchange of Protected Health Information via the SHIN-NY on or after the Consent Implementation Date.

3.3.2 Reliance on Existing Consents Executed Prior to the Consent Implementation Date

If HEALTHeLINK obtains a patient consent utilizing a patient consent substantially similar to a Level 1 Consent prior to the Consent Implementation Date (an "Existing Consent Form") HEALTHeLINK may continue to rely on such patient consent as long as such Existing Consent (i) complies with all applicable state and federal laws and regulations and (ii) if such Existing Consent is relied upon for the release of HIV-related information, such Existing Consent has been approved by NYS DOH.

3.3.3 Use of Existing Consent After Consent Implementation Date

HEALTHeLINK may continue to use an Existing Consent after the Consent Implementation Date if the Existing Consent is approved by NYS DOH.

4 References

- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1).*

Patient Request for Restrictions or Confidential Communications

Privacy Policy and Procedure
Policy No. P05

1 Policy Statement

Participants shall comply with applicable federal, state and local laws as well as HIPAA regulations regarding an individual's right to request for restrictions or confidential communications.

2 Scope

This policy applies to all Participants that have registered with and are participating in HEALTHeLINK that may Transmit, make available or Access health information through HEALTHeLINK.

3 Procedure

A. All requests for restrictions or requests for confidential communications must go through the Participants, not through HEALTHeLINK.

B. Any patient that directly contacts HEALTHeLINK with a request for Restrictions or Confidential Communication will receive from HEALTHeLINK, within 3 business days, directions on how to make such request of the applicable Participant including the contact information of the Privacy Officer of the Participant.

C. If a Participant agrees to an individual's request for restrictions or confidential communications, the Participant will ensure that it complies with the restrictions or confidential communications when releasing information obtained through HEALTHeLINK.

4 References

- 45 C.F.R. § 164.522.

Breach Response

Privacy Policy and Procedure
Policy No. P06

1 Policy Statement

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) establishes provisions for protecting the privacy and security of patient Protected Health Information. HIPAA regulations require Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information. As a Business Associate of the Covered Entities participating in HEALTHeLINK, it is the policy of HEALTHeLINK to comply with those requirements in accordance with the procedures set forth herein. As a business conducting business in New York State, HEALTHeLINK will also comply with the New York State Information Security Breach and Notification Act.

2 Scope

HEALTHeLINK and its Participants including but not limited to those who Access the HEALTHeLINK System and/or Transmit Protected Health Information contained therein, as well as those who maintain the HEALTHeLINK hardware and software.

3 Procedure

HEALTHeLINK will use appropriate administrative, technical, and physical safeguards to prevent a breach of unsecured Protected Health Information.

3.1 Reporting Requirements

A. HEALTHeLINK personnel and Participants, who discover, believe, or suspect that unsecured Protected Health Information has been Accessed, Used, Transmitted or Disclosed in a way that may violate the HIPAA Privacy or Security Rules, must immediately report such information to the HEALTHeLINK Privacy Officer/designee.

B. The HEALTHeLINK Privacy Officer/designee will report the breach or suspected breach to the effected Data Supplier(s), verbally, within 24 hours of HEALTHeLINK becoming aware of such breach followed by written notice within 72 hours of verbal notification.

1. HEALTHeLINK will include in the report, or provide to the Data Supplier(s) as promptly thereafter as the information becomes available, the following:
    i. Identification of each individual whose unsecured Protected Health Information has been, or is reasonably believed to have been, Accessed, Transmitted, acquired, or Disclosed;

    ii. A brief description of what happened, including the date of the breach and the date of the discovery of the breach.
2. HEALTHeLINK will not contact any individuals suspected to be affected by the breach without prior written approval of the effected Data Supplier(s).

C. HEALTHeLINK and/or Participant where breach occurred will:

1. Investigate the scope and magnitude of the breach;
2. Identify the root cause of the breach;
3. Mitigate, to the extent possible, damages caused by the breach;
4. If applicable, request the party who received such information to return and/or destroy the impermissibly disclosed information;
5. Apply sanctions to their respective staff members involved in the breach, as appropriate in accordance with their respective Privacy and Security policies and procedures and HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*

D. If the breach includes Protected Health Information contained in the nationwide health information network ("eHealth Exchange"), HEALTHeLINK will comply with the breach notification requirements of eHealth Exchange participants contained in the Data Use and Reciprocal Support Agreement ("DURSA") signed by HEALTHeLINK.

E. If the breach may impact the Statewide Health Information Network of New York (SHIN-NY) or other Qualified Entities, HEALTHeLINK will comply with the Security Incident and Breach Response Communication Framework of the SHIN-NY.

F. If applicable, HEALTHeLINK will report security breaches as required by the New York State Information Security Breach and Notification Act.

G. HEALTHeLINK will notify the HEALTHeLINK Operating Committee and the HEALTHeLINK Board of Directors of the breach.

4 References

- 45 C.F.R. Subpart D.
- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*
- HEALTHeLINK: *Terms and Conditions for Health Information Exchange Participation Agreement*.
- N.Y. State Information Security Breach and Notification Act (NY General Business Law § 899-aa).
- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1)*.
- Data Use and Reciprocal Support Agreement (DURSA), Current Version.

Privacy Complaints/Concerns

Privacy Policy and Procedure
Policy No. P07

HEALTHeLINK™

1 Policy Statement

Each Participant must have a mechanism for reporting, and encourage all workforce members, agents, and contractors to report any non-compliance with these policies to the Participant. Each Participant must also establish a process for individuals whose health information is included in HEALTHeLINK to report any non-compliance with these policies or concerns about improper Disclosures of information about them.

2 Scope

This policy applies to all Participants that have registered with and are participating in HEALTHeLINK that may Transmit, make available or Access health information through HEALTHeLINK.

3 Procedure

A. Any complaints/concerns about the confidentiality of patient information maintained by HEALTHeLINK must be reported to the affected entity's HIPAA Privacy Officer for investigation and follow-up.

B. The HEALTHeLINK Privacy Officer must be notified of any complaints/concerns related to HEALTHeLINK Policies and Procedures.

C. The HEALTHeLINK Privacy Officer/designee will coordinate the investigation of the complaint/concern with the affected entity, facilitate HEALTHeLINK's investigation and initiate steps by HEALTHeLINK, as necessary, to mitigate any privacy or security risks.

D. On completion of the investigation, a summary of the complaint/concern and action taken will be sent to the HEALTHeLINK President & CEO.

E. The HEALTHeLINK President & CEO/designee must archive the summaries of the complaints/reports for later reporting and discussion.

F. Any intimidation of a retaliation against an individual who reports a privacy compliant/concern may result in the imposition of sanctions by HEALTHeLINK (see HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures*).

4 References

- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*
- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1).*

Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures

Privacy Policy and Procedure
Policy No. P09

1 Policy Statement

HEALTHeLINK and each Participant shall implement system procedures to discipline and hold Authorized Users, workforce members, agents and contractors accountable for ensuring that they do not Use, Transmit, Disclose or Access Protected Health Information except as permitted by the HEALTHeLINK Privacy and Security Policies and Procedures and that they comply with these policies.

2 Scope

This policy applies to HEALTHeLINK and all Participants that have registered with and are participating in HEALTHeLINK that may Transmit, make available or Access health information through HEALTHeLINK.

3 Procedures

A. Any breach of patient Protected Health Information reported by HEALTHeLINK to a Participant (see HEALTHeLINK Policy P06, *Breach Response* and HEALTHeLINK Policy P07, *Privacy Complaints/Concerns*) will be handled according to the Participant's HIPAA Privacy and Security Policies.

B. Any breach reported to HEALTHeLINK by a Participant (see HEALTHeLINK Policy P06, *Breach Response* and HEALTHeLINK Policy P07, *Privacy Complaints/Concerns*) will be handled according to HEALTHeLINK's Privacy and Security Policies and Procedures.

C. HEALTHeLINK will impose sanctions on HEALTHeLINK personnel who are determined to have failed to adhere to HEALTHeLINK Privacy and Security Policies and Procedures.

D. Participants are solely responsible for all acts and omissions of the Authorized Users of their workforce. HEALTHeLINK will impose sanctions on a Participant whose Authorized Users fail to adhere to HEALTHeLINK Privacy and Security Policies and Procedures.

E. When determining the type of sanction to apply, HEALTHeLINK and/or the Participants will take into account the following factors:
   1. whether the violation was a first time or repeat offense;
   2. the level of culpability of the Participant or Authorized User, e.g., whether the violation was made intentionally, recklessly or negligently;
   3. whether the violation may constitute a crime under state or federal law; and

4. whether there is a reasonable expectation that the violation did or may result in harm to a patient or other person.

4 References

- HEALTHeLINK Policy P06, *Breach Response*.
- HEALTHeLINK Policy P07, *Privacy Complaints/Concerns*.
- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1)*.

Workforce Training for HEALTHeLINK Privacy and Security Policies and Procedures

Privacy Policy and Procedure
Policy No. P10

1 Policy Statement

HEALTHeLINK's Privacy and Security Policies and Procedures provide information regarding the secure Access of Protected Health Information through the health information exchange. Authorized Users must understand the policies and procedures and their responsibilities within such policies and procedures.

2 Scope

This policy applies to all HEALTHeLINK workforce members and all Participant workforce members that have registered with and are participating in HEALTHeLINK that may Transmit, make available or Access health information through HEALTHeLINK.

3 Procedure

A. To support HEALTHeLINK's commitment to information privacy and security, both new and existing members of the workforce of HEALTHeLINK and each Participant will be trained on all HEALTHeLINK Privacy and Security Policies and Procedures, including but not limited to those related to Authorized User Access, Transmission, and/or Disclosure of information, as well as patient consent. Training will be provided in one or more of the following methods:
   1. HEALTHeLINK staff will conduct training for each Authorized User;
   2. HEALTHeLINK staff will train a Participant trainer who will then conduct training of their workforce;
   3. HEALTHeLINK will publish a policies and procedures training video that may be viewed by any Authorized User.

B. Each Authorized User will sign a certificate that he/she has received training and will comply with all HEALTHeLINK Policies and Procedures prior to gaining access to HEALTHeLINK. Such certification may be made on a paper form or electronically and will be retained by HEALTHeLINK or the Participant for at least 6 years.

4 References

- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1)*.

Workforce Access to and Termination from HEALTHeLINK

Privacy Policy and Procedure
Policy No. P11

1 Policy Statement

In accordance with the requirements of HIPAA with respect to privacy principles of use limitation, security safeguards and controls, accountability and oversight, data integrity and quality, and remedies, Participants must make reasonable efforts to limit or determine Access as needed and use of Protected Health Information available through the HEALTHeLINK System.

In doing so, the HIPAA requirements for workforce training, sanctions for privacy and security violations, and the reporting of violations, will be followed in order to ensure the legitimate use of health data, the proper implementation of Participants' privacy and security practices, and the prompt identification of and undertaking of remedial action for privacy and security violations.

2 Scope

This policy applies to all institutions/groups or individuals that have registered with and are participating in HEALTHeLINK and that may Transmit, make available or Access health information through the HEALTHeLINK System.

3 Procedure

3.1 Access Provision

Access to the HEALTHeLINK System will only be provided to Participants' workforce members, agents, and/or contractors that have been identified, in writing to HEALTHeLINK, by the Participants as "Authorized Users". HEALTHeLINK will establish and provide a unique identifier to each Authorized User.

3.2 Access Control

A. Each Participant is responsible for monitoring and allowing Access to HEALTHeLINK System only by those workforce members, agents, and contactors who have a legitimate and appropriate need to Access the HEALTHeLINK System and/or release or obtain Protected Health Information through the HEALTHeLINK System.

B. Each Participant is responsible to oversee the activities of its Authorized User.

C. Any violation, by an Authorized User or any other individual who Accesses the HEALTHeLINK System either through the Participant or the Participant's Authorized Users, will be cause for sanctions (see HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures*).

4 References

- HEALTHeLINK Policy P09, *Sanction for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*
- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1).*

Release of Data for Research

Privacy Policy and Procedure
Policy No. P13

HEALTHeLINK™

1 Policy Statement

HEALTHeLINK may Disclose data to third party researchers for scholarly research purposes. The data subject to Disclosure will be limited to that which is available through HEALTHeLINK from Data Suppliers that have signed the HEALTHeLINK Participation Agreement and data made available to HEALTHeLINK from other sources subject to any contractual limitations placed on HEALTHeLINK by those sources.

The Disclosure of data will be compliant with all state and federal laws, shall not harm the reputation of HEALTHeLINK or any of its Participants, and shall not limit HEALTHeLINK's ability to perform its mission.

2 Scope

This policy applies to all HEALTHeLINK Participants and any researchers requesting data for Research.

3 Procedure

A. All requests for Access to data for Research purposes must be submitted to the HEALTHeLINK President & CEO on the HEALTHeLINK Data Use Request Application (DURA). Data may not be Accessed through HEALTHeLINK until the DURA is approved by HEALTHeLINK.

   1. An Institutional Review Board (IRB) approval letter or exempt letter must accompany the DURA. The IRB may be local or non-local but must be located in the United States.
   2. Researchers must notify HEALTHeLINK of any planned changes in the conduct of the Research from what was described in the approved DURA.
      i. Changed or modified DURAs will be reviewed by HEALTHeLINK for continued approval.
      ii. Failure to provide prior notification to HEALTHeLINK of a change may subject the Researcher to sanctions as described in HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures*, or as described in the Data Use Agreement (DUA).

B. If the proposed Research requires De-Identified Data or a Limited Data Set and it is deemed exempt by an IRB, the individual seeking to perform the Research must obtain approval for the Research from the HEALTHeLINK Research Committee.

   1. HEALTHeLINK will review each DURA and approve for submission to the Research Committee those complete DURAs with an overall favorable balance between risk, value, and operational impact. Essential criteria for assessing each DURA include, but it not limited to, the following:

i. Legal/Ethical – The DURA is compliant with state and federal laws and regulations and with HEALTHeLINK Policies and Procedures, contractual requirements, and ethics;
ii. HEALTHeLINK Mission impact – The DURA is not inconsistent with the HEALTHeLINK mission;
iii. HEALTHeLINK and Participant community reputation – Knowledge of the DURA in the wider community, including patients, medical professionals, regulators, business leaders, and political leaders, would not be perceived as harmful to HEALTHeLINK or its Participants' reputation in the community;
iv. Scientific merit – The DURA objectives and approach are scientifically sound and relevant to advancing the quality or reducing the cost of healthcare and/or the health of the population;
v. Availability of the data – The data requested by the DURA is available via HEALTHeLINK or can reasonably be made available via HEALTHeLINK;
vi. Operational impact – There is minimal impact on HEALTHeLINK operations and core mission by responding to the DURA;
vii. Cost – The cost to HEALTHeLINK to respond to the DURA.

2. DURAs that are not approved by the Research Committee will be returned to the applicant with a brief explanation of the reason(s) that the DURA was not approved. The applicant may submit a revised DURA.
3. All DURAs that are approved by the Research Committee require a fully executed DUA with the requesting researcher prior to the release of any data for Research. The DUA is the contractual agreement between HEALTHeLINK and the researcher describing the terms and conditions for the release of data to the researcher.
4. A HEALTHeLINK Participant may not opt-out of having its Protected Health Information de-identified or converted to a Limited Data Set and Used for Research approved by the Research Committee and that is compliant with this policy.

C. HEALTHeLINK may establish a fee for the provision of the data for Research. Such fees will compensate HEALTHeLINK for costs and efforts required to provide the data service and reflect potential commercialization opportunities, if any. The Research Committee may waive or adjust the fee, at its discretion, for requests with community level value.

D. HEALTHeLINK will establish sufficient controls to assure that:
1. Patient Data is protected in compliance with HEALTHeLINK Policies and Procedures and applicable state and federal laws, rules, and regulations; and
2. The data that is Disclosed is utilized in accordance with the DUA.

4 References

- 45 C.F.R. § 164.514(a) and (b).
- 45 C.F.R. § 164.512(i).
- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*
- NYS DOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participant in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1)*.

HEALTHeLINK™ Security Policies

Governance

Information Security Policy
Policy No. SP-001

1 Introduction

The purpose of this policy is to ensure that HEALTHeLINK's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Organizational Context

3.1.1 Aligning Cybersecurity With Organizational Mission

3.1.1.1 Senior Management must understand the organizational mission.

3.1.1.2 Senior Management must let the organizational mission inform cybersecurity risk management.

3.1.1.3 The Chief Executive Officer must share the organization's mission through vision and mission statements.

3.1.1.4 Senior Management must share the organization's mission through marketing.

3.1.1.5 Senior Management must share the organization's mission through service strategies.

3.1.1.6 The Security Officer must identify risks that may impede the mission based on the shared mission.

3.1.2 Stakeholder Needs Guide Cybersecurity Efforts

3.1.2.1 The Security Officer must understand internal and external stakeholders.

3.1.2.2 The Security Officer must consider the needs and expectations of these stakeholders regarding cybersecurity risk management.

3.1.2.3 The HR Director must, annually, identify relevant internal stakeholders.

3.1.2.4 The Security Officer must understand the cybersecurity-related expectations of these internal stakeholders.

3.1.2.5 Senior Management must, annually, identify relevant external stakeholders.

3.1.2.6 The Security Officer must understand the cybersecurity-related expectations of these external stakeholders.

3.1.3 Compliance With Cybersecurity Legal Obligations

3.1.3.1 The Security Officer must understand legal, regulatory, and contractual requirements regarding cybersecurity.

3.1.3.2 The Privacy Officer must manage privacy and civil liberties obligations.

3.1.3.3 The Security Officer must determine a process to track and manage legal and regulatory requirements protecting individuals' information.

3.1.3.4 The Security Officer must determine a process to track and manage contractual cybersecurity management requirements for supplier, customer, and partner information.

3.1.3.5 The Security Officer must align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements.

3.1.4 Compliance With SHIN-NY Policies and Procedures

3.1.4.1 The Security Officer must ensure that HEALTHeLINK establishes and implements policies and procedures to comply with the privacy and security guidance for Qualified Entities and their Participants (Privacy and Security Policies and Procedures for Qualified Entities and their Participants in New York State under 10 N.Y.C.R.R. § 300.3(b)(1), version 4.0, revised January 2023)

3.1.5 Communicating Critical Stakeholder Expectations

3.1.5.1 The Chief Executive Officer must understand critical objectives, capabilities, and services that stakeholders depend on or expect.

3.1.5.2 The Chief Executive Officer must communicate these critical objectives, capabilities, and services.

3.1.5.3 The Chief Executive Officer must establish criteria for determining the criticality of capabilities and services as viewed by stakeholders.

3.1.5.4 The Security Officer must, annually, determine assets and business operations vital to achieving mission objectives.

3.1.5.5 The Security Officer must, as-needed, assess the potential impact of a loss (or partial loss) of these operations.

3.1.5.6 The Security Officer must establish resilience objectives for delivering critical capabilities and services.

3.1.5.7 The Security Officer must communicate these resilience objectives in various operating states.

3.1.6 Clarifying Key Organizational Dependencies

3.1.6.1 The Chief Executive Officer must understand and communicate outcomes, capabilities, and services that the organization depends on.

3.1.6.2 The VP, Technology must, annually, create an inventory of the organization's dependencies on external resources.

3.1.6.3 The VP, Technology must, annually, document how these dependencies relate to organizational assets and business functions.

3.1.6.4 The Security Officer must, annually, identify and document external dependencies that are potential points of failure.

3.1.6.5 The Security Officer must, annually, share information on potential points of failure with appropriate personnel.

3.2 Risk Management Strategy

3.2.1 Setting Agreed-Upon Risk Management Goals

3.2.1.1 The Security Officer must, annually, establish risk management objectives.

3.2.1.2 Senior Management must, annually, agree on these objectives with organizational stakeholders.

3.2.1.3 The Security Officer must, annually, update near-term and long-term cybersecurity risk management objectives.

3.2.1.4 The Security Officer must, as-needed, update objectives when major changes occur.

3.2.1.5 The Security Officer must, annually, establish measurable objectives for cybersecurity risk management.

3.2.1.6 The Chief Executive Officer must, annually, ensure senior leaders agree about cybersecurity objectives.

3.2.1.7 The Security Officer must use agreed cybersecurity objectives for measuring and managing risk and performance.

3.2.2 Establishing And Maintaining Risk Thresholds

3.2.2.1 The Security Officer must establish risk appetite and risk tolerance statements.

3.2.2.2 The Security Officer must communicate and maintain these statements.

3.2.2.3 The Security Officer must determine and communicate risk appetite statements.

3.2.2.4 The Security Officer must translate risk appetite statements into specific, measurable, and broadly understandable risk tolerance statements.

3.2.2.5 The Security Officer must, as-needed, refine organizational objectives and risk appetite based on known risk exposure and residual risk.

3.2.3 Integrating Cybersecurity Into Enterprise Risk

3.2.3.1 The Security Officer must include cybersecurity risk management activities and outcomes in enterprise risk management processes.

3.2.3.2 The Security Officer must, annually, aggregate cybersecurity risks alongside other enterprise risks such as compliance, financial, operational, regulatory, reputational, and safety.

3.2.3.3 The Security Officer must, annually, include cybersecurity risk managers in enterprise risk management planning.

3.2.3.4 The Security Officer must establish criteria for escalating cybersecurity risks within enterprise risk management.

3.2.4 Defining And Communicating Risk Strategies

3.2.4.1 The Security Officer must establish and communicate strategic direction that describes appropriate risk response options.

3.2.4.2 The Security Officer must specify criteria for accepting and avoiding cybersecurity risk for various classifications of data.

3.2.4.3 The Controller must, annually, determine whether to purchase cybersecurity insurance.

3.2.4.4 The Security Officer must, as-needed, document conditions under which shared responsibility models are acceptable, such as outsourcing cybersecurity functions or using public cloud-based services.

3.2.5 Establishing Cybersecurity Communication Lines

3.2.5.1 The Security Officer must establish lines of communication across the organization for cybersecurity risks, including those from suppliers and other third parties.

3.2.5.2 The Security Officer must, quarterly, determine how to update senior executives, directors, and management on the organization's cybersecurity posture at agreed-upon intervals.

3.2.5.3 The Security Officer must identify communication methods for departments across the organization to discuss cybersecurity risks, including management, operations, internal auditors, legal, acquisition, physical security, and HR.

3.2.6 Standardizing Risk Assessment Methods

3.2.6.1 The Security Officer must establish and communicate a standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks.

3.2.6.2 The Security Officer must establish criteria for using a quantitative approach to cybersecurity risk analysis.

3.2.6.3 The Security Officer must specify probability and exposure formulas for cybersecurity risk analysis.

3.2.6.4 The Security Officer must create templates to document cybersecurity risk information, such as risk descriptions, exposure, treatment, and ownership.

3.2.6.5 The Security Officer must establish criteria for risk prioritization at the appropriate levels within the enterprise.

3.2.6.6 The Security Officer must use a consistent list of risk categories to support the integration, aggregation, and comparison of cybersecurity risks.

3.2.7 Including Strategic Opportunities In Risk Talks

3.2.7.1 The Security Officer must, annually, characterize strategic opportunities (i.e., positive risks) and include them in organizational cybersecurity risk discussions.

3.2.7.2 The Security Officer must define guidance for identifying opportunities.

3.2.7.3 The Security Officer must, as-needed, communicate methods for including opportunities in risk discussions, such as SWOT analysis.

3.2.7.4 Senior Management must, annually, identify stretch goals.

3.2.7.5 Senior Management must, annually, document identified stretch goals.

3.2.7.6 The Security Officer must, annually, calculate positive risks.

3.2.7.7 The Security Officer must, annually, document positive risks.

3.2.7.8 The Security Officer must, annually, prioritize positive risks alongside negative risks.

3.3 Roles, Responsibilities, And Authorities

3.3.1 Leadership Drives Ethical Risk Culture

3.3.1.1 Senior Management must ensure organizational leadership is responsible and accountable for cybersecurity risk.

3.3.1.2 The Chief Executive Officer must foster a culture that is risk-aware, ethical, and continually improving.

3.3.1.3 Senior Management must have leaders agree on their roles in developing, implementing, and assessing the cybersecurity strategy.

3.3.1.4 The Chief Executive Officer must share leaders' expectations for a secure and ethical culture.

3.3.1.5 The Security Officer must, as-needed, use current events to highlight examples of cybersecurity risk management.

3.3.1.6 The Chief Executive Officer must direct the CISO to maintain a comprehensive cybersecurity risk strategy.

3.3.1.7 The Security Officer must review and update the cybersecurity risk strategy annually and after major events.

3.3.1.8 The Security Officer must, annually, conduct reviews to ensure adequate authority and coordination among those managing cybersecurity risk.

3.3.2 Clarifying Cybersecurity Roles And Responsibilities

3.3.2.1 The Security Officer must establish roles, responsibilities, and authorities related to cybersecurity risk management.

3.3.2.2 The Security Officer must, annually, communicate and enforce these roles and responsibilities.

3.3.2.3 The Security Officer must document risk management roles and responsibilities in policy.

3.3.2.4 The Security Officer must document who is responsible and accountable for cybersecurity risk management activities.

3.3.2.5 The Security Officer must specify how teams and individuals are to be consulted and informed.

3.3.2.6 The HR Director must, annually, include cybersecurity responsibilities in personnel descriptions.

3.3.2.7 The Security Officer must document performance goals for personnel with cybersecurity risk management responsibilities.

3.3.2.8 The Security Officer must, quarterly, measure performance to identify areas for improvement.

3.3.2.9 The Security Officer must articulate cybersecurity responsibilities within operations, risk functions, and internal audit functions.

3.3.3 Allocating Resources For Cybersecurity Needs

3.3.3.1 The Controller must allocate adequate resources commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.

3.3.3.2 The Chief Executive Officer must, annually, conduct management reviews to ensure those responsible for cybersecurity risk management have the necessary authority.

3.3.3.3 The Controller must, annually, identify resource allocation and investment in line with risk tolerance and response.

3.3.3.4 The Chief Executive Officer must provide adequate people, process, and technical resources to support the cybersecurity strategy.

3.3.4 Incorporating Cybersecurity In Hr Practices

3.3.4.1 The HR Director must include cybersecurity in human resources practices.

3.3.4.2 The HR Director must integrate cybersecurity risk management considerations into human resources processes, including personnel screening, onboarding, change notification, and offboarding.

3.3.4.3 The HR Director must consider cybersecurity knowledge as a positive factor in hiring, training, and retention decisions.

3.3.4.4 The HR Director must, as-needed, conduct background checks prior to onboarding new personnel for sensitive roles.

3.3.4.5 The HR Director must, as-needed, repeat background checks for personnel in sensitive roles.

3.3.4.6 The Security Officer must define obligations for personnel to be aware of, adhere to, and uphold security policies related to their roles.

3.3.4.7 The Security Officer must enforce these obligations.

3.4 Policy

3.4.1 Establishing And Enforcing Risk Management Policy

3.4.1.1 The Security Officer must establish a policy for managing cybersecurity risks based on organizational context, cybersecurity strategy, and priorities.

3.4.1.2 The Security Officer must communicate and enforce the cybersecurity risk management policy.

3.4.1.3 The Security Officer must create a risk management policy with statements of management intent, expectations, and direction.

3.4.1.4 The HR Director must, annually, disseminate the risk management policy.

3.4.1.5 The Security Officer must, annually, maintain the risk management policy to keep it understandable and usable.

3.4.1.6 The Security Officer must, annually, review the policy and supporting processes and procedures.

3.4.1.7 The Security Officer must, annually, ensure alignment of the policy with risk management strategy objectives and the high-level direction of the cybersecurity policy.

3.4.1.8 The Chief Executive Officer must, annually, review and approve cybersecurity policy.

3.4.1.9 The Security Officer must, annually, communicate the cybersecurity risk management policy and supporting processes across the organization.

3.4.1.10 HR Staff must require personnel to acknowledge receipt of policy when first hired.

3.4.1.11 HR Staff must, annually, require personnel to acknowledge receipt of policy annually and whenever it is updated.

3.4.2 Updating Risk Management Policy Regularly

3.4.2.1 The Security Officer must, annually, review and update the policy for managing cybersecurity risks.

3.4.2.2 The Security Officer must, annually, communicate and enforce the updated policy.

3.4.2.3 The Security Officer must, annually, update policy based on periodic reviews of cybersecurity risk management results.

3.4.2.4 The Security Officer must, annually, ensure the policy maintains risk at an acceptable level.

3.4.2.5 The Security Officer must, annually, provide a timeline for reviewing changes to the organization's risk environment.

3.4.2.6 The Security Officer must, annually, communicate recommended policy updates.

3.4.2.7 The Security Officer must, as-needed, update policy to reflect changes in legal and regulatory requirements.

3.4.2.8 The VP, Technology must, as-needed, update policy to reflect changes in technology.

3.4.2.9 The Chief Executive Officer must, as-needed, update policy to reflect changes to the business.

3.5 Oversight

3.5.1 Reviewing And Adjusting Risk Strategy

3.5.1.1 The Security Officer must, annually, review cybersecurity risk management strategy outcomes.

3.5.1.2 The Security Officer must, annually, use reviews to inform and adjust strategy and direction.

3.5.1.3 The Chief Executive Officer must, annually, measure the effectiveness of the risk management strategy in aiding leaders' decision-making.

3.5.1.4 The Chief Executive Officer must, annually, measure how risk results have helped achieve organizational objectives.

3.5.1.5 The Chief Executive Officer must, annually, examine if cybersecurity risk strategies that impede operations need adjustment.

3.5.1.6 The Chief Executive Officer must, annually, examine if cybersecurity risk strategies that impede innovation need adjustment.

3.5.1.7 The Chief Executive Officer must establish a Security Committee comprised of representatives from HEALTHeLINK's stakeholders for the purposes of providing guidance, review and approval of security policies, and support for the security program in accordance with the Security Committee charter.

3.5.2 Ensuring Comprehensive Risk Strategy Review

3.5.2.1 The Security Officer must, annually, review the cybersecurity risk management strategy.

3.5.2.2 The Security Officer must, annually, adjust the strategy to ensure it covers organizational requirements and risks.

3.5.2.3 The Security Officer must, as-needed, review audit findings to confirm compliance with internal and external requirements.

3.5.2.4 The Security Officer must, annually, review the performance oversight of personnel in cybersecurity-related roles.

3.5.2.5 The Security Officer must, annually, determine if policy changes are necessary based on the oversight review.

3.5.2.6 Incident Response Team Members must, as-needed, review strategy in response to cybersecurity incidents.

3.5.3 Evaluating And Refining Cybersecurity Performance

3.5.3.1 The Security Officer must, annually, evaluate organizational cybersecurity risk management performance.

3.5.3.2 The Security Officer must, annually, review for adjustments needed in cybersecurity risk management.

3.5.3.3 The Chief Executive Officer must, quarterly, review key performance indicators to ensure policies achieve objectives.

3.5.3.4 The Security Officer must, quarterly, review key risk indicators to identify risks faced by the organization.

3.5.3.5 The Security Officer must assess the likelihood and potential impact of identified risks.

3.5.3.6 The Security Officer must, quarterly, collect metrics on cybersecurity risk management.

3.5.3.7 The Security Officer must, quarterly, communicate cybersecurity risk management metrics to senior leadership.

3.6 Cybersecurity Supply Chain Risk Management

3.6.1 Establishing A Supply Chain Risk Management Program

3.6.1.1 The Security Officer must establish and agree upon a cybersecurity supply chain risk management program, strategy, objectives, policies, and processes with organizational stakeholders.

3.6.1.2 The Security Officer must establish a strategy that expresses the objectives of the cybersecurity supply chain risk management program.

3.6.1.3 The Security Officer must develop the cybersecurity supply chain risk management program.

3.6.1.4 The Security Officer must create a plan with milestones, policies, and procedures that guide implementation and improvement of the program.

3.6.1.5 The Security Officer must, annually, share the policies and procedures with organizational stakeholders.

3.6.1.6 The Security Officer must develop and implement program processes based on the agreed-upon strategy, objectives, policies, and procedures.

3.6.1.7 The Security Officer must establish a cross-organizational mechanism that ensures alignment between functions contributing to cybersecurity supply chain risk management, such as cybersecurity, IT, operations, legal, human resources, and engineering.

3.6.2 Coordinating Cybersecurity Roles In Supply Chain

3.6.2.1 The Security Officer must establish and communicate cybersecurity roles and responsibilities for suppliers, customers, and partners both internally and externally.

3.6.2.2 The Security Officer must identify specific roles or positions responsible and accountable for cybersecurity supply chain risk management activities.

3.6.2.3 The Security Officer must, annually, document cybersecurity supply chain risk management roles and responsibilities in policy.

3.6.2.4 The Security Officer must, annually, create responsibility matrixes to document responsibilities and accountability for cybersecurity supply chain risk management.

3.6.2.5 The Security Officer must, annually, specify how teams and individuals will be consulted and informed in the responsibility matrixes.

3.6.2.6 The HR Director must, annually, include cybersecurity supply chain risk management responsibilities and performance requirements in personnel descriptions.

3.6.2.7 The HR Director must, annually, document performance goals for personnel with cybersecurity risk management-specific responsibilities.

3.6.2.8 The Security Officer must, quarterly, measure performance to demonstrate and improve performance.

3.6.2.9 The Security Officer must develop roles and responsibilities for suppliers, customers, and business partners regarding shared cybersecurity risks.

3.6.2.10 The Security Officer must integrate these roles and responsibilities into organizational policies and third-party agreements.

3.6.2.11 The Security Officer must internally communicate cybersecurity supply chain risk management roles and responsibilities for third parties.

3.6.2.12 The Security Officer must establish rules and protocols for information sharing and reporting processes with suppliers.

3.6.3 Integrating Supply Chain Risk Management

3.6.3.1 The Security Officer must integrate cybersecurity supply chain risk management into cybersecurity and enterprise risk management, risk assessment, and improvement processes.

3.6.3.2 The Security Officer must identify areas of alignment and overlap with cybersecurity and enterprise risk management.

3.6.3.3 The Security Officer must establish integrated control sets for cybersecurity risk management and cybersecurity supply chain risk management.

3.6.3.4 The Security Officer must integrate cybersecurity supply chain risk management into improvement processes.

3.6.3.5 The Security Officer must, as-needed, escalate material cybersecurity risks in supply chains to senior management.

3.6.3.6 The Chief Executive Officer must, as-needed, address these risks at the enterprise risk management level.

3.6.4 Prioritizing Suppliers By Criticality

3.6.4.1 Senior Management must, annually, identify and prioritize suppliers by criticality.

3.6.4.2 Senior Management must develop criteria for supplier criticality based on the sensitivity of data processed or possessed by suppliers, their access to the organization's systems, and the importance of their products or services.

3.6.4.3 Senior Management must keep a record of all suppliers.

3.6.4.4 Senior Management must, annually, prioritize suppliers based on the criticality criteria.

3.6.5 Integrating Cybersecurity Requirements In Contracts

3.6.5.1 The Security Officer must establish and prioritize requirements to address cybersecurity risks in supply chains.

3.6.5.2 The Chief Operating Officer must integrate these requirements into contracts and other agreements with suppliers and other relevant third parties.

3.6.5.3 Senior Management must establish security requirements for suppliers, products, and services based on their criticality level and potential impact if compromised.

3.6.5.4 The Chief Operating Officer must, as-needed, specify in contracts and other agreements the rights and responsibilities related to potential cybersecurity risks.

3.6.5.5 The Chief Operating Officer must include all cybersecurity and supply chain requirements in default contractual language.

3.6.5.6 The Security Officer must specify how compliance with these requirements may be verified.

3.6.5.7 The Chief Operating Officer must define the rules and protocols for information sharing between the organization and its suppliers and sub-tier suppliers in agreements.

3.6.5.8 The Chief Operating Officer must manage risk by including security requirements in agreements based on criticality and potential impact if compromised.

3.6.5.9 Senior Management must define security requirements in service-level agreements for monitoring suppliers for acceptable security performance throughout the supplier relationship lifecycle.

3.6.5.10 Senior Management must contractually require suppliers to disclose cybersecurity features, functions, and vulnerabilities of their products and services.

3.6.5.11 Senior Management must contractually require suppliers to provide and maintain a current component inventory for critical products.

3.6.5.12 The HR Director must contractually require suppliers to vet their employees and guard against insider threats.

3.6.5.13 The Security Officer must contractually require suppliers to provide evidence of performing acceptable security practices through mechanisms like self-attestation, known standards, certifications, or inspections.

3.6.6 Pre-Engagement Risk Reduction Planning

3.6.6.1 Senior Management must, as-needed, perform planning and due diligence to reduce risks before entering into formal supplier or third-party relationships.

3.6.6.2 Senior Management must, as-needed, perform thorough due diligence on prospective suppliers consistent with procurement planning.

3.6.6.3 Senior Management must ensure due diligence is commensurate with the level of risk, criticality, and complexity of each supplier relationship.

3.6.6.4 Senior Management must, as-needed, assess the suitability of the technology, cybersecurity capabilities, and risk management practices of prospective suppliers.

3.6.6.5 Senior Management must, annually, conduct supplier risk assessments against business and applicable cybersecurity requirements.

3.6.6.6 Senior Management must, as-needed, assess the authenticity, integrity, and security of critical products prior to acquisition and use.

3.6.7 Comprehensive Third-Party Risk Management

3.6.7.1 Senior Management must understand, record, prioritize, assess, respond to, and monitor the risks posed by suppliers, their products and services, and other third parties throughout the relationship.

3.6.7.2 Senior Management must, as-needed, adjust assessment formats and frequencies based on the third party's reputation and the criticality of the products or services provided.

3.6.7.3 The Security Officer must, annually, evaluate third parties' evidence of compliance with contractual cybersecurity requirements.

3.6.7.4 Senior Management must monitor critical suppliers to ensure they fulfill their security obligations throughout the supplier relationship lifecycle.

3.6.7.5 Senior Management must, annually, use various methods and techniques such as inspections, audits, tests, or evaluations for monitoring.

3.6.7.6 Senior Management must, as-needed, monitor critical suppliers, services, and products for changes to their risk profiles.

3.6.7.7 Senior Management must, as-needed, reevaluate supplier criticality and risk impact accordingly.

3.6.7.8 The Security Officer must, annually, plan for unexpected supplier and supply chain-related interruptions to ensure business continuity.

3.6.8 Integrating Third-Parties In Incident Management

3.6.8.1 The Security Officer must, annually, include relevant suppliers and other third parties in incident planning, response, and recovery activities.

3.6.8.2 The Security Officer must define and use rules and protocols for reporting incident response and recovery activities and status between the organization and its suppliers.

3.6.8.3 The Security Officer must identify and document the roles and responsibilities of the organization and its suppliers for incident response.

3.6.8.4 The Security Officer must, annually, include critical suppliers in incident response exercises and simulations.

3.6.8.5 The Security Officer must define and coordinate crisis communication methods and protocols between the organization and its critical suppliers.

3.6.8.6 The Security Officer must, as-needed, conduct collaborative lessons learned sessions with critical suppliers.

3.6.9 Integrating Supply Chain Security Practices

3.6.9.1 The Security Officer must integrate supply chain security practices into cybersecurity and enterprise risk management programs.

3.6.9.2 Senior Management must monitor the performance of these practices throughout the technology product and service life cycle.

3.6.9.3 Senior Management must require provenance records for all acquired technology products and services in policies and procedures.

3.6.9.4 The Security Officer must, quarterly, provide risk reporting to leaders about the authenticity and integrity of acquired components.

3.6.9.5 The VP, Technology must communicate among cybersecurity risk managers and operations personnel about acquiring software patches, updates, and upgrades only from authenticated and trustworthy providers.

3.6.9.6 The Security Officer must, annually, review policies to ensure they require approved supplier personnel to perform maintenance on supplier products.

3.6.9.7 Senior Management must, as-needed, require checking upgrades to critical hardware for unauthorized changes in policies and procedures.

3.6.10 Post-Partnership Risk Management Provisions

3.6.10.1 The Security Officer must include provisions for activities after the conclusion of a partnership or service agreement in cybersecurity supply chain risk management plans.

3.6.10.2 Senior Management must establish processes for terminating critical relationships under both normal and adverse circumstances.

3.6.10.3 Senior Management must define and implement plans for component end-of-life maintenance support and obsolescence.

3.6.10.4 The Security Officer must, as-needed, verify that supplier access to organization resources is deactivated promptly when no longer needed.

3.6.10.5 Senior Management must, as-needed, verify that assets containing the organization's data are returned or properly disposed of in a timely, controlled, and safe manner.

3.6.10.6 Senior Management must develop and execute a plan for terminating or transitioning supplier relationships that accounts for supply chain security risk and resiliency.

3.6.10.7 The Security Officer must, as-needed, mitigate risks to data and systems created by supplier termination.

3.6.10.8 The Security Officer must, as-needed, manage data leakage risks associated with supplier termination.

3.6.11 Business Associates

3.6.11.1 The Chief Executive Officer must implement Business Associate Agreements to document that Business Associates safeguard sensitive information.

3.6.11.2 The Chief Executive Officer must maintain an inventory of HEALTHeLINK's Business Associate Agreements, including a record of security requirements addressed in each agreement.

3.6.11.3 The Chief Executive Officer must, as-needed, review HEALTHeLINK's Business Associate Agreements to ensure that applicable requirements, appropriate to the nature and extent of system and information access, are addressed.

3.6.11.4 The Chief Executive Officer must ensure that Business Associates are required to comply with applicable legal and regulatory requirements.

3.6.11.5 The Chief Executive Officer must ensure that Business Associates are required to promptly report security incidents and breaches of which they become aware.

3.6.11.6 The Chief Executive Officer must ensure that subcontractors of Business Associates are required to comply with applicable legal and regulatory requirements.

3.6.11.7 The Chief Executive Officer must establish and maintain an inventory of HEALTHeLINK's arrangements with governmental entities.

3.6.11.8 Senior Management must assess risks specific to third party access prior to providing third party access to HEALTHeLINK's systems and facilities.

3.6.11.9 The Chief Executive Officer must ensure that the security requirements of contracts and statements of work that involve sensitive or protected information conform with applicable regulatory requirements.

3.6.11.10 The Chief Executive Officer must ensure that contracts and statements of work that involve sensitive or protected information are executed by an authorized HEALTHeLINK representative.

3.6.12 Third Parties

3.6.12.1 Senior Management must ensure that risks related to a third party accessing, processing, transmitting, storing, managing, or destroying HEALTHeLINK's sensitive information or information systems are identified and appropriately addressed.

3.6.12.2 The Security Officer must implement an evaluation and authorization process for potential or planned changes to information technologies, communications, or services for public facing or third parties to determine their impact to the confidentiality, integrity, availability, or compliance requirements of organization information.

3.6.12.3 The Security Officer must implement a third party risk assessment process and perform audits of third parties as appropriate in response to information security incidents or in accordance with the terms of service agreements.

3.6.12.4 The Security Officer must implement a review and risk assessment process commensurate with requested changes to third party service levels, governance processes, or internal third party changes.

3.6.12.5 The Security Officer must ensure that the services of third parties are monitored to verify compliance with the security requirements of agreements.

3.6.12.6 Senior Management must notify the Security Officer of any material change in HEALTHeLINK's relationship with or services from a third party service provider.

3.6.12.7 The Security Officer must establish a process for coordinating security event and audit information with external organizations, when necessary.

3.6.12.8 The Chief Executive Officer must ensure that service level agreements define performance expectations, measurable outcomes, and remedies and response requirements in the event of non-compliance.

3.6.12.9 The Chief Executive Officer must require third party service providers of external information systems to identify the location of those systems.

3.6.12.10 The Security Officer must notify appropriate third parties, as required by regulation or agreement, of significant changes to security and privacy certifications or roles.

3.6.12.11 Senior Management must maintain communication with third party service providers to ensure that the third parties coordinate, manage, and communicate service changes to HEALTHeLINK.

3.6.13 Health Information Exchanges

3.6.13.1 The Chief Executive Officer must ensure that the comprehensive, multi-party trust agreements required for health information exchanges are signed by all eligible entities who wish to exchange data via a particular network.

3.6.13.2 The Chief Executive Officer must ensure that the comprehensive, multi-party trust agreements required for health information exchanges include a common set of terms and conditions, including appropriate minimum control and policy requirements, that establish each signatory's obligations, responsibilities, and expectations.

3.6.13.3 The Chief Executive Officer must establish appropriate language in agreements with third parties regarding the classification of shared data and interpretation of classification labels.

3.7 Acceptable Use

3.7.1 Information Handling

3.7.1.1 Workforce members must use the organization's information and assets ethically and to support business needs.

3.7.1.2 Workforce members must not try to access, modify, remove, or test information systems without authorization.

3.7.1.3 Workforce members must not try to disable or circumvent security safeguards intended to protect Loptr's information.

3.7.1.4 Workforce members must protect the organization's information from disclosure, theft, and loss both within and outside of the organization's facilities.

3.7.1.5 Workforce members must protect information according to the organization's information classification guidance.

3.7.2 Mobile and Remote Access

3.7.2.1 Workforce members must not allow unauthorized people to use the organization's computers, devices, and applications.

3.7.2.2 Workforce members must immediately report the loss, theft, or exchange of the organization's computers, mobile devices, or media.

3.7.3 Access Control Credentials

3.7.3.1 Workforce members must not use someone else's login credentials to access Loptr's information systems.

3.7.3.2 Workforce members must use only the computers, devices, and networks you have been authorized to use to access the organization's information.

3.7.3.3 Workforce members must lock or log-off of computers or devices when they are not in use.

3.7.3.4 Workforce members must use passwords that meet the organization's standards and that are difficult to guess.

3.7.3.5 Workforce members must not share user IDs, passwords, remote access tokens, card keys, or other assigned credentials.

3.7.4 Incident Reporting

3.7.4.1 Workforce members must report any known or suspected security incident or weakness to the information security officer.

3.7.4.2 Workforce members must cooperate with incident response team members during incident investigations.

3.7.5 Security Program Responsibilities

3.7.5.1 Workforce members must protect the organization's information and assets from unauthorized access, modification, duplication, disclosure, or loss.

3.7.5.2 Workforce members must follow the laws and regulations that cover collecting, storage, appropriate use, and disposal of information.

3.7.6 Password Management

3.7.6.1 Workforce members must follow the organization's password standards when creating, changing, and storing passwords.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Identify Risks and Threats

Information Security Policy
Policy No. SP-002

1 Introduction

The purpose of this policy is to ensure that HEALTHeLINK's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Asset Management

3.1.1 Maintaining Hardware Inventories

3.1.1.1 IT Staff must maintain inventories of hardware managed by the organization.

3.1.1.2 IT Staff must maintain inventories for all types of hardware, including IT, IoT, OT, and mobile devices.

3.1.1.3 Network Administrators must constantly monitor networks to detect new hardware and automatically update inventories.

3.1.2 Maintaining Software And Service Inventories

3.1.2.1 IT Staff must maintain inventories of software, services, and systems managed by the organization.

3.1.2.2 IT Staff must maintain inventories for all types of software and services, including commercial-off-the-shelf, open-source, custom applications, API services, and cloud-based applications and services.

3.1.2.3 IT System Administrators must constantly monitor all platforms, including containers and virtual machines, for changes to software and service inventories.

3.1.2.4 IT Staff must maintain an inventory of the organization's systems.

3.1.3 Maintaining Network Flow Representations

3.1.3.1 Network Administrators must maintain representations of the organization's authorized network communication and internal and external network data flows.

3.1.3.2 Network Administrators must, quarterly, maintain baselines of communication and data flows within the organization's wired and wireless networks.

3.1.3.3 Network Administrators must, quarterly, maintain baselines of communication and data flows between the organization and third parties.

3.1.3.4 IT System Administrators must, quarterly, maintain baselines of communication and data flows for the organization's IaaS usage.

3.1.3.5 Network Administrators must, quarterly, maintain documentation of expected network ports, protocols, and services typically used among authorized systems.

3.1.4 Maintaining Supplier Service Inventories

3.1.4.1 Senior Management must maintain inventories of services provided by suppliers.

3.1.4.2 IT Staff must inventory all external services used by the organization, including IaaS, PaaS, SaaS, APIs, and other externally hosted application services.

3.1.4.3 IT Staff must, as-needed, update the inventory when a new external service is utilized to ensure adequate cybersecurity risk management monitoring.

3.1.5 Prioritizing Assets By Criticality And Impact

3.1.5.1 The Security Officer must, annually, prioritize assets based on classification, criticality, resources, and impact on the mission.

3.1.5.2 The Security Officer must, annually, define criteria for prioritizing each class of assets.

3.1.5.3 The VP, Technology must, annually, apply the prioritization criteria to assets.

3.1.5.4 The VP, Technology must, as-needed, track the asset priorities and update them periodically or when significant organizational changes occur.

3.1.6 Maintaining Data And Metadata Inventories

3.1.6.1 The Security Officer must maintain inventories of data and corresponding metadata for designated data types.

3.1.6.2 The Security Officer must maintain a list of designated data types of interest, such as PII, PHI, financial account numbers, organizational IP, and operational technology data.

3.1.6.3 IT Staff must continuously discover and analyze ad hoc data to identify new instances of designated data types.

3.1.6.4 The Security Officer must, as-needed, assign data classifications to designated data types through tags or labels.

3.1.6.5 The Security Officer must track the provenance, data owner, and geolocation of each instance of designated data types.

3.1.7 Lifecycle Management Of It Assets

3.1.7.1 IT Staff must manage systems, hardware, software, services, and data throughout their life cycles.

3.1.7.2 The Security Officer must integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services.

3.1.7.3 Development Staff must integrate cybersecurity considerations into product life cycles.

3.1.7.4 The VP, Technology must, as-needed, identify unofficial uses of technology to meet mission objectives (i.e., shadow IT).

3.1.7.5 The VP, Technology must, annually, identify redundant systems, hardware, software, and services that increase the attack surface.

3.1.7.6 IT System Administrators must, as-needed, properly configure and secure systems, hardware, software, and services prior to their deployment in production.

3.1.7.7 IT Staff must, as-needed, update inventories when systems, hardware, software, and services are moved or transferred within the organization.

3.1.7.8 The Security Officer must, as-needed, securely destroy stored data based on the organization's data retention policy and manage a record of the destructions.

3.1.7.9 IT Staff must, as-needed, securely sanitize data storage when hardware is retired, decommissioned, reassigned, or sent for repairs or replacement.

3.1.7.10 The Manager, Infrastructure must, as-needed, offer methods for destroying paper, storage media, and other physical forms of data storage.

3.2 Risk Assessment

3.2.1 Identifying And Recording Asset Vulnerabilities

3.2.1.1 IT Security Analysts must identify, validate, and record vulnerabilities in assets.

3.2.1.2 IT System Administrators must use vulnerability management technologies to identify unpatched and misconfigured software.

3.2.1.3 Network Administrators must, monthly, assess network and system architectures for design and implementation weaknesses that affect cybersecurity.

3.2.1.4 Development Staff must, as-needed, review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities.

3.2.1.5 The Manager, Infrastructure must, annually, assess facilities housing critical computing assets for physical vulnerabilities and resilience issues.

3.2.1.6 The Security Officer must monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services.

3.2.1.7 Senior Management must, annually, review processes and procedures for weaknesses that could be exploited to affect cybersecurity.

3.2.2 Gathering Cyber Threat Intelligence

3.2.2.1 The Security Officer must receive cyber threat intelligence from information sharing forums and sources.

3.2.2.2 IT Staff must configure cybersecurity tools and technologies to securely ingest cyber threat intelligence feeds.

3.2.2.3 IT Security Analysts must receive and review advisories on current threat actors and their TTPs from reputable third parties.

3.2.2.4 The Security Officer must monitor sources of cyber threat intelligence for information on vulnerabilities that emerging technologies may have.

3.2.3 Identifying And Recording Threats

3.2.3.1 IT Security Analysts must identify and record internal and external threats to the organization.

3.2.3.2 IT Security Analysts must use cyber threat intelligence to maintain awareness of threat actors likely to target the organization and their probable TTPs.

3.2.3.3 IT Security Analysts must perform threat hunting to look for signs of threat actors within the environment.

3.2.3.4 The HR Director must implement processes for identifying internal threat actors.

3.2.4 Assessing Threat Impacts And Likelihoods

3.2.4.1 The Security Officer must identify and record the potential impacts and likelihoods of threats exploiting vulnerabilities.

3.2.4.2 The Security Officer must, as-needed, work with business leaders and cybersecurity risk management practitioners to estimate the likelihood and impactor risk scenarios and record them in risk registers.

3.2.4.3 The Security Officer must, annually, enumerate the potential business impacts of unauthorized access to the organization's communications, systems, and data processed in or by those systems.

3.2.4.4 The VP, Technology must account for the potential impacts of cascading failures for systems of systems.

3.2.5 Informing Risk Response With Threat Data

3.2.5.1 The Security Officer must use threats, vulnerabilities, likelihoods, and impacts to understand inherent risk and inform risk response prioritization.

3.2.5.2 IT Security Analysts must develop threat models to better understand risks to the data.

3.2.5.3 The Security Officer must identify appropriate risk responses based on the developed threat models.

3.2.5.4 The Controller must prioritize cybersecurity resource allocations and investments based on estimated likelihoods and impacts.

3.2.6 Managing And Communicating Risk Responses

3.2.6.1 The Security Officer must choose, prioritize, plan, track, and communicate risk responses.

3.2.6.2 The Security Officer must, as-needed, apply the vulnerability management plan's criteria to decide whether to accept, transfer, mitigate, or avoid risk.

3.2.6.3 The Security Officer must, as-needed, apply the vulnerability management plan's criteria to select compensating controls for mitigating risk.

3.2.6.4 The Security Officer must track the progress of risk response implementation using tools like POA&M, risk register, and risk detail report.

3.2.6.5 The Security Officer must use risk assessment findings to inform risk response decisions and actions.

3.2.6.6 The Security Officer must, as-needed, communicate planned risk responses to affected stakeholders in priority order.

3.2.7 Tracking Changes And Managing Exceptions

3.2.7.1 The VP, Technology must manage, assess for risk impact, record, and track changes and exceptions.

3.2.7.2 The VP, Technology must, as-needed, implement procedures for the formal documentation, review, testing, and approval of proposed changes and requested exceptions.

3.2.7.3 The VP, Technology must, as-needed, document the possible risks of making or not making each proposed change.

3.2.7.4 The VP, Technology must, as-needed, provide guidance on rolling back changes.

3.2.7.5 The Security Officer must, as-needed, document the risks related to each requested exception and the plan for responding to those risks.

3.2.7.6 The Security Officer must, annually, review risks that were accepted based on planned future actions or milestones.

3.2.8 Managing Vulnerability Disclosures

3.2.8.1 The Security Officer must establish processes for receiving, analyzing, and responding to vulnerability disclosures.

3.2.8.2 Senior Management must conduct vulnerability information sharing between the organization and its suppliers following defined rules and protocols in contracts.

3.2.8.3 The Security Officer must assign responsibilities for processing, analyzing the impact of, and responding to cybersecurity threat, vulnerability, or incident disclosures.

3.2.8.4 The Security Officer must verify the execution of procedures for responding to disclosures by suppliers, customers, partners, and government cybersecurity organizations.

3.2.9 Assessing Integrity Before Use

3.2.9.1 Senior Management must assess the authenticity and integrity of hardware and software prior to acquisition and use.

3.2.9.2 Senior Management must assess the authenticity and cybersecurity of critical technology products and services before acquisition and use.

3.2.10 Evaluating Critical Suppliers Pre-Acquisition

3.2.10.1 Senior Management must assess critical suppliers prior to acquisition.

3.2.10.2 Senior Management must conduct supplier risk assessments against business and applicable cybersecurity requirements, including the supply chain.

3.2.11 Assess CMS-defined Controls

3.2.11.1 The Security Officer must include a partial set of the CMS Catalog of Minimum Acceptable Risk Security and Privacy Controls in HEALTHeLINK's risk assessment activities, such that all controls are assessed in three years.

3.3 Improvement

3.3.1 Identifying Improvements From Evaluations

3.3.1.1 The Security Officer must identify improvements from evaluations.

3.3.1.2 The VP, Technology must, annually, perform self-assessments of critical services considering current threats and TTPs.

3.3.1.3 The Security Officer must, annually, invest in third-party assessments or independent audits to evaluate the effectiveness of the cybersecurity program.

3.3.1.4 The Security Officer must, as-needed, identify areas needing improvement from these assessments or audits.

3.3.1.5 The Security Officer must evaluate compliance with selected cybersecurity requirements through automated means constantly.

3.3.2 Improvements From Security Tests And Coordination

3.3.2.1 The Security Officer must, as-needed, identify improvements from security tests and exercises, including those done with suppliers and third parties.

3.3.2.2 The Security Officer must, as-needed, identify improvements for future incident response activities based on findings from incident response assessments.

3.3.2.3 The Security Officer must, as-needed, identify improvements for future business continuity, disaster recovery, and incident response activities based on exercises with critical service providers and product suppliers.

3.3.2.4 The Security Officer must involve internal stakeholders in security tests and exercises as appropriate.

3.3.2.5 IT Security Analysts must, annually, perform penetration testing on selected high-risk systems to identify opportunities to improve security.

3.3.2.6 Senior Management must, annually, exercise contingency plans for handling situations where products or services were compromised before receipt.

3.3.2.7 IT Security Analysts must collect and analyze performance metrics using security tools and services to inform improvements to the cybersecurity program.

3.3.3 Operational Process-Driven Improvements

3.3.3.1 The Chief Executive Officer must identify improvements from the execution of operational processes, procedures, and activities.

3.3.3.2 Senior Management must conduct collaborative lessons learned sessions with suppliers.

3.3.3.3 The Security Officer must, annually, review cybersecurity policies, processes, and procedures to incorporate lessons learned.

3.3.3.4 The VP, Technology must use metrics to assess operational cybersecurity performance over time.

3.3.4 Enhancing Incident Response Plans

3.3.4.1 The Security Officer must establish, communicate, maintain, and improve incident response plans and other cybersecurity plans that affect operations.

3.3.4.2 The Security Officer must establish contingency plans for responding to and recovering from adverse events.

3.3.4.3 The Security Officer must include contact and communication information, processes for handling common scenarios, and criteria for prioritization, escalation, and elevation in all contingency plans.

3.3.4.4 IT Security Analysts must, annually, create a vulnerability management plan to identify, assess, prioritize, test, and implement risk responses for all types of vulnerabilities.

3.3.4.5 The Security Officer must communicate cybersecurity plans and updates to those responsible for implementation and to affected parties.

3.3.4.6 The Security Officer must, annually, review and update cybersecurity plans.

3.3.4.7 The Security Officer must, as-needed, review and update cybersecurity plans when significant improvements are needed.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Cybersecurity Protection

Information Security Policy
Policy No. SP-003

1 Introduction

The purpose of this policy is to ensure that safeguards to manage HEALTHeLINK's cybersecurity risks are used.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Identity Management, Authentication, And Access Control

3.1.1 Managing Identities And Credentials

3.1.1.1 IT Staff must manage identities and credentials for authorized users, services, and hardware.

3.1.1.2 HR Staff must, as-needed, initiate requests for new or additional access for employees, contractors, and others.

3.1.1.3 IT Staff must track, review, and fulfill access requests with necessary permissions from system or data owners.

3.1.1.4 IT Staff must issue, manage, and revoke cryptographic certificates, identity tokens, cryptographic keys, and other credentials.

3.1.1.5 IT Staff must select a unique identifier for each device from immutable hardware characteristics or securely provisioned identifiers.

3.1.1.6 IT Security Analysts must, as-needed, physically label authorized hardware with an identifier for inventory and servicing purposes.

3.1.2 Binding Identities To Credentials Contextually

3.1.2.1 IT Staff must proof and bind identities to credentials based on the context of interactions.

3.1.2.2 IT Security Analysts must verify a person's claimed identity at enrollment using government-issued identity credentials.

3.1.2.3 IT Staff must issue a different credential for each person to prevent credential sharing.

3.1.3 Authenticating Users And Hardware

3.1.3.1 IT Staff must authenticate users, services, and hardware.

3.1.3.2 IT Staff must require multifactor authentication.

3.1.3.3 IT Staff must enforce policies for the minimum strength of passwords, PINs, and similar authenticators.

3.1.3.4 IT Staff must periodically reauthenticate users, services, and hardware based on risk.

3.1.3.5 IT Security Analysts must ensure that authorized personnel can access accounts essential for protecting safety under emergency conditions.

3.1.4 Securing Identity Assertions

3.1.4.1 IT Staff must protect, convey, and verify identity assertions.

3.1.4.2 IT Staff must protect identity assertions used in single sign-on systems.

3.1.4.3 IT Staff must protect identity assertions used between federated systems.

3.1.4.4 IT Staff must implement standards-based approaches for identity assertions in all contexts.

3.1.4.5 IT Staff must follow all guidance for the generation, protection, and verification of identity assertions.

3.1.5 Managing Access With Least Privilege

3.1.5.1 IT Staff must define access permissions, entitlements, and authorizations in a policy, manage, enforce, and review them, incorporating the principles of least privilege and separation of duties.

3.1.5.2 IT Security Analysts must, quarterly, review logical and physical access privileges.

3.1.5.3 HR Staff must, as-needed, review access privileges whenever someone changes roles or leaves the organization.

3.1.5.4 IT Staff must promptly rescind privileges that are no longer needed.

3.1.5.5 IT Staff must consider attributes of the requester and the requested resource for authorization decisions.

3.1.5.6 IT Staff must restrict access and privileges to the minimum necessary.

3.1.5.7 IT Security Analysts must, quarterly, review the privileges associated with critical business functions to confirm proper separation of duties.

3.1.6 Managing Physical Access By Risk Level

3.1.6.1 The Manager, Infrastructure must manage, monitor, and enforce physical access to assets commensurate with risk.

3.1.6.2 IT Security Analysts must use security measures like guards, cameras, locked entrances, and alarm systems to monitor facilities and restrict access.

3.1.6.3 IT Security Analysts must employ additional physical security controls for areas containing high-risk assets.

3.1.6.4 IT Security Analysts must, as-needed, escort guests, vendors, and other third parties within areas containing business-critical assets.

3.2 Awareness And Training

3.2.1 Training Personnel On Cybersecurity Awareness

3.2.1.1 The Security Officer must, annually, provide personnel with awareness and training so they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.

3.2.1.2 The Security Officer must, annually, provide basic cybersecurity awareness and training to all users of the organization's non-public resources.

3.2.1.3 The Security Officer must, annually, train personnel to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks.

3.2.1.4 HR Staff must, annually, explain the consequences of cybersecurity policy violations to individual users and the organization.

3.2.1.5 The Security Officer must, monthly, assess or test users on their understanding of basic cybersecurity practices.

3.2.1.6 The Security Officer must, annually, require refreshers to reinforce existing practices and introduce new practices.

3.2.2 Training Specialized Roles In Cybersecurity

3.2.2.1 The Security Officer must, annually, provide individuals in specialized roles with awareness and training so they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.

3.2.2.2 HR Staff must, annually, identify specialized roles within the organization that require additional cybersecurity training.

3.2.2.3 The Security Officer must, annually, provide role-based cybersecurity awareness and training to individuals in specialized roles, including contractors and third parties.

3.2.2.4 The Security Officer must, annually, assess or test users on their understanding of cybersecurity practices for their specialized roles.

3.2.2.5 The Security Officer must, annually, require refreshers to reinforce existing practices and introduce new practices for those in specialized roles.

3.3 Data Security

3.3.1 Protecting Data-At-Rest

3.3.1.1 The Security Officer must protect the confidentiality, integrity, and availability of data-at-rest.

3.3.1.2 The Security Officer must use encryption, digital signatures, and cryptographic hashes to protect stored data in files, databases, virtual machine disk images, and other resources.

3.3.1.3 IT System Administrators must use full disk encryption to protect data stored on user endpoints.

3.3.1.4 IT Security Analysts must confirm the integrity of software by validating signatures.

3.3.1.5 IT Security Analysts must restrict the use of removable media to prevent data exfiltration.

3.3.1.6 The Manager, Infrastructure must physically secure removable media containing unencrypted sensitive information in secure locations like locked offices or file cabinets.

3.3.2 Securing Data-In-Transit

3.3.2.1 IT Security Analysts must protect the confidentiality, integrity, and availability of data-in-transit.

3.3.2.2 IT Security Analysts must use encryption, digital signatures, and cryptographic hashes to protect network communications.

3.3.2.3 The Security Officer must automatically encrypt or block outbound emails and other communications containing sensitive data, based on data classification.

3.3.2.4 Network Administrators must block access to personal email, file sharing, and storage services from organizational systems and networks.

3.3.2.5 The Security Officer must prevent reuse of sensitive data from production environments in non-production environments.

3.3.3 Ensuring Data-In-Use Protection

3.3.3.1 Development Staff must protect the confidentiality, integrity, and availability of data-in-use.

3.3.3.2 IT System Administrators must remove data that must remain confidential from processors and memory as soon as it is no longer needed.

3.3.3.3 IT Security Analysts must protect data in use from access by other users and processes on the same platform.

3.3.4 Ensuring And Testing Data Backups

3.3.4.1 IT System Administrators must create, protect, maintain, and test backups of data.

3.3.4.2 IT System Administrators must continuously back up critical data in near-real-time, and frequently back up other data as per agreed schedules.

3.3.4.3 IT System Administrators must, quarterly, test backups and restores for all types of data sources.

3.3.4.4 IT System Administrators must securely store some backups offline and offsite to protect them from incidents or disasters.

3.3.4.5 IT System Administrators must enforce geographic separation and geolocation restrictions for data backup storage.

3.4 Platform Security

3.4.1 Applying Configuration Management Practices

3.4.1.1 The Manager, Infrastructure must establish and apply configuration management practices.

3.4.1.2 The Manager, Infrastructure must establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities.

3.4.1.3 Development Staff must, as-needed, review all default configuration settings for cybersecurity impacts when installing or upgrading software.

3.4.1.4 The Manager, Infrastructure must monitor implemented software for deviations from approved baselines.

3.4.2 Managing Software Lifecycle By Risk

3.4.2.1 Development Staff must maintain, replace, and remove software commensurate with risk.

3.4.2.2 IT Staff must perform routine and emergency patching as specified in the vulnerability management plan.

3.4.2.3 IT Staff must update container images and deploy new container instances to replace existing instances.

3.4.2.4 Development Staff must, as-needed, replace end-of-life software and service versions with supported, maintained versions.

3.4.2.5 IT Security Analysts must, as-needed, uninstall and remove unauthorized software and services that pose undue risks.

3.4.2.6 IT Security Analysts must, as-needed, uninstall and remove any unnecessary software components that might be misused by attackers.

3.4.2.7 Development Staff must define and implement plans for software and service end-of-life maintenance support and obsolescence.

3.4.3 Managing Hardware Lifecycle By Risk

3.4.3.1 IT Staff must maintain, replace, and remove hardware commensurate with risk.

3.4.3.2 IT Staff must, as-needed, replace hardware that lacks needed security capabilities or cannot support software with needed security capabilities.

3.4.3.3 IT Staff must define and implement plans for hardware end-of-life maintenance support and obsolescence.

3.4.3.4 The Manager, Infrastructure must, as-needed, perform hardware disposal in a secure, responsible, and auditable manner.

3.4.4 Generating Logs For Continuous Monitoring

3.4.4.1 IT Security Analysts must generate log records and make them available for continuous monitoring.

3.4.4.2 IT System Administrators must configure operating systems, applications, and services to generate log records.

3.4.4.3 IT Security Analysts must configure log generators to securely share their logs with the organization's logging infrastructure.

3.4.4.4 IT Security Analysts must ensure log generators record data needed by zero-trust architectures.

3.4.5 Preventing Unauthorized Software Use

3.4.5.1 The Security Officer must prevent the installation and execution of unauthorized software.

3.4.5.2 The Security Officer must restrict software execution to permitted products only when risk warrants it.

3.4.5.3 IT System Administrators must verify the source and integrity of new software before installation.

3.4.5.4 Network Administrators must configure platforms to use only approved DNS services that block access to known malicious domains.

3.4.5.5 IT System Administrators must allow the installation of only organization-approved software on platforms.

3.4.6 Integrating Secure Software Development Practices

3.4.6.1 Development Staff must integrate secure software development practices and monitor their performance throughout the software development life cycle.

3.4.6.2 Development Staff must protect all components of organization-developed software from tampering and unauthorized access.

3.4.6.3 Development Staff must ensure all software produced by the organization has minimal vulnerabilities in their releases.

3.4.6.4 The Manager, Infrastructure must maintain software used in production environments and securely dispose of software once it is no longer needed.

3.4.7 Certified Applications

3.4.7.1 IT Staff must ensure that access to sensitive information by Certified Applications is permitted in accordance with SHIN-NY encryption requirements, including the use of FIPS 140-2-compliance and NIST-validated modules where applicable, and other authorization requirements

3.4.7.2 IT Staff must ensure that access to sensitive information by Certified Applications is permitted in accordance with SHIN-NY authentication requirements

3.4.7.3 IT Staff must ensure that access to sensitive information by Certified Applications is permitted in accordance with SHIN-NY access control requirements

3.5 Technology Infrastructure Resilience

3.5.1 Securing Networks Against Unauthorized Access

3.5.1.1 IT Security Analysts must protect networks and environments from unauthorized logical access and usage.

3.5.1.2 Network Administrators must logically segment organization networks and cloud-based platforms according to trust boundaries and platform types, permitting only required communications between segments.

3.5.1.3 Network Administrators must logically segment organization networks from external networks, permitting only necessary communications from external networks into the organization's networks.

3.5.1.4 IT Security Analysts must implement zero trust architectures to restrict network access to each resource to the minimum necessary.

3.5.1.5 IT Staff must check the cyber health of endpoints before allowing access to and usage of production resources.

3.5.2 Protecting Assets From Environmental Threats

3.5.2.1 The Manager, Infrastructure must protect the organization's technology assets from environmental threats.

3.5.2.2 The Manager, Infrastructure must protect organizational equipment from environmental threats like flooding, fire, wind, and excessive heat and humidity.

3.5.2.3 Senior Management must include protection from environmental threats and provisions for adequate operating infrastructure in contracts with service providers.

3.5.3 Implementing Mechanisms For Resilience

3.5.3.1 The Security Officer must implement mechanisms to achieve resilience requirements in normal and adverse situations.

3.5.3.2 The Manager, Infrastructure must avoid single points of failure in systems and infrastructure.

3.5.3.3 Network Administrators must use load balancing to increase capacity and improve reliability.

3.5.3.4 The Manager, Infrastructure must use high-availability components like redundant storage and power supplies to enhance system reliability.

3.5.4 Maintaining Resource Capacity For Availability

3.5.4.1 The Manager, Infrastructure must maintain adequate resource capacity to ensure availability.

3.5.4.2 Senior Management must monitor usage of storage, power, compute, network bandwidth, and other resources.

3.5.4.3 The Manager, Infrastructure must, annually, forecast future needs and scale resources accordingly.

3.6 Record Retention

3.6.1 Clinical/Medical Records

3.6.1.1 Senior Management must retain clinical/medical records for six years from the date of discharge or death, or for individuals who are minors, for the longer of six years or three years after the individual reaches the age of majority.

3.6.1.2 IT Staff must compress and archive to digital media clinical/medical information which is retained in excess of ten years.

3.6.1.3 IT Staff must store archived clinical/medical information, including backups of such information, in secure areas.

3.6.1.4 IT Staff must maintain backups of retained clinical/medical information, including backups of archived versions of the information.

3.6.1.5 The Chief Executive Officer must ensure that controls are implemented to maintain the security of clinical/medical records, if retained, for at least 50 years following the date of death of the individual.

3.6.1.6 The Chief Executive Officer must ensure that notices issued by HEALTHeLINK, written acknowledgments of notice receipt, and record of efforts to obtain acknowledgment are retained for a period of six years.

3.6.1.7 The Chief Executive Officer must ensure that records of restrictions, designated record sets that are subject to access by individuals, the titles of those responsible for receiving and processing requests for access by individuals, and accountings of disclosure are retained for a period of six years.

3.6.2 Audit Logs

3.6.2.1 IT Staff must retain audit logs of HEALTHeLINK applications in an online, immediately accessible form for at least 180 days.

3.6.2.2 IT Staff must archive audit logs of the HEALTHeLINK applications that are older than 180 days but less than 10 years on digital storage media stored in secure areas.

3.6.3 Security Program Records

3.6.3.1 The Security Officer must verify that records of security-related actions, activities, and assessments (e.g., decisions related to addressable HIPAA implementation specifications, user rights of access, security incidents and investigations, business associate agreements, documentation of security-related repairs to facilities, changes to security-related policies and procedures) are retained for at least 6 years.

3.6.4 Information Assets

3.6.4.1 IT Staff must implement operational controls to retain and dispose of information assets, taking into account retention requirements, if applicable, based on an asset's data classification.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Threat Detection

Information Security Policy
Policy No. SP-004

1 Introduction

The purpose of this policy is to ensure that possible cybersecurity attacks and compromises are found and analyzed.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Continuous Monitoring

3.1.1 Monitoring Networks For Adverse Events

3.1.1.1 Network Administrators must monitor networks and network services to find potentially adverse events.

3.1.1.2 Network Administrators must monitor DNS, BGP, and other network services for adverse events.

3.1.1.3 Network Administrators must monitor wired networks for connections from unauthorized endpoints.

3.1.1.4 Network Administrators must monitor wireless networks for connections from unauthorized endpoints.

3.1.1.5 IT Security Analysts must, as-needed, monitor facilities for unauthorized or rogue wireless networks.

3.1.1.6 Network Administrators must compare actual network flows against baselines to detect deviations.

3.1.1.7 Network Administrators must monitor network communications to identify changes in security postures for zero trust purposes.

3.1.2 Monitoring Physical Environments For Risks

3.1.2.1 The Manager, Infrastructure must monitor the physical environment to find potentially adverse events.

3.1.2.2 IT Security Analysts must monitor logs from physical access control systems to find unusual access patterns.

3.1.2.3 IT Security Analysts must monitor logs from physical access control systems to find failed access attempts.

3.1.2.4 HR Staff must, monthly, review physical access records.

3.1.2.5 HR Staff must, monthly, monitor physical access records from visitor registration and sign-in sheets.

3.1.2.6 IT Security Analysts must, as-needed, monitor physical access controls for signs of tampering.

3.1.2.7 IT Security Analysts must monitor the physical environment using alarm systems.

3.1.2.8 IT Security Analysts must monitor the physical environment using cameras.

3.1.2.9 IT Security Analysts must monitor the physical environment using security guards.

3.1.3 Monitoring Personnel And Tech Usage

3.1.3.1 The HR Director must monitor personnel activity and technology usage to find potentially adverse events.

3.1.3.2 IT Staff must use behavior analytics software to detect anomalous user activity.

3.1.3.3 The Security Officer must use this software to mitigate insider threats.

3.1.3.4 IT Staff must monitor logs from logical access control systems to find unusual access patterns.

3.1.3.5 IT Staff must monitor logs from logical access control systems to find failed access attempts.

3.1.3.6 IT System Administrators must continuously monitor deception technology, including user accounts, for any usage.

3.1.4 Monitoring External Service Providers

3.1.4.1 The Manager, Infrastructure must monitor external service provider activities and services to find potentially adverse events.

3.1.4.2 The Manager, Infrastructure must, as-needed, monitor remote and onsite administration and maintenance activities performed by external providers on organizational systems.

3.1.4.3 IT System Administrators must monitor activity from cloud-based services for deviations from expected behavior.

3.1.4.4 Network Administrators must, as-needed, monitor activity from internet service providers for deviations from expected behavior.

3.1.4.5 The Manager, Infrastructure must, as-needed, monitor activity from other service providers for deviations from expected behavior.

3.1.5 Monitoring Computing Environments

3.1.5.1 IT Staff must monitor computing hardware and software, runtime environments, and their data to find potentially adverse events.

3.1.5.2 IT Staff must monitor email, web, file sharing, and collaboration services to detect malware.

3.1.5.3 IT Staff must monitor these services to detect phishing, data leaks, and exfiltration.

3.1.5.4 IT System Administrators must monitor authentication attempts to identify attacks against credentials.

3.1.5.5 IT System Administrators must monitor authentication attempts to identify unauthorized credential reuse.

3.1.5.6 IT Staff must monitor software configurations for deviations from security baselines.

3.1.5.7 IT Staff must, as-needed, monitor hardware and software for signs of tampering.

3.1.5.8 IT System Administrators must use endpoint technologies to detect cyber health issues such as missing patches.

3.1.5.9 IT System Administrators must use endpoint technologies to detect malware infections and unauthorized software.

3.1.5.10 IT System Administrators must redirect endpoints to a remediation environment before access is authorized if issues are detected.

3.2 Adverse Event Analysis

3.2.1 Analyzing Adverse Events

3.2.1.1 Incident Response Team Members must, as-needed, analyze potentially adverse events to better understand associated activities.

3.2.1.2 IT System Administrators must use security information and event management (SIEM) or other tools to continuously monitor log events.

3.2.1.3 IT Security Analysts must monitor for known malicious and suspicious activity using these tools.

3.2.1.4 The Security Officer must utilize up-to-date cyber threat intelligence in log analysis tools.

3.2.1.5 IT Security Analysts must improve detection accuracy using this intelligence.

3.2.1.6 IT Security Analysts must, as-needed, characterize threat actors, their methods, and indicators of compromise.

3.2.1.7 IT System Administrators must conduct manual reviews of log events.

3.2.1.8 IT System Administrators must focus manual reviews on technologies that cannot be sufficiently monitored through automation.

3.2.1.9 IT System Administrators must use log analysis tools to generate reports on findings.

3.2.2 Correlating Information From Various Sources

3.2.2.1 IT System Administrators must, as-needed, correlate information from multiple sources.

3.2.2.2 Network Administrators must constantly transfer log data to a relatively small number of log servers.

3.2.2.3 IT System Administrators must use event correlation technology, such as SIEM, to collect information.

3.2.2.4 IT System Administrators must, as-needed, ensure that this technology captures data from multiple sources.

3.2.2.5 The Security Officer must utilize cyber threat intelligence to help correlate events among log sources.

3.2.3 Estimating Impact And Scope Of Events

3.2.3.1 Senior Management must, as-needed, understand the estimated impact and scope of adverse events.

3.2.3.2 IT System Administrators must use SIEMs or other tools to estimate the impact and scope of adverse events.

3.2.3.3 The VP, Technology must, annually, review and refine these estimates.

3.2.3.4 The VP, Technology must create personal estimates of impact and scope.

3.2.4 Disseminating Information On Events

3.2.4.1 The Security Officer must, as-needed, provide information on adverse events to authorized staff and tools.

3.2.4.2 IT System Administrators must use cybersecurity software to generate alerts.

3.2.4.3 IT System Administrators must provide these alerts to the security operations center (SOC).

3.2.4.4 Incident Response Team Members must provide alerts to incident responders.

3.2.4.5 IT System Administrators must provide alerts to incident response tools.

3.2.4.6 Incident Response Team Members must ensure incident responders and other authorized personnel can access log analysis findings at all times.

3.2.4.7 IT Staff must automatically create and assign tickets when certain types of alerts occur.

3.2.4.8 IT Staff must, as-needed, manually create and assign tickets when technical staff discover indicators of compromise.

3.2.5 Integrating Cyber Threat Intelligence

3.2.5.1 The Security Officer must integrate cyber threat intelligence and other contextual information into the analysis.

3.2.5.2 IT System Administrators must securely provide cyber threat intelligence feeds to detection technologies.

3.2.5.3 The Security Officer must securely provide cyber threat intelligence feeds to processes and personnel.

3.2.5.4 IT Staff must, as-needed, securely provide information from asset inventories to detection technologies.

3.2.5.5 IT Staff must, as-needed, securely provide information from asset inventories to processes and personnel.

3.2.5.6 IT Security Analysts must rapidly acquire and analyze vulnerability disclosures from suppliers, vendors, and third-party security advisories.

3.2.6 Declaring Incidents Based On Criteria

3.2.6.1 Incident Response Team Members must, as-needed, declare incidents when adverse events meet the defined incident criteria.

3.2.6.2 Incident Response Team Members must, as-needed, apply incident criteria to known and assumed characteristics of activity.

3.2.6.3 Incident Response Team Members must, as-needed, determine whether an incident should be declared based on these criteria.

3.2.6.4 IT System Administrators must, as-needed, take known false positives into account when applying incident criteria.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Incident Response

Information Security Policy
Policy No. SP-005

1 Introduction

The purpose of this policy is to ensure that actions regarding a detected cybersecurity incident are taken.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Incident Management

3.1.1 Executing Incident Response Plans

3.1.1.1 The Security Officer must, as-needed, execute the incident response plan in coordination with relevant third parties once an incident is declared.

3.1.1.2 IT Security Analysts must ensure detection technologies automatically report confirmed incidents.

3.1.1.3 The Security Officer must, as-needed, request incident response assistance from the organization's incident response outsourcer.

3.1.1.4 The Security Officer must, as-needed, designate an incident lead for each incident.

3.1.1.5 The Security Officer must, as-needed, initiate execution of additional cybersecurity plans as needed to support incident response, such as business continuity and disaster recovery plans.

3.1.2 Triage And Validation Of Incident Reports

3.1.2.1 IT Security Analysts must triage and validate incident reports.

3.1.2.2 IT Security Analysts must preliminarily review incident reports to confirm they are cybersecurity-related and necessitate incident response activities.

3.1.2.3 The Security Officer must, as-needed, apply criteria to estimate the severity of an incident.

3.1.3 Categorizing And Prioritizing Incidents

3.1.3.1 The Security Officer must categorize and prioritize incidents.

3.1.3.2 The Security Officer must review and categorize incidents based on the type, such as data breach, ransomware, DDoS, or account compromise.

3.1.3.3 The Security Officer must prioritize incidents based on their scope, likely impact, and time-critical nature.

3.1.3.4 The Security Officer must, as-needed, select incident response strategies for active incidents, balancing quick recovery with the need to observe the attacker or conduct a thorough investigation.

3.1.4 Escalating Incidents As Necessary

3.1.4.1 The Security Officer must, as-needed, escalate or elevate incidents as needed.

3.1.4.2 The Security Officer must track and validate the status of all ongoing incidents.

3.1.4.3 The Security Officer must, as-needed, coordinate incident escalation or elevation with designated internal and external stakeholders.

3.1.5 Applying Incident Recovery Criteria

3.1.5.1 The Security Officer must, as-needed, apply criteria for initiating incident recovery.

3.1.5.2 The Security Officer must, as-needed, apply incident recovery criteria to known and assumed characteristics of the incident to determine whether to initiate incident recovery processes.

3.1.5.3 The Security Officer must, as-needed, consider the possible operational disruption of incident recovery activities.

3.2 Incident Analysis

3.2.1 Analyzing Incidents For Root Cause

3.2.1.1 Incident Response Team Members must, as-needed, perform analysis to establish what has occurred during an incident and identify the root cause.

3.2.1.2 Incident Response Team Members must, as-needed, determine the sequence of events that occurred during the incident and identify which assets and resources were involved in each event.

3.2.1.3 Incident Response Team Members must, as-needed, attempt to determine what vulnerabilities, threats, and threat actors were directly or indirectly involved in the incident.

3.2.1.4 Incident Response Team Members must, as-needed, analyze the incident to find the underlying, systemic root causes.

3.2.1.5 IT Security Analysts must, as-needed, check any cyber deception technology for additional information on attacker behavior.

3.2.2 Recording Investigative Actions

3.2.2.1 Incident Response Team Members must record actions performed during an investigation and preserve the integrity and provenance of the records.

3.2.2.2 Incident Response Team Members must require each person involved in incident response to record their actions immutably.

3.2.2.3 Incident Response Team Members must require the incident lead to document the incident in detail and preserve the integrity of the documentation and the sources of all information reported.

3.2.3 Collecting And Preserving Incident Data

3.2.3.1 IT Security Analysts must collect and preserve incident data and metadata, ensuring their integrity and provenance.

3.2.3.2 IT Security Analysts must collect, preserve, and safeguard all pertinent incident data and metadata based on evidence preservation and chain-of-custody procedures.

3.2.4 Estimating And Validating Incident Magnitude

3.2.4.1 The Security Officer must, as-needed, estimate and validate the magnitude of an incident.

3.2.4.2 IT Security Analysts must, as-needed, review other potential targets of the incident to search for indicators of compromise and evidence of persistence.

3.2.4.3 IT Security Analysts must, as-needed, run automated tools on targets to look for indicators of compromise and evidence of persistence.

3.3 Incident Response Reporting And Communication

3.3.1 Notifying Stakeholders Of Incidents

3.3.1.1 The Security Officer must, as-needed, notify internal stakeholders of incidents.

3.3.1.2 The Security Officer must, as-needed, notify external stakeholders of incidents.

3.3.1.3 The Chief Operating Officer must, as-needed, follow the organization's breach notification procedures after discovering a data breach, including notifying affected customers.

3.3.1.4 Senior Management must, as-needed, notify business partners and customers of incidents in accordance with contractual requirements.

3.3.1.5 The Security Officer must, as-needed, notify law enforcement agencies and regulatory bodies of incidents based on criteria in the incident response plan and management approval.

3.3.2 Sharing Incident Information

3.3.2.1 The Security Officer must, as-needed, share information with designated internal and external stakeholders.

3.3.2.2 The Security Officer must, as-needed, securely share information consistent with response plans and information sharing agreements.

3.3.2.3 IT Security Analysts must, as-needed, voluntarily share information about an attacker's observed TTPs, with all sensitive data removed, with an Information Sharing and Analysis Center (ISAC).

3.3.2.4 The HR Director must, as-needed, notify HR when malicious insider activity is detected.

3.3.2.5 The Security Officer must, as-needed, update senior leadership on the status of major incidents.

3.3.2.6 The Chief Operating Officer must, as-needed, follow the rules and protocols defined in contracts for incident information sharing between the organization and its suppliers.

3.3.2.7 Communications Manager must, as-needed, coordinate crisis communication methods between the organization and its critical suppliers.

3.4 Incident Mitigation

3.4.1 Containing Incidents

3.4.1.1 Incident Response Team Members must, as-needed, contain incidents.

3.4.1.2 IT Security Analysts must, as-needed, utilize cybersecurity technologies and cybersecurity features of other technologies to automatically perform containment actions.

3.4.1.3 Incident Response Team Members must, as-needed, allow incident responders to manually select and perform containment actions.

3.4.1.4 IT Security Analysts must, as-needed, allow a third party, such as an ISP or MSSP, to perform containment actions on behalf of the organization.

3.4.1.5 Network Administrators must, as-needed, automatically transfer compromised endpoints to a remediation VLAN.

3.4.2 Eradicating Incidents

3.4.2.1 Incident Response Team Members must, as-needed, eradicate incidents.

3.4.2.2 IT Security Analysts must, as-needed, utilize cybersecurity technologies and cybersecurity features of other technologies to automatically perform eradication actions.

3.4.2.3 Incident Response Team Members must, as-needed, allow incident responders to manually select and perform eradication actions.

3.4.2.4 IT Security Analysts must, as-needed, allow a third party, such as a managed security service provider, to perform eradication actions on behalf of the organization.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Incident Recovery

Information Security Policy
Policy No. SP-006

1 Introduction

The purpose of this policy is to ensure that assets and operations affected by a cybersecurity incident are restored.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Incident Recovery Plan Execution

3.1.1 Executing Recovery From Incident Response

3.1.1.1 The Security Officer must, as-needed, execute the recovery portion of the incident response plan once initiated from the incident response process.

3.1.1.2 Incident Response Team Members must, as-needed, begin recovery procedures during or after incident response processes.

3.1.1.3 The Security Officer must, as-needed, make all individuals with recovery responsibilities aware of the plans for recovery and the authorizations required to implement each aspect of the plans.

3.1.2 Selecting And Performing Recovery Actions

3.1.2.1 The Security Officer must, as-needed, select, scope, prioritize, and perform recovery actions.

3.1.2.2 The Security Officer must, as-needed, select recovery actions based on the criteria defined in the incident response plan and available resources.

3.1.2.3 The Security Officer must, as-needed, change planned recovery actions based on a reassessment of organizational needs and resources.

3.1.3 Verifying Integrity Of Restoration Assets

3.1.3.1 IT System Administrators must, as-needed, verify the integrity of backups and other restoration assets before using them for restoration.

3.1.3.2 IT System Administrators must, as-needed, check restoration assets for indicators of compromise, file corruption, and other integrity issues before use.

3.1.4 Establishing Post-Incident Norms

3.1.4.1 The Security Officer must, as-needed, consider critical mission functions and cybersecurity risk management to establish post-incident operational norms.

3.1.4.2 The Security Officer must, as-needed, use business impact and system categorization records to validate that essential services are restored in the appropriate order.

3.1.4.3 The Security Officer must, as-needed, work with system owners to confirm the successful restoration of systems and the return to normal operations.

3.1.4.4 Senior Management must, as-needed, monitor the performance of restored systems to verify the adequacy of the restoration.

3.1.5 Verifying And Restoring Operational Integrity

3.1.5.1 IT System Administrators must, as-needed, verify the integrity of restored assets, restore systems and services, and confirm normal operating status.

3.1.5.2 IT Security Analysts must, as-needed, check restored assets for indicators of compromise and remediation of root causes of the incident before production use.

3.1.5.3 IT System Administrators must, as-needed, verify the correctness and adequacy of the restoration actions taken before putting a restored system online.

3.1.6 Declaring End Of Incident Recovery

3.1.6.1 The Security Officer must, as-needed, declare the end of incident recovery based on criteria and complete incident-related documentation.

3.1.6.2 The Security Officer must, as-needed, prepare an after-action report that documents the incident, the response and recovery actions taken, and lessons learned.

3.1.6.3 The Security Officer must, as-needed, declare the end of incident recovery once the criteria are met.

3.2 Incident Recovery Communication

3.2.1 Communicating Recovery Progress

3.2.1.1 The Security Officer must, as-needed, communicate recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.

3.2.1.2 Senior Management must, as-needed, securely share recovery information, including restoration progress, consistent with response plans and information sharing agreements.

3.2.1.3 The Security Officer must, as-needed, update senior leadership on recovery status and restoration progress for major incidents.

3.2.1.4 Senior Management must, as-needed, follow defined rules and protocols for incident information sharing between the organization and its suppliers.

3.2.1.5 Senior Management must, as-needed, coordinate crisis communication between the organization and its critical suppliers.

3.2.2 Sharing Public Updates On Recovery

3.2.2.1 Senior Management must, as-needed, share public updates on incident recovery using approved methods and messaging.

3.2.2.2 The Chief Operating Officer must, as-needed, follow the organization's breach notification procedures when recovering from a data breach incident.

3.2.2.3 Senior Management must, as-needed, explain the steps being taken to recover from the incident and to prevent a recurrence.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

Participant Requirements

Information Security Policy
Policy No. SP-007

1 Introduction

The purpose of this policy is to establish HEALTHeLINK's expectations with respect to the security responsibilities of HEALTHeLINK participants.

2 Scope

This policy applies to all members of the workforce including full-time and part-time employees, temporary workers, contractors, consultants, vendors, auditors, and others engaged to perform work for or on behalf of HEALTHeLINK.

This policy applies to all of the physical locations owned, leased, or otherwise occupied by HEALTHeLINK. Wherever applicable, this policy further applies to physical locations outside of HEALTHeLINK where work is performed for or on behalf of HEALTHeLINK.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or used by HEALTHeLINK.

This policy applies to information throughout the information technology lifecycle and to any stage of an activity, function, project, or product involving information.

3 Policy Statement

3.1 Security Program

3.1.1 Responsibilities

3.1.1.1 HEALTHeLINK Authorized Users must be responsible and accountable for protecting HEALTHeLINK information and assets from unauthorized access, modification, duplication, disclosure, or loss.

3.1.1.2 HEALTHeLINK Authorized Users must be responsible and accountable for adherence with all applicable laws, regulations, and directives with respect to the collection, storage, safeguarding, appropriate use, and disposal of HEALTHeLINK information.

3.1.2 General

3.1.2.1 HEALTHeLINK Authorized Users must use and administer HEALTHeLINK's information and assets in an ethical manner and for authorized purposes only.

3.1.2.2 HEALTHeLINK Authorized Users must not share or disclose authentication credentials to another individual.

3.1.2.3 HEALTHeLINK Authorized Users must not attempt to perform unauthorized security testing including validating suspected weaknesses or accessing, modifying, or deleting information on information systems or services.

3.1.2.4 HEALTHeLINK Authorized Users must not disable nor attempt to disable or circumvent technical or other security controls and countermeasures intended to protect HEALTHeLINK's systems and facilities.

3.1.3 Information Handling

3.1.3.1 HEALTHeLINK Authorized Users must protect sensitive information against disclosure, theft, and loss, both within and outside of HEALTHeLINK's facilities, in printed form or fax, media, and on a portable device.

3.2 Access Control

3.2.1 Credentials

3.2.1.1 HEALTHeLINK Authorized Users must use only the user IDs, network addresses, and network connections issued to them to access HEALTHeLINK's information systems.

3.2.1.2 HEALTHeLINK Authorized Users must use passwords that are complex, are difficult to guess, and are not contained in a dictionary.

3.2.1.3 HEALTHeLINK Authorized Users must not share user IDs, passwords, remote access tokens, card keys, or other individually assigned credentials or authentication tools.

3.3 Incident Reporting

3.3.1 Incident Reporting

3.3.1.1 HEALTHeLINK Authorized Users must promptly report any known or suspected security incident, security weakness, or system fault to the Help Desk.

3.3.1.2 HEALTHeLINK Authorized Users must, as-needed, cooperate with Management and members of the Incident Response Team (IRT) during reporting and incident response activities.

3.4 HEALTHeLINK User Access

3.4.1 Access and Use

3.4.1.1 HEALTHeLINK Authorized Users must, as-needed, complete and submit an account setup form prior to being granted access to HEALTHeLINK applications.

3.4.1.2 Participant Authoritative Contacts must, as-needed, verify information submitted on an account setup form prior to submitting a new Authorized User to the Help Desk.

3.4.1.3 HEALTHeLINK Authorized Users must acknowledge and accept terms of use of HEALTHeLINK applications prior to accessing an application.

3.4.2 Administration

3.4.2.1 Participant Authoritative Contacts must, as-needed, verify the accuracy of the user information of Authorized Users and the need for access of each Authorized User.

3.5 Data Maintenance

3.5.1 Data Suppliers

3.5.1.1 Data Suppliers must send unfiltered data to HEALTHeLINK.

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

Non-compliance with information security policies may lead to disciplinary action that may include termination of employment. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

Workforce members must report instances of non-compliance with this information security policy to the Security Officer for incident response and/or exception handling.

HEALTHeLINK™

Glossary

Glossary

Privacy and Security Policies and Procedures
Policy No. GL-01

In addition to the terms below or otherwise defined in these Policies and Procedures, refer to the current Statewide Health Information Network for New York (SHIN-NY) Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 N.Y.C.R.R. § 300.3(b)(1) and Health Insurance Portability and Accountability Act of 1996 (HIPAA).

AUTHORIZED PURPOSES

HEALTHeLINK and its Participants shall permit Authorized Users to Access Protected Health Information of a patient via the SHIN-NY only for purposes consistent with a patient's Affirmative Consent or an exception, Participation Agreement and regulatory requirements.

AVAILABILITY

Property that data or information is accessible and usable upon demand by an authorized person.

BUSINESS ASSOCIATE (BA)

A person or entity meeting the HIPAA definition of 45 C.F.R. § 160.103 that performs certain functions or activities that involve the use or disclosure of Protected Health Information on behalf of, or provides services to, a HIPAA covered entity.

CLINICAL/MEDICAL RECORD

All data that is created, received, or maintained as part of HEALTHeLINK's normal business activities, which may be stored on any electronic media (e.g., tape, hard drive, disk, or other electronic storage device).

DATA INTEGRITY

The assurance that data stored on computer systems has not been altered or destroyed in an unauthorized manner.

DATA USE AGREEMENT (DUA)

The contractual agreement between HEALTHeLINK and the data use applicant describing the terms and conditions for the release of data to the applicant. The approved DURA will be attached to the DUA as a schedule as will the documented IRB decision.

DATA USE AND RECIPROCAL SUPPORT AGREEMENT (DURSA)

The data use agreement entered into by HEALTHeLINK as a requirement for participation in the eHealth Exchange.

DATA USE REQUEST APPLICATION (DURA)

A form to be completed by the requester that identifies the entity requesting data, the purpose(s) and objective(s) for the Research, a description of the Research and methodology, justification for release of the data especially focusing on the merit(s) of the Research including the risks and benefits, how the results of the Research will be used, details of the funding sources supporting the Research, and full disclosure of commercialization opportunities.

DESIGNATED RECORD SET

The same meaning as the term “Designated Record Set”, as defined in 45 C.F.R. § 164.501.

DURSA PARTICIPANT

Any organization that meets the requirements for participation as contained in the DURSA Operating Policies and Procedures, is provided with digital credentials, and is a signatory to the DURSA or a Joinder Agreement. HEALTHeLINK is a DURSA Participant.

DURSA PARTICIPANT USER

Any person who has been authorized to transact Message Content (as defined in the DURSA) through the respective DURSA Participant’s system in a manner defined by the respective DURSA Participant. DURSA Participant Users may include, but are not limited to, Health Care Providers; Health Plans; individuals whose health information is contained within, or available through, a DURSA Participant’s System; and employees, contractors, or agents of a DURSA Participant. Participants and their Authorized Users, as defined in the Participation Agreement, are DURSA Participant Users.

EMPLOYEES

Employees, students/trainees, volunteers, consultants and other individuals under the direct control of HEALTHeLINK or a Participant, whether or not they are paid or whether their access to the system is temporary or long-term.

ENCRYPTION

Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

EVENT

Any observable occurrence in a system.

EXTERNAL NETWORKS

Statewide, nationwide or other health information exchange networks, including but not limited to the SHIN-NY, which enable the secure exchange of health information among authorized parties.

HEALTH INFORMATION EXCHANGE (HIE)

HEALTHeLINK's systems, devices, mechanisms and infrastructure to facilitate the electronic movement of Patient Data among Participants according to nationally recognized standards.

HEALTHELINK INFORMATION

Information for which HEALTHeLINK fulfills the role of Information Owner.

HEALTHELINK RESEARCH COMMITTEE

A committee of HEALTHeLINK that is organized to review and approve Research proposals and which meets the requirements set forth at 45 C.F.R. § 164.512(i)(1)(i)(B), meaning that the committee (i) has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the Research protocol on individuals' privacy rights and related interests; (ii) includes at least one member who is not an employee, contractor, officer or director of HEALTHeLINK or any entity conducting or sponsoring the research, and is not related to any person who meets any of the forgoing criteria; and (iii) does not have any member participating in a review of any project in which the member has a conflict of interest.

INCIDENT

An occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

Set of policies and procedures for systematically managing an organization's sensitive data.

INFORMATION SYSTEM

An interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

INSTITUTIONAL REVIEW BOARD (IRB)

The IRB is an administrative body established to protect the rights and welfare of human Research subjects recruited to participate in research activities conducted under the auspices of the institution with which it is affiliated.

INTEGRITY

Property that data or information have not been altered or destroyed in an unauthorized manner.

MALWARE

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host.

MINOR

A person under eighteen (18) years of age.

MINOR CONSENT INFORMATION

Protected Health Information relating to medical treatment of a minor for which the minor provided his or her own consent without a parent’s or guardian’s permission, as permitted by New York law or other applicable laws for certain types of health services (e.g., reproductive health, HIV testing, STI, mental health or substance use treatment) or services consented to by an Emancipated Minor.

Minor consent patient information includes, but is not limited to patient information concerning:

(i) treatment of such patient for sexually transmitted disease or the performance of an abortion as provided in section 17 of the Public Health Law;
(ii) the diagnosis, treatment or prescription for a sexually transmitted disease as provided in section 2305 of the Public Health Law;
(iii) medical, dental, health and hospital services relating to prenatal care as provided in section 2504(3) of the Public Health Law;
(iv) an HIV test as provided in section 2781 of the Public Health Law;
(v) mental health services as provided in section 33.21 of the Mental Hygiene Law;
(vi) alcohol and substance abuse treatment as provided in section 22.11 of the Mental Hygiene Law;
(vii) any patient who is the parent of a child or has married as provided in section 2504 of the Public Health Law or an otherwise legally emancipated minor;

(viii) treatment that a minor has a Constitutional right to receive without a parent's or guardian's permission as determined by courts of competent jurisdiction;

(ix) Treatment for a minor who is a victim of sexual assault as provided in section 2805-i of the Public Health Law;

(x) Emergency care as provided in section 2504(4) of the Public Health Law.

MINOR CONSENTED SERVICES

Healthcare services provided to a minor that generate Minor Consent Information.

PASSWORD

Confidential authentication information composed of a string of characters.

PATIENT DATA

Health information that is created or received by a health care provider, payer, employer, or other Covered Entity and relates to the past, present, or future physical or mental health condition of an individual or the provision of health care to an individual and that identifies the individual, or the past, present, or future payment for the provision of health care to an individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, including such information that is made available for exchange by a Data Provider or Data Supplier.

PRIVACY OFFICER

The privacy official, designated in compliance with HIPAA requirement of 45 C.F.R. § 164.530(a)(1), who is responsible for the development and implementation of privacy policies and procedures.

REGISTRATION APPLICATION

The application submitted by a person or entity that wishes to become a Participant.

RESEARCH COMMITTEE

Charter Members representatives and at-large members as may be appointed by the HEALTHeLINK Board of Directors from time to time, that establish the process and criteria for approving the release of data for research.

SAFEGUARD

Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system.

SECURITY INCIDENT

Has the same meaning as the term “Security Incident”, as defined in 45 C.F.R. § 164.304, but shall not include (i) unsuccessful attempts to penetrate computer networks, or severs maintained by Business Associate, and (ii) immaterial incidents that occur on a routine basis, such as general “pinging” or “denial of service” attacks.

SECURITY OFFICER

Primary responsible person for an entity’s security-related affairs.

SECURITY OR SECURITY MEASURES

Encompass all of the administrative, physical, and technical safeguards in an information system.

SHIN-NY POLICY GUIDANCE

The set of policies and procedures, including technical standards and SHIN-NY services and products, that are developed through the Statewide Collaboration Process and adopted by NYS DOH as provided in 10 N.Y.C.R.R. Section 300.3.

STAKEHOLDER

A Charter Member.

VENDOR

Each third party vendor of software, hardware and/or related services that, together with the software, hardware and/or related services provided by other Vendors, comprise the HIE and its services.

WORKFORCE

The employees, volunteers, trainees, and other persons whose work is under the direct control of a Covered Entity or Business Associate, regardless of whether they are paid.

HEALTHeLINK™

Revision History

Revision History

Privacy and Security Policies and Procedures
Document No. RH-001

Privacy Policies and Procedures

Preamble
Policy P00

Effective Date: 06/23/25
Review Dates:
Revision Effective Dates:

Compliance with Law and HEALTHeLINK Policies
Policy P01

Effective Date: 09/13/07
Review Dates:
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, ARCHIVED 06/30/16

Amendment of Data
Policy P02

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19
Revision Effective Dates: 06/25/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/01/18, ARCHIVED 07/29/19

Authorized User Access (formerly Minimum Necessary Access)
Policy P03

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 06/28/21, 06/27/22, 06/30/23, 12/23/24, 06/23/25

Patient Consent
Policy P04

Effective Date: 09/25/08
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 10/14/10, 04/25/13, 06/01/13, 06/30/16, 11/27/17, 07/01/18, 07/29/19, 06/29/20, 06/28/21, 06/27/22, 06/30/23, 12/23/24, 06/23/25

Patient Request for Restrictions or Confidential Communications Policy P05

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/23/25

Breach Response Policy P06

Effective Date: 06/29/08
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 04/01/10, 09/16/11, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/23/25

Privacy Complaints/Concerns Policy P07

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/30/23, 06/23/25

Access, Use, and Disclosure of Protected Health Information (PHI) Policy P08

Effective Date: 06/29/08
Review Dates: 05/26/16
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, ARCHIVED 06/30/16

Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures Policy P09

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 04/01/10, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/27/22, 06/23/25

Workforce Training for HEALTHeLINK Privacy and Security Policies and Procedures (formerly Participant Workforce Training for HEALTHeLINK Privacy and Security Policies and Procedures)

Policy P10

Effective Date: 06/29/08
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/23/25

Workforce Access to and Termination from HEALTHeLINK (formerly Workforce, Agent and Contractor Access to and Termination from HEALTHeLINK)

Policy P11

Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/23/25

Request for Accounting of Disclosures

Policy P12

Effective Date: 09/13/07
Review Dates: 05/26/16, 07/13/17
Revision Effective Dates: 06/25/09, 04/01/10, 04/25/13, 06/01/13, 06/30/16, ARCHIVED 08/17/17

Data for Research (formerly Release of Population Data)

Policy P13

Effective Date: 05/12/14
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20, 06/27/22, 06/30/23, 06/23/25

Alerts

Policy P14

Effective Date: 06/30/16
Review Dates: 10/26/17
Revision Effective Dates: ARCHIVED 11/27/17

Patient Engagement and Access
Policy P15

Effective Date: 11/27/17
Review Dates: 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 07/29/19, 06/28/21, 06/27/22, 06/30/23, ARCHIVED 06/23/25

Audit
Policy P16

Effective Date: 11/27/17
Review Dates: 05/24/18, 06/27/19, 05/28/20, 05/27/21, 05/26/22, 05/25/23, 11/21/24, 05/22/25
Revision Effective Dates: 07/29/19, 06/27/22, 06/30/23, ARCHIVED 06/23/25

Security Policies

Governance
Policy SP-001

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Identify Risks and Threats
Policy SP-002

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Cybersecurity Protection
Policy SP-003

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Threat Detection
Policy SP-004

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Incident Response
Policy SP-005

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Incident Recovery
Policy SP-006

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Participant Requirements
Policy SP-007

Effective Date: 05/23/24
Review Dates: 05/22/25
Revision Effective Dates: 06/28/24

Previous versions of the HEALTHeLINK Security Policies (as listed below) have been archived and replaced by the HEALTHeLINK Security Policies effective 05/23/24.

Effective Date: 09/13/07
Last Review Date: 05/25/23
Last Revision Effective Date: 06/30/23

Participant Requirements (SP-001)
Security Program (SP-002)
Risk Management (SP-003)
Personnel Security (SP-004)
Physical Security (SP-005)
Acceptable Use (SP-006)
Technical Security (SP-007)
Access Control (SP-008)

Effective Date: 09/16/11
Last Review Date: 05/25/23
Last Revision Effective Date: 06/30/23

Incident Reporting (SP-010)

Effective Date: 01/15/15
Last Review Date: 05/25/23
Last Revision Effective Date: 06/30/23

System Development Life Cycle (SP-009)
Incident Management (SP-011)
Business Continuity (SP-012)
Record Retention (SP-013)