HEALTHeLINK™

Privacy and Security Policies and Procedures

Privacy Officer: Patti Burandt
Security Officer: Chris Klimek

Table of Contents

Privacy and Security Policies and Procedures

Privacy Policies and Procedures

Security Policies

HEALTHeLINK™

Privacy Policies and Procedures

1 Policy Statement

HEALTHeLINK 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 PHI only for purposes consistent with a patient's Affirmative Consent or an exception as identified in HEALTHeLINK Policy P04, *Patient Consent*.

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 Authentication

3.1.1 Obligation to Ensure Authentication of Identity of Authorized User Prior to Access

HEALTHeLINK shall authenticate, or shall require their Participants to authenticate, each Authorized User's identity prior to providing such Authorized User with Access to Protected Health Information via HEALTHeLINK. Such authentication shall take place in accordance with the provisions of this Section 3.1.

3.1.2 Authentication Requirements

In light of the importance of strong security measures regarding the protection of patient data and authentication standard requirements for exchanges, including but not limited to the New York State Medicaid Program, HEALTHeLINK shall authenticate, and shall require their Participants to authenticate, each Authorized User through an authentication methodology that meets the minimum technical requirements for Authenticator Assurance Level 2 (AAL2) set forth in National Institute of Standards and Technology Special Publication 800-63 (hereinafter, "NIST SP 800-63").

3.1.3 Compliance with Policies Resulting from Statewide Risk Analysis

In the event that New York State conducts a statewide risk analysis of the potential harm and likelihood of adverse impacts that could result from an error in identity authentication within the SHIN-NY that indicates that authentication policies and procedures that differ from, or are in addition to, those set forth in this Section 3.1, should be adopted, any such authentication policies and procedures shall be developed and approved through the SCP before adoption.

3.1.4 Authentication of Certified Applications and Downstream Users

HEALTHeLINK, by permitting Access to the SHIN-NY by Participants through Certified Applications, must (i) implement systems consistent with the SHIN-NY Policy Standards for authenticating a Certified Application's credentials in connection with each Access request; and (ii) require each Participant Accessing Protected Health Information through a Certified Application to authenticate the Participant's users in a manner consistent with Section 3.1 of these Policies and Procedures.

3.2 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.

3.3 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.

3.4 Access Limited to Minimum Necessary Information

HEALTHeLINK and Participants must ensure that reasonable efforts are made, except in the case of access for Treatment, to limit the information accessed via HEALTHeLINK to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

3.5 Compliance With HIPAA Privacy Rule and HIPAA Security Rule

A. Each Participant that is a Covered Entity shall comply with the HIPAA Privacy Rule and HIPAA Security Rule.

B. Each Participant that is not a Covered Entity, other than a public health authority or a health oversight agency under HIPAA (45 C.F.R. Sections 164.501 and 164.512[b] and [d]), shall adopt the administrative, physical and technical safeguards that are required under the HIPAA Security Rule related to such Protected Health Information and shall assess whether addressable safeguards under the HIPAA Security Rule should be adopted. In determining which addressable safeguards to adopt, such Participants shall take into account their size, complexity, capabilities, and other factors set forth under 45 C.F.R. Section 164.306(b). Nothing herein shall be construed to require Participants to comply with the HIPAA Security Rule and the HIPAA Privacy Rule with respect to information that does not constitute Protected Health Information.

3.6 Community-Based Organizations Not Subject to HIPAA

HEALTHeLINK may conduct due diligence in regards to a Community-Based Organization that is not a Covered Entity that is seeking to become HEALTHeLINK's Participant, and may reject such organization's request to become a Participant on the basis that the organization does not have sufficient security protocols or any other reason related to privacy or security, so long as such reason does not constitute illegal discrimination. If HEALTHeLINK recognizes a Community-Based Organization that is not a Covered Entity as a Participant, then the following requirements shall apply, in addition to those set forth in Section 3.5.B:

A. A Community-Based Organization that is not a Covered Entity may Access Protected Health Information via the SHIN-NY if the patient has executed an Affirmative Consent that permits Disclosure to such Community-Based Organization and HEALTHeLINK abides by the minimum necessary requirements set forth in P03 Section 3.6.C.

B. HEALTHeLINK and their Participants may Transmit Protected Health Information to a Community-Based Organization that is not a Covered Entity if the Transmittal occurs via direct or another encrypted means of communication and the following conditions are met:
   i. the patient has executed an Affirmative Consent that permits Disclosure to such Community-Based Organization; or
   ii. the Transmittal meets the requirements of a One-to-One Exchange under P04 Section 3.2.1 or is a Patient Care Alert that meets the requirements of P04 Section 3.2.9, and the Transmittal occurs in compliance with the HIPAA Privacy Rule and any other applicable federal law.

C. 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.

D. A Community-Based Organization that is not a Covered Entity may redisclose the Protected Health Information it receives via the SHIN-NY only to (i) the patient or the patient's Personal Representative; and (ii) another Participant for purposes of Treatment or Care Management.

4 References

- 45 C.F.R. § 164.514(d)(2)(i).
- HEALTHeLINK Policy P04, *Patient Consent.*
- 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).*

1 Policy Statement

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

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 Requirement to Obtain Affirmative Consent

Except as set forth in Section 3.2 of this Policy, HEALTHeLINK shall not Disclose a patient's PHI via HEALTHeLINK to a Participant unless the patient has provided an Affirmative Consent authorizing the Participant to Access or receive such PHI. An Affirmative Consent may be executed by an electronic signature as permitted by Section 3.9.5.

3.2 Exceptions to Affirmative Consent Requirement

Affirmative Consent shall not be required under the circumstances set forth below. Disclosures of Protected Health Information without Affirmative Consent shall comply with applicable federal, state and local laws and regulations, including 42 C.F.R. Part 2. Protected Health Information subject to 42 C.F.R. Part 2 shall not be Disclosed without Affirmative Consent unless 42 C.F.R. Part 2 specifically allows for such Disclosure.

3.2.1 One-to-One Exchanges

Affirmative Consent (as defined in the definitions section) shall not be required for a Transmittal of a patient's Protected Health Information originating from one Participant to another Participant if such Transmittal meets all the requirements of a One-to-One Exchange (including the requirements that the Transmittal occur with the patient's implicit or explicit consent) provided the Participants comply with existing federal and state laws and regulations requiring patient consent for the Disclosure and re-disclosure of information by health care providers.[1] If Protected Health Information is Transmitted to a Payer Organization under a One-to-One Exchange, such exchange must comply with Section 3.9.13 which allows an individual to request a restriction on the Disclosure of Protected Health Information.

3.2.2 Public Health Reporting and Access

A. If a Data Supplier or Participant is permitted to Disclose PHI to a government agency for purposes of public health reporting, including monitoring disease trends, conducting outbreak investigations, responding to public health emergencies, assessing the comparative effectiveness of medical treatments (including pharmaceuticals), conducting adverse drug event reporting, and informing new payment reforms, without patient consent under applicable state and federal laws and regulations, HEALTHeLINK may make that Disclosure on behalf of the Data Supplier or Participant without Affirmative Consent.

B. HEALTHeLINK may Disclose Protected Health Information to a Public Health Agency without Affirmative Consent for public health activities authorized by law, including:

i. To investigate suspected or confirmed cases of communicable disease (pursuant to PHL § 2[1][1] and 10 N.Y.C.R.R. Part 2);
ii. To ascertain sources of infection (pursuant to 10 N.Y.C.R.R. Part 2);
iii. To conduct investigations to assist in reducing morbidity and mortality (pursuant to 10 N.Y.C.R.R. Part 2);
iv. As authorized by PHL § 206(1)(d) to investigate the causes of disease, epidemics, the sources of mortality, and the effect of localities, employments and other conditions, upon the public health, and by PHL § 206(1)(j) for scientific studies and research which have for their purpose the reduction of morbidity and mortality and the improvement of the quality of medical care through the conduction of medical audits;
v. For purposes allowed by Article 21, including Article 21, Title 3 and 10 N.Y.C.R.R. Part 63 (HIV) and Article 21, Title 6 and 10 N.Y.C.R.R. Part 66 (immunizations);
vi. For purposes allowed by PHL § 2(1)(n), Article 23 and 10 N.Y.C.R.R. Part 23 (STD);
vii. For purposes allowed by PHL § 2401 and 10 N.Y.C.R.R. § 1.31 (cancer);
viii. For the activities of the Electronic Clinical Laboratory Reporting System (ECLRS), the Electronic Syndromic Surveillance System (ESSS),the Health Emergency Response Data System (HERDS), and the Statewide Planning and Research Cooperative System (SPARCS);
ix. For purposes allowed by PHL § 2004 and 10 N.Y.C.R.R. Part 62 (Alzheimer's);
x. For purposes allowed by PHL § 2819 (infection reporting);
xi. For quality improvement and quality assurance under PHL Article 29-D, Title 2, including quality improvement and quality assurance activities under PHL § 2998-e (office-based surgery);
xii. For purposes allowed under 10 N.Y.C.R.R. Part 22 (environmental diseases);
xiii. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. Part 67)

[1] New York law currently requires patient consent for the disclosure of information by health care providers for non-emergency treatment purposes. For general medical information, this consent may be explicit or implicit, written or oral, depending on the circumstances. The disclosure of certain types of sensitive health information may require a specific written consent. Under federal law (HIPAA), if the consent is not a HIPAA-compliant authorization, disclosures for health care operations are limited to the minimum necessary information to accomplish the intended purpose of the disclosure. Also, disclosures of information to another Participant for health care operations of the Participant that receives the information are only permitted if each entity either has or had a relationship with the patient, and the information pertains to such relationship.

xiv. For purposes allowed by 10 N.Y.C.R.R. Part 69 (including newborn disease screening, newborn hearing screening and early intervention);
xv. For purposes allowed under 10 N.Y.C.R.R. § 400.22 (Statewide Perinatal Data System);
xvi. For purposes allowed under 10 N.Y.C.R.R. § 405.29 (cardiac data); or
xvii. For any other public health activities authorized by law. "Law" means a federal, state or local constitution, statute, regulation, rule, common law, or other governmental action having the force and effect of law, including the Charter, Administrative Code and Rules of the City of New York.

C. HEALTHeLINK may Disclose Protected Health Information without Affirmative Consent to the New York State Office of Mental Health ("OMH") for public health purposes if HEALTHeLINK Discloses Protected Health Information to NYS DOH in its role as a Public Health Agency and OMH is authorized to obtain such information under applicable state and federal law. Permissible public health purposes for disclosure to OMH shall consist of investigations aimed at reducing morbidity and mortality, monitoring of disease trends, and responding to public health emergencies, consistent with the public health activities described in 3.2.2 (B)(i)-(xvii), above.

D. A patient's denial of consent for all Participants in HEALTHeLINK to Access the patient's Protected Health Information under Section 3.9.6 shall not prevent or otherwise restrict HEALTHeLINK from Disclosing to a Public Health Agency the patient's PHI through HEALTHeLINK for the purposes stated above.

E. HEALTHeLINK may Disclose the reports and information subject to 10 N.Y.C.R.R. § 63.4 (HIV clinical laboratory test results), for purposes of linkage to and retention in care, to Participants engaged in Care Management that have a clinical, diagnostic, or public health interest in the patient, to the extent permitted under 10 N.Y.C.R.R. § 63.4(c)(3). Participants engaged in Care Management with a clinical, diagnostic, or public health interest in a patient may include, but are not limited to, Provider Organizations or Practitioners with a Treatment relationship with a patient, Health Homes, and Payer Organizations providing Care Management to their enrollees. HEALTHeLINK shall work in consultation with the New York State Department of Health, AIDS Institute, prior to implementing any program under this provision.

3.2.3 Disclosures for Disaster Tracking

A. For the purpose of locating patients during an Emergency Event, HEALTHeLINK may Disclose to a Disaster Relief Agency the following information without Affirmative Consent:
   i. Patient name and other demographic information in a Record Locator Services and Other Comparable Directories;
   ii. Name of the facility or facilities from which the patient received care during the Emergency Event as well as dates of patient admission and/or discharge.

B. HEALTHeLINK may Disclose information under this section during an Emergency Event only.

C. Information Disclosed under this section shall not reveal the nature of the medical care received by the patient who is the subject of the Disclosure unless the Governor of New York, through Executive Order, temporarily suspends New York State health information confidentiality laws that would otherwise prohibit such Disclosure, as authorized under N.Y. Executive Law Section 29-a.

D. A patient's denial of consent for all Participants in HEALTHeLINK to Access or receive the patient's PHI under Section 3.9.6 shall not restrict HEALTHeLINK from Disclosing information to a Disaster Relief Agency as permitted by this section.

3.2.4 Emergency Disclosures of PHI When Treating a Patient with an Emergency Condition or "Break the Glass"

A. Affirmative Consent shall not be required for HEALTHeLINK to Disclose Protected Health Information to (i) a Practitioner, (ii) an Authorized User acting under the direction of a Practitioner; or (iii) an Emergency Medical Technician and these individuals may Break the Glass if the following conditions are met:
   i. Treatment may be provided to the patient without informed consent because, in the Practitioner's or Emergency Medical Technician's judgment,
      a) An emergency condition exists; **and**
      b) The patient is in immediate need of medical attention; **and**
      c) An attempt to secure consent would result in delay of treatment which would increase the risk to the patient's life or health.
   ii. The Practitioner or Emergency Medical Technician determines, in such individual's reasonable judgment, that information that may be held by or accessible via the SHIN-NY may be material to emergency treatment. The individual "Breaking the Glass" may do so in a facility, an ambulance, or another location, provided that such individual accesses Protected Health Information only after the determination in subsection (A)(i) has been made;
   iii. No denial of consent to Access or receive the patient's information is currently in effect with respect to the Participant with which the Practitioner, Authorized User acting under the direction of a Practitioner or Emergency Medical Technician is affiliated;
   iv. In the event that an Authorized User acting under the direction of Practitioner Breaks the Glass, such Authorized User must record the name of the Practitioner providing such direction;
   v. The Practitioner, Emergency Medical Technician or Authorized User acting under the direction of a Practitioner attests that all of the foregoing conditions have been satisfied, and HEALTHeLINK software maintains a record of this Disclosure.

B. Emergency Protected Health Information Access by an Authorized User acting under the direction of a Practitioner must be granted by a Practitioner on a case-by-case basis.

C. Participants must ensure that Disclosure of PHI via Break the Glass does not occur after the completion of the emergency treatment.

D. Sensitive Health Information is included in information that may be Disclosed through Break the Glass.

E. HEALTHeLINK shall promptly notify their Data Suppliers that are federally-assisted alcohol or drug abuse programs when PHI from the Data Supplier's records is Disclosed through HEALTHeLINK under this Section 3.2.4. This notice shall include (i) the name of the Participant that received the PHI; (ii) the name of the Authorized User within the Participant that received the PHI; (iii) the date and time of the Disclosure; and (iv) the nature of the emergency.

F. Upon a patient's discharge from a Participant's emergency room, if emergency Disclosure of PHI occurred during the emergency room visit, the Participant or HEALTHeLINK shall notify the patient of such incident and inform the patient of what clinical records were Disclosed at that encounter.
   i. The notice required by this Section must be provided within 10 days of the patient's discharge and may be provided by HEALTHeLINK on behalf of the Participant.

3.2.5 Converting Data

Affirmative Consent shall not be required for the conversion of paper patient medical records into electronic form or for the uploading of PHI from the records of a Data Supplier to HEALTHeLINK since (i) HEALTHeLINK is serving as the Data Supplier's Business Associate (as defined in 45 C.F.R. § 160.103) and (ii) HEALTHeLINK does not Disclose the information until Affirmative Consent is obtained, except as otherwise permitted in these Policies and Procedures.

3.2.6 HEALTHeLINK Access for Operations and Other Purposes

A. Affirmative Consent is not required for HEALTHeLINK or its contractors to Access or receive PHI to enable HEALTHeLINK to perform system maintenance, testing and troubleshooting and to provide similar operational and technical support.

B. Affirmative Consent is not required for HEALTHeLINK or its contractors to Access or receive PHI at the request of a Participant in order to assist the Participant in carrying out activities for which the Participant has obtained the patient's Affirmative Consent. Such Access or receipt must be consistent with the terms of the Business Associate Agreement entered into by the Participant and HEALTHeLINK.

C. Affirmative Consent is not required for HEALTHeLINK, government agencies or their contractors to Access or receive PHI for the purpose of evaluating and improving HEALTHeLINK operations.

3.2.7 De-Identified Data

Affirmative Consent is not required for HEALTHeLINK to Disclose De-Identified Data for specified uses as set forth in Section 3.6.

3.2.8 Organ Procurement Organization Access

HEALTHeLINK may Disclose Protected Health Information to an Organ Procurement Organization without Affirmative Consent solely for the purposes of facilitating organ, eye, or tissue donation and transplantation. A patient's denial of Affirmative Consent for all Participants in HEALTHeLINK to Access the patient's PHI under Section 3.9.3 will not prevent or otherwise restrict an Organ Procurement Organization from Accessing or receiving the patient's PHI for the purposes set forth in this Section 3.2.8.

3.2.9 Patient Care Alerts

A. A Patient Care Alert may be Transmitted to a Participant without Affirmative Consent provided that the recipient of such Patient Care Alert is a Participant that provides, or is responsible for providing, Treatment or Care Management to the patient. Such categories of Participants may include, but are not limited to, Practitioners, Accountable Care Organizations, Health Homes, Payer Organizations, PPS Centralized Entities, PPS Partners, and home health agencies who meet the requirements of the preceding sentence. If a patient or a patient's Personal Representative affirmatively denies consent to a Participant to Access the patient's information, then Patient Care Alerts shall not be Transmitted to such Participant.

B. Patient Care Alerts may be Transmitted from facilities subject to the New York Mental Hygiene Law without Affirmative Consent only if such alerts are sent to Payer Organizations, Health Homes, or other entities authorized by the New York State Office of Mental Health and the sending of such alerts otherwise complies with Mental Hygiene Law § 33.13(d).

C. Patient Care Alerts shall be Transmitted in an encrypted form that complies with U.S. Health and Human Services Department Guidance to Render Unsecured Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals.

3.2.10 Disclosures to Payer Organizations for Quality

Affirmative Consent shall not be required for HEALTHeLINK to Disclose Protected Health Information to a Payer Organization (including NYS DOH in regards to its operation of the New York State Medicaid program) or a Business Associate of a Payer Organization to the extent such Disclosure is necessary to (i) calculate performance of HEDIS or QARR measures; or (ii) in the case of disclosures to NYS DOH, determine payments to be made under the New York State Medicaid program or to evaluate services or initiatives, determine trends, or coordinate care under the Medicaid program, to the extent permitted by the HIPAA Privacy Rule.

3.2.11 Death Notifications

Affirmative Consent shall not be required for HEALTHeLINK to Disclose the death of a patient to a Participant that (a) was responsible for providing Treatment or Care Management to such patient prior to the patient's death; or (b) is a Payer Organization that provided health coverage to the patient immediately prior to the patient's death. A death notification may only include Demographic Information and the date and time of death. Cause of death and information on the patient's diagnoses, health conditions, and treatments, as well as location of death, shall not be included in the death notification absent Affirmative Consent.

3.2.12 Disclosures to Death Investigators

Affirmative Consent shall not be required for HEALTHeLINK to Disclose Protected Health Information to a Participant for the purposes of determining the cause of a patient's death provided that all of the following are met:

i. The individual accessing or receiving the Protected Health Information is a licensed physician or nurse practitioner whose professional responsibilities include determining the cause of death of a patient, or an individual acting under the supervision of such Practitioner. Such individuals may include Medical Examiners and Coroners who are licensed as physicians or nurse practitioners, or an individual acting under the supervision of such a Medical Examiner or Coroner;
ii. HEALTHeLINK and the Participant abide by the minimum necessary standard set forth at P03 § 3.4;
iii. Protected Health Information originating from a facility subject to the New York Mental Hygiene Law is Disclosed only if the facility has requested that an investigation be conducted into the death of a patient and the recipient is a Medical Examiner or Coroner that is licensed as physician or nurse practitioner.

3.2.13 Telehealth

A. General. Affirmative Consent shall not be required for HEALTHeLINK to disclose a patient's Protected Health Information to a Participant that provides telehealth services to such patient if:
   i. The Participant has asked the patient if the Participant may Access or receive the patient's Protected Health Information, and the patient has verbally consented to such request;
   ii. The Participant uses the Protected Health Information only for Level 1 purposes;
   iii. The Participant keeps a record of the patient having provided verbal consent, which may take the form of a notation in the electronic record of such consent, an audio recording of the consent, or another appropriate means of recording consent;
   iv. The Participant does not Access or receive any Protected Health Information subject to 42 C.F.R. Part 2 or Mental Hygiene Law § 33.13 unless the patient has provided consent in written or electronic form and a signature that is recognized by the Electronic Signatures and Records Act, including an audio signature recording to the extent recognized under that act; and
   v. The Participant Accesses or receives the patient's Protected Health Information only during the time period specified in subsection B.

B. Duration of telehealth verbal consent. The patient's verbal consent shall remain in effect for the duration of the telehealth encounter, but no longer than 72 hours.

C. Applicability to electronic consents. If a Participant obtains the patient's electronic signature, including a recording of oral consent, that is recognized by the Electronic Signatures and Records Act, then such consent shall be governed by P04 Section 3.9.5 and shall not be subject to the requirements of this section.

3.3 Form of Patient Consent

Consents shall be obtained through an Approved Consent. HEALTHeLINK may approve an alternative to a Level 1 Consent or a Level 2 Consent if the Alternative Consent includes the information specified in this section. HEALTHeLINK is responsible for ensuring that any approved Alternative Consents comply with applicable federal, state and local laws and regulations. If an Alternative Consent is to be used as a basis for exchanging information subject to 42 C.F.R. Part 2, HEALTHeLINK shall ensure that such form meets the requirements of 42 C.F.R. Part 2.

3.3.1 Level 1 Uses

Affirmative Consent to Access or receive information via the SHIN-NY for Level 1 Uses shall be obtained using a Level 1 Consent or an Alternative Consent approved by HEALTHeLINK under this section, which shall include the following information:

A. A description of the information which the Participant may Access or receive, including specific reference to HIV, mental health, alcohol and substance use, reproductive health, sexually-transmitted disease, and genetic testing information, if such categories of information may be Disclosed to the recipient;

B. The Participant's intended uses for the information. A general description, such as "for treatment, care management or quality improvement," shall meet this requirement;

C. The name(s) or description of both the source(s) and potential recipient(s) of the patient's information. A general description, such as "information may be exchanged among providers that provide me with treatment," shall meet this requirement; and

D. The signature of the patient or the patient's Personal Representative. If the consent language required under subsections (A), (B), and (C) above is incorporated into another document such as a health insurance enrollment form in accordance with Section 3.3.5, the signature need not appear on the same page as the language required under subsections (A), (B), and (C) above.

3.3.2 Level 2 Uses

Consent to Access or receive information via the SHIN-NY for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an Alternative Consent approved by HEALTHeLINK under this Section 3.3.2, which shall include (i) the information required pursuant to Section 3.3.1 and (ii) the following information:

A. The specific purpose for which information is being Disclosed;

B. Whether HEALTHeLINK and/or its Participants will benefit financially as a result of the Disclosure of the patient's information;

C. The date or event upon which the patient's consent expires;

D. Acknowledgement that the payers may not condition health plan enrollment and receipt of benefits on the patient's decision to grant or withhold consent;

E. A list of or reference to all Data Suppliers at the time of the patient's consent, as well as an acknowledgement that Data Suppliers may change over time and instructions for patients to access an up-to-date list of Data Suppliers through HEALTHeLINK's website or other means; the consent form shall also identify whether HEALTHeLINK is party to data sharing agreements with other QEs and, if so, provide instructions for patients to access an up-to-date list of Data Suppliers from HEALTHeLINK's website or by other means;

F. Acknowledgement of the patient's right to revoke consent and assurance that treatment will not be affected as a result;

G. Whether and to what extent information is subject to re-disclosure; and

H. The date of execution of the consent.

3.3.3 Requirements for Separate Consents

A. Consent for Level 1 Uses and consent for Level 2 Uses may not be combined.

B. Consent for different Level 2 Uses may not be combined.

C. Consent for a Level 1 or Level 2 Use shall not be combined with any other document except with the approval of HEALTHeLINK. If HEALTHeLINK agrees to allow an Alternative Consent that is combined with a health insurance enrollment form, such Alternative Consent shall expire no later than the date on which the patient's health insurance enrollment terminates.

3.3.4 Education Requirement for Level 2 Consents Relating to Marketing

When HEALTHeLINK or a Participant obtains a Level 2 Consent to Access or receive PHI via the SHIN-NY for the purpose of Marketing, HEALTHeLINK or its Participant must provide the patient with information about the nature of such Marketing.

3.3.5 Naming of QEs and Recognition of Consents

A. HEATHeLINK shall permit the Disclosure of Protected Health Information based on an individual's execution of an affirmative consent.

B. HEALTHeLINK may permit the Disclosure of Protected Health Information based on a Level 1 Alternative Consent executed only if:
   i. The Alternative Consent has been approved and issued by a New York State agency;
   ii. The Alternative Consent was obtained by a hospital Participant, or a Provider Organization Participant that uses such Alternative Consent in multiple states, and such Participant used such Alternative Consent prior to the Statewide Consent Date;
   iii. The Alternative Consent permits Disclosures to a Participant that is not included among the potential recipients of Protected Health Information under the SHIN-NY Consent; or
   iv. The Alternative Consent was obtained by an individual or entity that is not a Participant in any QE.

   Nothing herein limits the ability of HEALTHeLINK to recognize a Level 1 Alternative Consent or a Level 2 Alternative Consents executed either before or after the Consent Implementation Date.

C. An Affirmative Consent form is not required to include the name of a QE.

D. Up until a date to be determined by NYS DOH, HEALTHeLINK may continue to use an Affirmative Consent form on which the name of such QE appears.

E. In the case where an Affirmative Consent form does not include the name of HEALTHeLINK, HEALTHeLINK shall Disclose to a Participant a patient's Protected Health Information even if HEALTHeLINK's name does not appear on the Affirmative Consent form so long as:
   i. the patient signed the Affirmative Consent form;
   ii. the Affirmative Consent form names the Participant or indicates that Protected Health Information may be disclosed to a class of Participants (for example, treating providers) that includes the Participant in accordance with Section 3.3.1(C); and
   iii. the Disclosure otherwise complies with these Policies and Procedures.

3.4 Sensitive Health Information

3.4.1 General

An Affirmative Consent may authorize Participant(s) listed in the consent to Access or receive all the patient's PHI referenced in the consent, including Sensitive Health Information.

3.4.2 Withholding Sensitive Health Information

HEALTHeLINK and Participants may, but shall not be required to, subject Sensitive Health Information to certain additional requirements, including but not limited to providing patients the option to withhold certain pieces of Sensitive Health Information from Disclosure. In the event that HEALTHeLINK or a Participant has provided the patient the option to withhold certain pieces of Sensitive Health Information from

Disclosure, and the patient has exercised that option, the patient's record may, but is not required to, carry an alert indicating that data has been withheld from the record.

3.4.3 Re-disclosure Warning

A. HEALTHeLINK will place a warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of records of federally-assisted alcohol or drug abuse programs regulated under 42 C.F.R. Part 2 that contains the language required by 42 C.F.R. § 2.32. HEALTHeLINK may satisfy this requirement by placing such a re-disclosure warning on all records that are made accessible through HEALTHeLINK.

B. HEALTHeLINK will include a warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of HIV/AIDS information protected under Article 27-F of N.Y. Public Health Law that contains the language required by Article 27-F (see Public Health Law § 2782[5]). Such a re-disclosure warning will be placed on the same screen as the re-disclosure warning required at Section 3.4.3(A) or on the log-in screen that Authorized Users must view before logging into HEALTHeLINK.

C. HEALTHeLINK will include a warning statement that is viewed by Authorized Users whenever they are obtaining Access to or receiving Transmittals of records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities that contains language notifying the Authorized User that such records may not be re-disclosed except as permitted by the New York Mental Hygiene Law. Such a re-disclosure warning will be placed on the same screen as the re-disclosure warning required at Section 3.4.3(A) or on the log-in screen that Authorized Users must view before logging into HEALTHeLINK.

3.4.4 Re-disclosure of Sensitive Health Information by Participants

Prior to re-disclosing Sensitive Health Information, Participants must implement systems to identify and denote Sensitive Health Information in order to ensure compliance with applicable state and federal laws and regulations governing re-disclosure of such information, including, but not limited to, those applicable to HIV/AIDS, alcohol and substance use information, and records of facilities licensed or operated by the New York State Office of Mental Health or the New York State Office for People With Developmental Disabilities.

3.5 Special Provisions Relating to Minors

A. A Participant may Access or receive PHI about minors – other than Minor Consent Information – based on an Affirmative Consent executed by the minor's Personal Representative. On the minor individual's 18th birthday, when the minor becomes an adult, Participant access to the PHI will no longer be available until the individual executes his/her own Affirmative Consent.

B. A Participant may Access or receive Minor Consent Information based on an Affirmative Consent executed by the minor's Personal Representative unless federal or state law or regulation requires the minor's authorization for such Disclosure, in which case a Participant may not Access or receive such information without the minor's Affirmative Consent.

C. 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.

D. Notwithstanding Section 3.5.B above, HEALTHeLINK and Participants may not Disclose Minor Consent Information to the minor's Personal Representative without the minor's written consent. HEALTHeLINK must provide or arrange for training for their Participants on compliance with this Section 3.5.D.

3.6 De-Identified Data

A. HEALTHeLINK may Disclose De-Identified Data without Affirmative Consent if HEALTHeLINK enters into a data use agreement with the recipient in accordance with Section 3.6.D, unless HEALTHeLINK determines that (a) such De-Identified Data is to be used to assist in Marketing activities that would not comply with the HIPAA Privacy Rule, or (b) the proposed use of the De-Identified Data is not in keeping with the mission of the SHIN-NY as described in 10 N.Y.C.R.R. § 300.1. Notwithstanding the foregoing, a data use agreement shall not be required if HEALTHeLINK solely is Transmitting to a third party that is designing a clinical trial or other clinical research study a count of the number of patients who appear to meet the inclusion and/or exclusion criteria being considered for such clinical trial or study, so long as there is no reasonable basis to believe that the count, when combined with the qualifying criteria, can be used to identify an individual.

B. Affirmative Consent shall not be required for HEALTHeLINK to Transmit to a third party that is designing a clinical trial or other clinical research study a count of the number of patients who appear to meet the inclusion and/or exclusion criteria being considered for such clinical trial or study, so long as there is no reasonable basis to believe that the count, when combined with the qualifying criteria, can be used to

identify an individual.

C. HEALTHeLINK shall, or shall require Participants to, comply with standards for the de-identification of data set forth in 45 C.F.R. § 164.514.

D. HEALTHeLINK shall ensure that a data use agreement required under this Section 3.6:
   1. Establishes the permitted uses of the De-Identified Data by the recipient and prohibits the recipient or any third parties from using the De-Identified Data for any purposes other than the permitted uses, unless otherwise required by law;
   2. Prohibits the recipient from re-identifying or attempting to re-identify the De-Identified Data;
   3. Provides HEALTHeLINK, or a Participant who holds Protected Health Information that was used in whole or in part to create the De-Identified Data set, with a right to audit the practices of the recipient regarding ensuring the data is not re-identified;
   4. Requires the recipient to report to HEALTHeLINK if the recipient has knowledge that the De-Identified Data has been re-identified or if there have been any other violations of the data use agreement;
   5. Mandates that the recipient may not disclose the De-Identified data to any third party unless the agreement explicitly permits such a Disclosure and the third party also agrees in writing to follow the restrictions set forth in this Section 3.6.D.

E. Any Disclosures of De-Identified Data shall comply with any applicable terms in the Business Associate Agreement between HEALTHeLINK and the Data Suppliers that are the source of the De-Identified Data.

3.7 Research

3.7.1 Research Involving De-Identified Data

Affirmative Consent shall not be required for HEALTHeLINK to Disclose De-Identified Data for purposes of Research (See HEALTHeLINK Policy P13, *Release of Data for Research*).

3.7.2 Research Involving a Limited Data Set

Affirmative Consent shall not be required for HEALTHeLINK to Disclose a Limited Data Set for purposes of Research (See HEALTHeLINK Policy P13, *Release of Data for Research*).

3.7.3 Research Involving Protected Health Information

A. Use of Protected Health Information for Patient Recruitment for Research. Affirmative Consent shall not be required for HEALTHeLINK to review Protected Health Information on behalf of a researcher to determine which individuals may qualify for a Research study. In addition, Affirmative Consent shall not be required for HEALTHeLINK to Disclose the name and other identifying information of an

individual who may qualify for a Research study to a Participant that has a treating relationship with such individual so that the Participant may contact the individual to determine his or her willingness to participate in such study, provided that all of the following requirements are met:

i. an Institutional Review Board has approved of such Disclosure;
ii. the HEALTHeLINK Research Committee has approved of such Disclosure;
iii. the Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for the Disclosure of their Protected Health Information for purposes of Research; and
iv. the Disclosure does not include any mental health clinical information governed by Section 33.13 of the Mental Hygiene Law, unless the recipient of the Disclosure is a facility as defined in the Mental Hygiene Law.

B. Use of Protected Health Information for Retrospective Research. Affirmative Consent shall not be required for HEALTHeLINK to Disclose Protected Health Information to a researcher conducting Retrospective Research if:

i. an Institutional Review Board has approved of such Disclosure;
ii. the HEALTHeLINK Research Committee has approved of such Disclosure; and
iii. the Data Supplier(s) that are the source of the Protected Health Information have agreed to allow for Disclosures of their Protected Health Information for purposes of Research.

3.8 Transmittals to Non-Participants

3.8.1 Transmittals to Business Associates

In any case where a Participant has a right to Access or receive Protected Health Information under these Policies and Procedures, the Participant may request that HEALTHeLINK Transmit such information to a Business Associate of the Participant, and HEALTHeLINK may comply with such request, so long as the conditions set forth in subsections (A) through (F) are met. Nothing in this section shall allow HEALTHeLINK to treat a Business Associate as a Participant unless the Business Associate otherwise meets the definition of a Participant.

A. The Participant and the Business Associate have entered into a Business Associate Agreement under which the Business Associate agrees to protect the confidentiality of the Protected Health Information being Transmitted to the Business Associate.

B. The Participant represents to HEALTHeLINK in writing that its Business Associate is seeking the Participant's information in accordance with the terms of the Business Associate Agreement between the two parties.

C. The Business Associate and the Participant agree to provide a copy of their Business Associate Agreement to HEALTHeLINK upon request.

D. HEALTHeLINK reasonably believes that the Transmittal is in accordance with state

and federal law and the terms of the Business Associate Agreement.

E. HEALTHeLINK either enters into an agreement with the Business Associate requiring the Business Associate to comply with these Policies and Procedures or the Participation Agreement between the Participant and HEALTHeLINK holds the Participant responsible for the actions of the Business Associate.

F. The Business Associate agrees not to further Disclose the Protected Health Information except where these Policies and Procedures allows for such Disclosure.

3.8.2 Transmittals to Other Non-Participants

HEALTHeLINK may Transmit a patient's Protected Health Information from HEALTHeLINK (or any other QE that has agreed to such Transmittal) to a health care provider or other entity that is not a Participant or a Business Associate of a Participant only if all of the following conditions are met:

A. The patient has granted Affirmative Consent for the Transmittal, provided that Affirmative Consent shall not be required if the Transmittal is provided to a public health authority, as defined at 45. C.F.R. § 164.501. The Affirmative Consent shall meet all the requirements of a Level 1 Consent or Alternative Consent, provided that if the recipient is a life or disability insurer that is not a governmental entity then the form shall have been approved by the applicable department(s) of insurance. For the avoidance of doubt, (i) a Transmittal may be made to a non-Participant on the basis of any Affirmative Consent that applies to such non-Participant, and (ii) none of the exceptions to the Affirmative Consent requirement set forth in Section 3.2 other than Section 3.2.2 shall apply to Transmittals under this section.

B. The recipient of the Transmittal is not a Participant and is one of the following:
   i. A Covered Entity that does not operate in New York State, or a Business Associate of such Covered Entity;
   ii. A Health Information Exchange Organization that does not operate in New York State;
   iii. A public health authority, as defined at 45. C.F.R. § 164.501, that is not located in New York State;
   iv. A health care facility that is operated by the United States Department of Veteran Affairs or the United States Department of Defense;
   v. A disability insurer or life insurer that has (i) issued a disability or life insurance policy to the patient; (ii) received an application from the patient for such a policy; or (iii) received a claim for benefits from the patient.

C. HEALTHeLINK takes reasonable measures, or requires the recipient to take reasonable measures, to authenticate that the person who has granted the Affirmative Consent is the patient or the patient's Personal Representative.

D. HEALTHeLINK takes reasonable measures to authenticate that the recipient is the same individual or entity authorized in the patient's Affirmative Consent to receive the patient's Protected Health Information.

E. HEALTHeLINK enters into an agreement with the recipient that requires the recipient to:
   i. Obtain the Affirmative Consent of the patient that is the subject of the Protected Health Information, or ensure that another entity or organization has obtained such consent;
   ii. Abide by the terms of patients' Affirmative Consents and applicable law (e.g., health privacy laws for a Covered Entity, insurance laws for life and disability insurers), including any restrictions on re-disclosure;
   iii. Notify HEALTHeLINK in writing and in the most expedient time possible if the recipient becomes aware of any actual or suspected Breach of Unsecured Protected Health Information;
   iv. Represent that the recipient is not excluded, debarred, or otherwise ineligible from participating in any federal health care programs; and
   v. Not engage in the sale of the Protected Health Information provided to the recipient, or the use or disclosure of such Protected Health Information for marketing purposes in a manner that would be prohibited by the HIPAA Privacy Rule if such rule were applicable to the recipient, unless the recipient obtains the patient's authorization to do so in a form that complies with the HIPAA Privacy Rule.

Nothing in this section shall be construed to prohibit a patient from Disclosing any of the patient's Protected Health Information the patient has received from HEALTHeLINK under P15 Sections 3.2 or 3.3 to an individual or entity of the patient's choice.

3.9 Other Policies and Procedures Related to Consent

3.9.1 Consent Process

Unless an exception applies (see Section 3.2), a Participant will be unable to Access a patient's PHI 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.

3.9.2 Affiliated Practitioners

An Affirmative Consent that applies to a Participant shall apply to an Affiliated Practitioner of the Participant provided that (i) such Affiliated Practitioner is providing health care services to the patient at the Participant's facilities; (ii) such Affiliated Practitioner is providing health care services to the patient in such Affiliated

Practitioner's capacity as an employee or contractor of the Participant or; (iii) such Affiliated Practitioner is providing health care services to the patient in the course of a cross-coverage or on-call arrangement with the Participant or one of its Affiliated Practitioners.

3.9.3 Consents Covering Multiple Participants

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

A. The organization offering the consent to the patient must inform the patient that the patient has an option to sign a consent form that applies only to a single Participant. The organization may provide such information verbally, in the text of the consent form itself, or otherwise.

B. If the multi-Participant consent allows a Participant to Access or receive any patient records that are subject to the rules governing federally-assisted alcohol or drug abuse programs at 42 C.F.R. Part 2, the consent form must comply with all relevant restriction in 42 C.F.R. Part 2.

C. An Affirmative Consent may apply to Participants who join HEALTHeLINK after the date the patient signs the consent form, provided that:
   1. HEALTHeLINK maintains a list of its Participants on its website and updates that list within 24 hours of when a new Participant is granted Access to patient information via the SHIN-NY;
   2. HEALTHeLINK mails a hard copy list of its Participants without charge to any patient who requests that list within 5 business days of the request;
   3. the consent form provides patients with information on how they may obtain a list of Participants; and
   4. Access to any patient records that are subject to the rules governing federally-assisted alcohol or drug abuse programs complies with 42 C.F.R. Part 2.

3.9.4 Consent Obtained by HEALTHeLINK

HEALTHeLINK may obtain consents on behalf of their Participants, provided such consents meet all of the requirements set forth in this Section 3.

3.9.5 Electronic Signatures

Affirmative Consent may be obtained electronically provided that there is an electronic signature that meets the requirements of the federal ESIGN statute, 15 U.S.C. § 7001 et seq., or any other applicable state or federal laws or regulations. See Electronic Signatures and Records Act (State Technology Law Article III, 9 N.Y.C.R.R. Part 540, New York State Office of Information Technology Services ESRA Guidelines NYS-G04-001).

3.9.6 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. "Yes, Except Specific Participant(s)"; or
2. "Yes, Only Specific Participant(s)"; or
3. "No, Except in an Emergency"; or
4. "No, Even in an Emergency".

B. A patient's decision not to sign a consent form will not be construed as a "denial of consent" for emergency Access under Section 3.2.4(A)(iii). If a patient chooses to give consent for Participants to Access his/her electronic health information with the exception of certain identified Participants, the identified Participants will not have Access to the patient's PHI except in an emergency.

C. Providers/Payers must not condition treatment/coverage on the patient's willingness to consent to the Access of their PHI through HEALTHeLINK.

3.9.7 Durability

An Affirmative Consent for Level 1 Uses does not have to be time-limited. An Affirmative Consent for Level 2 Uses shall be time-limited and shall expire no more than two years after the date such Level 2 Consent is executed, except to the extent a longer duration is required to complete a Research protocol.

3.9.8 Withdrawal of Consent

Patients may withdraw their consent at any time upon written request. If a patient withdraws consent, data that has been Accessed by a Participant up to the time of withdrawal will remain as part of the Participant's records.

3.9.9 Notification of HEALTHeLINK's Data Suppliers

Patients will be provided a reference to all HEALTHeLINK Data Suppliers through its website at the time the Participant obtains the patient's Affirmative Consent. A complete and accurate updated list of Data Suppliers will be maintained on the HEALTHeLINK website at all times.

3.9.10 Compliance with Business Associate Agreements with Data Suppliers

HEALTHeLINK shall execute a Business Associate Agreement with each Data Supplier that is a Covered Entity. HEALTHeLINK shall not use or Disclose Protected Health Information in any manner that violates HEALTHeLINK's Business Associate Agreements.

3.9.11 Disclosure to HEALTHeLINK Vendors

HEALTHeLINK, acting under the authority of a Business Associate Agreement with its Participants, may Disclose Protected Health Information to vendors that assist in carrying out HEALTHeLINK's authorized activities provided (i) HEALTHeLINK requires the vendors to protect the confidentiality of the Protected Health Information in accordance with HEALTHeLINK's Business Associate Agreements with its Participants and (ii) the vendor does not make such information available to a Participant that has

not obtained Affirmative Consent.

3.9.12 Compliance with Existing Law

All Access to Protected Health Information via the SHIN-NY governed by HEALTHeLINK shall be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exist or that other conditions be met prior to Accessing or receiving Protected Health Information for a particular purpose, Participants shall ensure that they have obtained the required documentation or met the requisite conditions and shall provide evidence of such as applicable.

3.9.13 Compliance with Requests for Restrictions on Disclosures to a Payer Organization

Provider Participants must ensure that a Payer Organization does not Access or receive PHI through HEALTHeLINK if a patient has requested, in accordance with the HIPAA Privacy Rule and HITECH, that the Provider Organization creating such information not Disclose it to the Payer Organization.

A. Upon a Provider Organization's receipt of a patient's request that PHI created by the Provider Organization not be Disclosed to a Payer Organization, the Provider Organization will obtain the patient's written revocation of access previously granted to such Payer Organization by having the patient execute a new Affirmative Consent that excludes the Payer Organization (i.e., "Yes, Except Specific Participant(s)"). Such revocation remains in effect permanently unless and until the patient's request is withdrawn; and

B. Upon subsequent receipt of a new Affirmative Consent covering a Payer Organization that was previously revoked, HEALTHeLINK will notify the patient in writing that his or her provision of the Affirmative Consent will revoke any prior request for a restriction on the Disclosure of PHI by any Provider Organization to the Payer Organization. The Affirmative Consent is rejected if the patient indicates he or she does not agree to the revocation of his or her prior request.

3.9.14 Development of Policies Governing Disclosures to Government Agencies for Health Oversight

HEALTHeLINK shall adopt policies governing HEALTHeLINK's response to requests from government agencies for Access to or receipt of Protected Health Information for health oversight purposes, such as Medicaid audits, professional licensing reviews, and fraud and abuse investigations. Such policies shall address whether HEALTHeLINK will Disclose information without Affirmative Consent in instances where Disclosure is permitted but not required by law, and whether HEALTHeLINK will notify its Participants of such requests. This section does not cover Disclosure of Protected Health Information to Public Health Agencies under Section 3.2.2.

3.9.15 Indication of Presence of Medical Order for Life Sustaining Treatment ("MOLST") or Other Advance Directive

HEALTHeLINK may note whether a patient has signed a MOLST or other advance directive in a Record Locator Service or Other Comparable Directory without Affirmative Consent.

3.9.16 Consent for Access by ACOs and IPAs

An Affirmative Consent authorizing Access by an Accountable Care Organization (ACO) or Independent Practice Association (IPA) shall cover only the ACO or IPA entity itself and not the health care providers participating in the ACO or IPA.

3.10 Patient Consent Transition Rules

3.10.1 Use of Approved Consents

Except as set forth in Section 3.10.2, 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 governed by HEALTHeLINK on or after the Consent Implementation Date.

3.10.2 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.

3.10.3 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.

3.11 Waivers During a Public Health Emergency

A. NYS DOH may waive provisions in this Section 3 and other provisions of these Policies and Procedures during a public health emergency under Section 319 of the Public Health Services Act if (i) the waiver assists HEALTHeLINK and/or their Participants in their response to the public health emergency; (ii) NYS DOH provides public notice of such waiver; and (iii) the waiver complies with applicable state and federal law.

B. HEALTHeLINK will conduct an internal management review for adopting and implementing some or all of the waiver terms set forth in subsection A to HEALTHeLINK operations.

4 References

- 45 C.F.R. Part 164.

- 42 C.F.R. Part 2.
- 42 C.F.R. § 489.24.
- 42 C.F.R. § 486.
- HEALTHeLINK Policy P13, *Release of Population Data.*
- HEALTHeLINK Policy P15, *Patient Engagement and Access.*
- New York State Public Health Law Article 27-F.
- New York State Public Health Law § 2504.
- New York State Mental Hygiene Law § 33.13.
- New York State Civil Rights Law § 79-1.
- New York State Public Health Law § 17.
- 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)* § 1.

Patient Request for Restrictions or Confidential Communications

Privacy Policy and Procedure
Policy No. P05

1 Policy Statement

HEALTHeLINK 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 PHI. 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 PHI 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 PHI.

3.1 Reporting Requirements

A. HEALTHeLINK personnel and HEALTHeLINK Participants, who discover, believe, or suspect that unsecured PHI 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 PHI has been, or is reasonably believed to have been, Accessed, Transmitted, acquired, Used 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 PHI 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, Exhibit A.*
- 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)* § 7.
- Restatement I of the Data Use and Reciprocal Support Agreement (DURSA). Version Date: May 3, 2011

Privacy Complaints/Concerns

Privacy Policy and Procedure
Policy No. P07

1 Policy Statement

Each HEALTHeLINK 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 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 PHI 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. HEALTHeLINK and/or Participants and Public Health Agencies shall inform all Authorized Users about HEALTHeLINK's sanctions policies.

B. Any breach of patient PHI reported by HEALTHeLINK to a HEALTHeLINK 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.

C. 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.

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

E. HEALTHeLINK 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.

F. 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.

G. Sanctions will include, but do not necessarily have to be limited to, the following:
   1. requiring an Authorized User to undergo additional training with respect to participation in HEALTHeLINK;
   2. temporarily restricting an Authorized User's Access to HEALTHeLINK;
   3. terminating the Access of an Authorized User to HEALTHeLINK;
   4. suspending or terminating a Participant's participation in HEALTHeLINK; and
   5. The assessment of fines or other monetary penalties.

H. Any Sanction involving the termination of a Participation Agreement resulting from a failure to comply with HEALTHeLINK Policies and Procedures, must first be presented to the HEALTHeLINK Operating Committee for review and approval.

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)* § 9.

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 PHI 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 HEALTHeLINK Participant will be trained on all HEALTHeLINK Privacy and Security Policies and Procedures, including but not limited to those related to Authorized User Access, Use 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.

C. Each Authorized User will be required to undergo continuing and/or refresh training on an annual basis as a condition of maintaining authorization to Access patient information via HEALTHeLINK. Records of such training will be maintained and available for audit by the training organization for at least 6 years.

4 References

- 42 C.F.R. § 164.530.
- 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, HEALTHeLINK Participants must make reasonable efforts to limit or determine Access as needed and use of PHI 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 PHI through the HEALTHeLINK System.

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

C. Each Participant must notify HEALTHeLINK of the termination of an Authorized User's employment or affiliation with the Participant immediately or as promptly as reasonably practicable but in any event within 1 business day of termination.

D. Each Participant must notify HEALTHeLINK as promptly as reasonably practicable following a change in an Authorized User's role that renders the Authorized User's continued Access to HEALTHeLINK inappropriate.

E. 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*).

F. HEALTHeLINK will terminate Access in the following situations:
   1. Immediately or as promptly as reasonably practicable but in any event within 1 business day of termination of the Participant's Participation Agreement with HEALTHeLINK;
   2. Immediately or as promptly as reasonably practicable but in any event within 1 business day of notification of termination of an Authorized User's employment or affiliation with the Participant;
   3. Immediately or as promptly as reasonably practicable but in any event within 1 business day of notification of a change in an Authorized User's role with the Participant.

4 References

- 45 C.F.R. § 164.530.
- 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

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 PHI 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 P04, *Patient Consent.*
- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies and Procedures.*
- 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).

1 Policy Statement

HEALTHeLINK will provide educational material for patients and/or their Personal Representatives with respect to the consent process and the terms and conditions upon which their Protected Health Information can be shared with Authorized Users, including conforming to any patient education program standards developed through the SHIN-NY Statewide Collaboration Process (SCP), and informing the patient and/or his or her Personal Representative of the benefits and risks of providing an Affirmative Consent for his or her Protected Health Information to be shared through HEALTHeLINK.

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 Patient Education and Resources

A. HEALTHeLINK shall be required to educate patients and/or their Personal Representatives with respect to the consent process and the terms and conditions upon which their Protected Health Information can be shared with Authorized Users, including conforming to any patient education program standards developed through the SCP, and informing the patient and/or his or her Personal Representative of the benefits and risks of providing an Affirmative Consent for his or her Protected Health Information to be shared through HEALTHeLINK.

B. To facilitate informed consent and to ensure that patients know where information about them is being generated, HEALTHeLINK shall provide, or shall require their Participants to provide, patients or their Personal Representatives, as appropriate, with
   i. notice -in a manner easily understood by patients -that their Protected Health Information is being uploaded to HEALTHeLINK;
   ii. a list of or reference to all Data Suppliers (consistent with P04 Section 3.9.9);
   iii. information about how to contact Data Suppliers;
   iv. a description of how patients may deny consent for all HEALTHeLINK Participants to Access their Protected Health Information through HEALTHeLINK in accordance with P04 Section 3.9.6;
   v. information about how patients can submit requests to correct erroneous data;
   vi. information about how patients can submit requests for Audit Logs, in compliance with P16 Section 3.4; and
   vii. information about the security practices of the SHIN-NY, including the right of patients to be notified of certain breaches and how data sent outside the SHIN-NY upon a patient request may no longer be subject to HIPAA.

C. The materials referenced in Sections A and B shall be made available on HEALTHeLINK's website. In addition, HEALTHeLINK shall make available appropriate materials to their Participants, in either written or electronic form, so such Participants can provide information to their patients about the SHIN-NY and the consent process.

D. As required in P16 Section 3.4, HEALTHeLINK shall, or shall require their Participants to, provide patients with information about how their Protected Health Information was Disclosed by HEALTHeLINK.

3.2 Patient Access to SHIN-NY Data

HEALTHeLINK shall facilitate the access of patients and their Personal Representatives to patients Protected Health Information maintained by HEALTHeLINK through one of the mechanisms set forth in Sections 3.2.1, 3.2.2, 3.2.3, or 3.2.4. Each patient shall have the right to indicate the scope of the Protected Health Information and which of the mechanisms he or she prefers to utilize to obtain access to his or her information, and HEALTHeLINK shall abide by the patient's request unless applicable law (including the patient access provisions under the HIPAA Privacy Rule or the requirements for the "content and manner" exception or another exception to the Information Blocking Rules) permit or require HEALTHeLINK to limit the scope and form of the Protected Health Information provided to the patient. HEALTHeLINK shall only facilitate such access after confirming the identity of the patient or the patient's Personal Representative through adequate identity proofing procedures.

1. HEALTHeLINK's own web-based portal or Participants' web-based portals;
2. A web-based portal established by or maintained by a third party on behalf of a patient, including a Patient App, provided the requirements related to disclosures to third parties set forth in Section 3.3 are met;
3. A paper or electronic copy of information maintained about the patient by HEALTHeLINK;
4. Any other mechanism requested by the patient (provided that HEALTHeLINK need not provide the Protected Health Information via the requested mechanism if applicable law, including the Information Blocking Rules, permit HEALTHeLINK to use an alternative mechanism).

3.3 Patient Direction to Patient Apps and Other Third Parties

HEALTHeLINK shall have the means of receiving and responding to requests from patients and Personal Representatives to Disclose such patients' Protected Health Information to third parties, including but not limited to Patient Apps, friends and family of patients, and legal representatives of patients. HEALTHeLINK shall abide by the following requirements in response to such requests:

1. HEALTHeLINK shall Disclose the patient's Protected Health Information in response to the patient's or Personal Representative's request only after confirming the identity of the patient or the patient's Personal Representative that submitted the request through adequate identity proofing procedures;

2. HEALTHeLINK shall decline to fulfill the request, or fulfill the request only in part, only if applicable law permits HEALTHeLINK to do so or if the patient or Personal Representative withdraws the request. Applicable law may include, but is not limited to, the patient access provisions under the HIPAA Privacy Rule, the Information Blocking Rules, or state laws that limit disclosures to Patient Apps;
3. If the third party to receive the patient's Protected Health Information is a Patient App, HEALTHeLINK shall educate the patient or the patient's Personal Representative about the risks of Disclosure to such Patient App prior to making the Disclosure. Such education shall be based on analyses or recommendations of neutral third parties that evaluate Patient Apps, such as the CARIN Alliance, and comply with any guidance issued by NYS DOH and/or the State Designated Entity regarding the nature of such education. If the patient or the patient's Personal Representative does not withdraw the request in response to such information, HEALTHeLINK shall comply with the request unless applicable law permits HEALTHeLINK to decline to fulfill the request in whole or in part;
4. HEALTHeLINK may require a patient, a patient's Personal Representative, or a third party to pay a fee prior to Disclosing Protected Health Information to a third party only if applicable law, including the patient access provisions under the HIPAA Privacy Rule and the Information Blocking Rule, permit such fee to be charged. For example, if HEALTHeLINK establishes a portal or other internet-based method that allows a patient, a patient's Personal Representative, or third party to Access Protected Health Information, HEALTHeLINK may not charge a fee for use of that system if no manual effort was required by HEALTHeLINK to fulfill the request.

3.4 Information About Minors

HEALTHeLINK will not provide Personal Representatives of minors between the ages 10 and 17 with access to any of the minor's Protected Health Information.

3.5 Patient Input and Participation

HEALTHeLINK shall develop a plan and process for assuring meaningful patient/ consumer input and participation in HEALTHeLINK operations and decision making.

3.6 Requests to Correct Erroneous Information

A. HEALTHeLINK shall direct patients to the appropriate Participants who can assist them in a timely fashion to resolve an inquiry or dispute over the accuracy or integrity of their Protected Health Information, and to have erroneous information corrected or to have a dispute documented if their request to revise data is denied.

B. HEALTHeLINK shall require its Participants and Data Suppliers to notify HEALTHeLINK if, in response to a request by a patient, the Participant or Data Supplier makes any corrections to the patient's erroneous information.

C. HEALTHeLINK shall make reasonable efforts to provide its Participants with information indicating which other HEALTHeLINK Participants have Accessed or received erroneous information that the Participant has corrected at the request of patients in accordance with Section 3.6.A.

D. If HEALTHeLINK determines that the error is due in part to HEALTHeLINK's data aggregation and exchange activities (instead of solely due to an error in the underlying record maintained by the applicable Participant[s]), then HEALTHeLINK shall comply with P16 Section 3.6.

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) § 5.*

1 Policy Statement

Audits are necessary for verifying compliance with access controls developed to prevent/limit inappropriate access to information. This policy sets forth requirements for logging and auditing access to health information via HEALTHeLINK.

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.

3 Procedure

3.1 Maintenance of Audit Logs

HEALTHeLINK shall maintain Audit Logs that document all Disclosures of Protected Health Information via HEALTHeLINK.

A. Audit Logs shall, at a minimum, include the following information regarding each instance of Access to Protected Health Information via HEALTHeLINK:
   i. The identity of the patient whose Protected Health Information was Accessed;
   ii. The identity of the Authorized User Accessing the Protected Health Information;
   iii. The identity of the Participant with which such Authorized User is affiliated;
   iv. The type of Protected Health Information or record Accessed (e.g., pharmacy data, laboratory data, etc.);
   v. The date and time of Access;
   vi. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the Accessed Protected Health Information was derived);
   vii. Unsuccessful Access (log-in) attempts; and
   viii. Whether Access occurred through a Break the Glass incident.

B. Audit Logs shall, at a minimum, include the following information regarding each Transmittal of Protected Health Information via HEALTHeLINK:
   i. The identity of the patient whose Protected Health Information was Transmitted;
   ii. The identity of the recipient of the Protected Health Information in the case of a Transmittal;
   iii. The type of Protected Health Information or record Transmitted (e.g., pharmacy data, laboratory data, etc.);
   iv. The date and time of Transmittal; and
   v. The source of the Protected Health Information (i.e., the identity of the Participant from whose records the Transmittal of Protected Health Information was derived).

3.1.1 Other Requirements Regarding Audit Logs and Access

A. With respect to Access to Protected Health Information through HEALTHeLINK by a Certified Application, the Audit Log shall include each instance in which such Protected Health Information was Accessed (i) by the Certified Application through HEALTHeLINK and (ii) by an individual user of the Participant through the Participant's system.

B. With respect to Access to Protected Health Information through HEALTHeLINK by an Authorized User of a Public Health Agency, HEALTHeLINK shall track at the time of Access the reason(s) for each Authorized User's Access of Protected Health Information.

3.1.2 Other Requirements Regarding Audit Logs and Transmittals

A. HEALTHeLINK shall not be required to include a Transmittal with an Audit Log in cases where HEALTHeLINK Transmits Protected Health Information from one Participant to another Participant, or to a Business Associate of another Participant, in accordance with written instructions from the recipient and without modification to the data being Transmitted (as may occur in the case of a One-to-One Exchange).

B. In the case where HEALTHeLINK performs analytics on behalf of a Participant by running queries on a data set, if a patient's Protected Health Information is returned in response to such query, then such result shall not be considered a Transmittal, and HEALTHeLINK shall not be required to include a record of such query in the patient's Audit Log. If the analytics process results in the production of a data set which is Transmitted by HEALTHeLINK to the Participant and such data set includes Protected Health Information of a patient that is derived from the records of any Data Supplier other than the Participant receiving the data set, HEALTHeLINK shall record such Transmittal in the patient's Audit Log.

3.1.3 General Audit Log Requirements

A. Audit Logs shall be immutable. An immutable Audit Log requires either that log information cannot be altered by anyone regardless of Access privilege or that any alterations are tamper evident.

B. Audit Logs shall be maintained for a period of at least six years from the date on which information is Disclosed.

3.2 Obligation to Conduct Periodic Audits

HEALTHeLINK shall conduct, or shall require each of its Participants to conduct, periodic audits to monitor use of HEALTHeLINK by Participants and their Authorized Users and ensure compliance with the Policies and Procedures and all applicable laws, rules and regulations.

A. HEALTHeLINK shall audit, or require its Participants to audit, the following:
   1. That Affirmative Consents are on file for patients whose Protected Health Information is Disclosed via HEALTHeLINK, other than in Break the Glass situations;

2. That Authorized Users who Access Protected Health Information via the SHIN-NY do so for Authorized Purposes; and
3. That applicable requirements were met, as outlined in P04 3.2.4 where Protected Health Information was Disclosed through a Break the Glass incident.

B. If a Participant Accesses Protected Health Information via the SHIN-NY through a Certified Application, the audits described in Section 3.2.A shall include Access by the Participant's users through the Participant's system.

C. The activities of all or a statistically significant subset of HEALTHeLINK's Participants shall be audited.

D. Periodic audits shall be conducted at least on an annual basis. HEALTHeLINK shall consider their own risk analyses and organizational factors, such as current technical infrastructure, hardware and software security capabilities and whether Access was obtained through a Certified Application, to determine the reasonable and appropriate frequency with which to conduct audits more often than annually. Notwithstanding the foregoing, all Break the Glass incidents shall be audited.

E. Periodic audits shall be conducted using a statistically significant sample size.

F. If audits are conducted by Participants rather than by HEALTHeLINK, HEALTHeLINK shall:
1. Require each Participant to conduct the audit within such time period as reasonable requested by HEALTHeLINK; and
2. Require each Participant to report the results of the audit to HEALTHeLINK within such time period and in such format as reasonable requested by HEALTHeLINK.

3.3 Participant Access to Audit Logs

A. HEALTHeLINK shall provide the Participant, upon request, with the following information regarding any patient of the Participant whose Protected Health Information was Disclosed via the SHIN-NY:
1. The name of each Authorized User who Accessed such patient's Protected Health Information in the prior 6-year period;
2. The time and date of such Disclosure; and
3. The type of Protected Health Information or record that was Disclosed (e.g., clinical data, laboratory data, etc.).

B. A Participant shall only be entitled to receive Audit Log information pursuant to Section 3.3.A for patients who have provided Affirmative Consent for that Participant to Access his or her Protected Health Information.

C. HEALTHeLINK shall provide such information as promptly as reasonably practicable but in no event more than 10 calendar days after receipt of the request.

3.4 Patient Access to Audit Information

A. HEALTHeLINK shall provide patients, upon request, with the following information:
   1. The name of each Participant that Accessed or received the patient's Protected Health Information in up to the prior 6-year period;
   2. The time and date of the Disclosure; and
   3. The type of Protected Health Information or record that was Disclosed (e.g., clinical data, laboratory data, etc.).

B. If a patient requests the name(s) of the Authorized User(s) who Accessed his or her Protected Health Information through a specific Participant in up to the prior 6-year period, HEALTHeLINK and that Participant shall take the following actions:
   1. HEALTHeLINK shall inform the Participant of the request and shall provide the Participant with the list of the Participant's Authorized User(s) who Accessed the patient's Protected Health Information through HEALTHeLINK in up to the prior 6-year period;
   2. The Participant shall either provide the list of Authorized User(s) to the patient or undertake an audit to determine if the Authorized User(s) on the list appropriately Accessed the patient's Protected Health Information for Authorized Purposes;
   3. If the Participant chooses to undertake an audit of its Authorized User Access and determines that all of the Authorized User(s) Accessed the patient's information for Authorized Purposes, the Participant shall inform the patient of this finding and need not provide the patient with the names of the Authorized User(s) who Accessed that patient's information;
   4. If the Participant chooses to undertake an audit of its Authorized User Access and determines that one or more of the Authorized User(s) did not Access the patient's information for Authorized Purposes, the Participant shall (i) inform the patient of this finding; (ii) provide the patient with the name(s) of the Authorized User(s) who inappropriately Accessed the patient's information unless the Participant has a reasonable belief that such disclosure could put the Authorized User at risk of harm, in which case the Participant shall provide the patient with an opportunity to appeal this determination to a representative who is more senior to the individual(s) who made the original determination; and (iii) inform HEALTHeLINK of the inappropriate Access and otherwise comply with the requirements in HEALTHeLINK Policy P06, *Breach Response*.

C. If requested, HEALTHeLINK shall, or shall require their Participants to, provide such information to patients at no cost once in every 12-month period. HEALTHeLINK may establish a reasonable fee for any additional requests within a given 12-month period; provided that HEALTHeLINK shall waive any such fee where such additional request is based on a patient's allegation of unauthorized Access to the patient's Protected Health Information via HEALTHeLINK.

D. If applicable, HEALTHeLINK shall, or shall require their Participants to, provide notice of the availability of such information on any patient portals maintained by HEALTHeLINK or its Participants.

3.5 Public Availability of Audits

HEALTHeLINK shall make the results of its periodic audit available on HEALTHeLINK's website. Such results shall be made available as promptly as reasonably practicable, but in any event not more than 30 days after completion of the audit.

3.6 Correction of Erroneous Data

In the most expedient time possible HEALTHeLINK shall investigate (or require the applicable Participant to investigate) the scope and magnitude of any data inconsistency or potential error that was made in the course of HEALTHeLINK's data aggregation and exchange activities and, if an error is determined to exist, identify the root cause of the error and ensure its correction. HEALTHeLINK shall log all such errors, the actions taken to address them and the final resolution of the error. HEALTHeLINK shall also make reasonable efforts to identify Participants that Accessed or received such erroneous information and to notify them of corrections. This provision does not apply to updates to data that are made by Data Suppliers in the ordinary course of their clinical activities nor does it apply to updates to Demographic Information.

3.7 Weekly Audit Reports by Organ Procurement Organizations

HEALTHeLINK shall require weekly confirmation by Organ Procurement Organizations that all instances in which Protected Health Information was Accessed through HEALTHeLINK by the Organ Procurement Organization's Authorized Userswere consistent with the terms of these Policies and Procedures (based upon a listing sent by the HEALTHeLINK).

3.8 Additional Requirements Related to Auditing of Public Health Access

HEALTHeLINK shall use special safeguards with respect to audits of Access by Public Health Agencies, which shall include at least the following:

A. HEALTHeLINK shall create, on a regular basis, an audit report of Authorized User activity for each Public Health Agency workgroup that will include, at a minimum, the patient names, times, dates and reason for Access for each Authorized User;

B. The name of the particular Public Health Agency shall be listed in the patient Audit Logs;

C. HEALTHeLINK shall follow-up with workgroup manager(s) if approval of an audit report is not received. If the attempt to contact the workgroup manager(s) is unsuccessful, HEALTHeLINK may suspend all Authorized User accounts associated with that particular workgroup until the situation is resolved.

4 References

- HEALTHeLINK Policy P06, *Breach Response.*
- 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).*

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.

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.

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

HEALTHeLINK™

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

HEALTHeLINK™

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.

Glossary

ACCESS

The ability of an Authorized User or Certified Application to view Protected Health Information on HEALTHeLINK's electronic health information system following the Authorized User's or Certified Application's logging on to HEALTHeLINK.

ACCOUNTABLE CARE ORGANIZATION (ACO)

An organization of clinically integrated health care providers certified by the Commissioner of Health under N.Y. Public Health Law Article 29-E.

ADMINISTRATIVE SAFEGUARDS

Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic Protected Health Information and to manage the conduct of the covered entity's or business associate's workforce in relation to the protection of that information.

AFFILIATED PRACTITIONER

(i) A Practitioner employed by or under contract to a Provider Organization to render health care services to the Provider Organization's patients; (ii) a Practitioner on a Provider Organization's formal medical staff or (iii) a Practitioner providing services to a Provider Organization's patients pursuant to a cross-coverage or on-call arrangement.

AFFIRMATIVE CONSENT

The consent of a patient obtained through the patient's execution of (i) a Level 1 Consent; (ii) a Level 2 Consent; (iii) an Alternative Consent; or (iv) a consent that may be relied upon under the Patient Consent Transition Rules.

ALTERNATIVE CONSENT

A consent form approved under Policy P04, *Patient Consent*, Section 3.3, as an alternative to a Level 1 Consent or a Level 2 Consent.

AMERICAN RECOVERY AND REINVESTMENT ACT (ARRA)

The American Recovery and Reinvestment Act of 2009 (ARRA) is an economic stimulus bill created to help the United States economy recover from an economic downturn that began in late 2007. Congress enacted ARRA February 17, 2009.

APPROVED CONSENT

An Affirmative Consent other than a consent relied upon by a Participant under the Patient Consent Transition Rules.

AUDIT LOG

An electronic record of the Disclosure of information via the SHIN-NY governed by HEALTHeLINK, such as, for example, queries made by Authorized Users, type of information Disclosed, information flows between HEALTHeLINK and Participants, and date and time markers for those activities.

AUTHENTICATOR ASSURANCE LEVEL 2 (AAL2)

The authentication categorization set forth in NIST SP 800-63 which provides high confidence that the individual seeking access controls authenticator(s) bound to the Authorized User's account. Under AAL2, proof of possession and control of two distinct authentication factors are required through secure authentication protocol(s).

AUTHORIZED PURPOSES

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

AUTHORIZED USER

An individual who has been authorized by a Participant or HEALTHeLINK to Access patient information via the SHIN-NY governed by HEALTHeLINK in accordance with these Policies and Procedures.

AVAILABILITY

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

BREACH

The acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the Protected Health Information. An acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless the Participant or HEALTHeLINK can demonstrate that there is a low probability that the Protected Health Information has been compromised based on a risk assessment of at least the following factors: (i) the nature and extent of the Protected Health Information involved, including the types of identifiers and the likelihood of re-identification; (ii) the unauthorized person who used the Protected Health Information or to whom the disclosure was made; (iii) whether the Protected Health Information was actually acquired or viewed; and (iv) the extent to which the risk to the Protected Health Information has been mitigated. Breach excludes: (i) any unintentional acquisition, access, or use of Protected Health Information by a workforce member or person acting under the authority of HEALTHeLINK or a Participant, if such acquisition,

access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule; (ii) any inadvertent disclosure by a person who is authorized to access Protected Health Information at HEALTHeLINK or a Participant to another person authorized to access Protected Health Information at HEALTHeLINK or a Participant, or organized health care arrangement in which a Participant participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or (iii) a disclosure of Protected Health Information where HEALTHeLINK or a Participant has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

BREAK THE GLASS

The ability of an Authorized User to Access a patient's Protected Health Information without obtaining an Affirmative Consent.

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.

BUSINESS ASSOCIATE AGREEMENT (BAA)

A written signed agreement meeting the HIPAA requirements of 45 C.F.R. § 164.504(e).

CARE MANAGEMENT

(i) Assisting a patient in obtaining appropriate medical care, (ii) improving the quality of health care services provided to a patient, (iii) coordinating the provision of multiple health care services to a patient or (iv) supporting a patient in following a plan of medical care.

CARIN ALLIANCE

The multi-sector collaborative that seeks to advance consumer-directed exchange of health information and which has developed a list of recommended Patient Apps via its "My Health Application" website.

CENTRALIZED RESEARCH COMMITTEE

A committee that includes representatives of all QEs in the SHIN-NY, NYS DOH, and other relevant stakeholders that is organized to review and approve Research proposals under which a researcher seeks information from more than one QE. The Centralized Research Committee shall meet 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 a QE or any entity conducting or sponsoring the research, and is not related to any person who meets any of the foregoing criteria; and (iii) does not have any member participating in a review of any project in which the member has a conflict of interest.

CERTIFIED APPLICATION

A computer application certified by HEALTHeLINK that is used by a Participant to Access Protected Health Information from HEALTHeLINK on an automated, system-to-system basis without direct Access to HEALTHeLINK's system by an Authorized User.

CHARTER MEMBERS

The entities as defined in the HEALTHeLINK bylaws as Charter Members.

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).

COMMUNITY-BASED ORGANIZATION (CBO)

An organization, which may be a not-for-profit entity or government agency, which has the primary purpose of providing social services such as housing assistance, nutrition assistance, employment assistance, or benefits coordination. A Community-Based Organization may or may not be a Covered Entity.

CONSENT IMPLEMENTATION DATE

The date by which the NYS DOH requires HEALTHeLINK to begin to utilize an Approved Consent. In establishing such date, NYS DOH shall take into account the time that will be required for HEALTHeLINK to come into compliance with the Policies and Procedures regarding consent set forth herein.

CORONER

Any individual elected to serve as a county's coroner in accordance with New York State County Law § 400.

COVERED ENTITY (CE)

Has the meaning ascribed to this term in 45 C.F.R. § 160.103 and is thereby bound to comply with the HIPAA Privacy Rule and HIPAA Security Rule.

CYBER SECURITY POLICIES AND PROCEDURES (CSPP)

HEALTHeLINK's and the State Designated Entities' set of policies and procedures that aim to protect HEALTHeLINK and SHIN-NY Enterprise's information systems data.

DATA INTEGRITY

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

DATA PROVIDER

A Participant that is registered to provide Patient Data to the HIE.

DATA SUPPLIER

An individual or entity that supplies Protected Health Information to or through HEALTHeLINK. Data Suppliers include both Data Providers and entities that supply but do not Access Protected Health Information via the SHIN-NY governed by HEALTHeLINK (such as clinical laboratories and pharmacies). Government agencies, including Public Health Agencies, may be Data Suppliers.

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.

DE-IDENTIFIED DATA

Data that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. Data may be considered de-identified only if it satisfies the requirements of 45 C.F.R. § 164.514(b).

DEMOGRAPHIC INFORMATION

A patient's name, gender, address, date of birth, Social Security number, and other personally identifiable information, but shall not include any information regarding a patient's health or medical treatment or the names of any Data Suppliers that maintain medical records about such patient.

DESIGNATED RECORD SET

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

DIRECTOR

An executive-level manager of HEALTHeLINK.

DISASTER RELIEF AGENCY

(i) A government agency with authority under federal, state or local law to declare an Emergency Event or assist in locating individuals during an Emergency Event or (ii) a third-party contractor to which such a government agency delegates the task of assisting in the location of individuals in such circumstances.

DISCLOSURE

The release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information. HEALTHeLINK engages in a Disclosure of information if HEALTHeLINK (i) provides the Participant with Access to such information and the Participant views such information as a result of such Access, or (ii) Transmits such information to a Participant or other third party.

DOB

Date of Birth.

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. HEALTHeLINK Participants and their Authorized Users, as defined in the PA, are DURSA Participant Users.

ELECTRONIC MEDICAL RECORD (EMR)

An electronic medical record (EMR) is an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization.

ELECTRONIC PROTECTED HEALTH INFORMATION (EPHI)

Information that comes within paragraphs 1(i) or 1(ii) of the definition of "Protected Health Information", as defined in 45 C.F.R. § 160.103.

ELECTRONIC SIGNATURE

A signature that meets the requirements of the federal Electronic Signature in Global and National Commerce Act (ESIGN), 15 USC § 7001 et seq., or the New York State Electronic Signatures and Records Act (ESRA), NY Tech. Law § 301, et seq.

EMANCIPATED MINOR

A minor who is emancipated on the basis of being married or in the armed services, or who is otherwise deemed emancipated under New York law or other applicable laws.

EMERGENCY EVENT

A circumstance in which a government agency declares a state of emergency or activates a local government agency incident command system or similar crisis response system.

EMERGENCY MEDICAL TECHNICIAN

A person certified pursuant to the New York State Emergency Services Code at 10 N.Y.C.R.R. §§ 800.3 and 800.6 as an emergency medical technician, emergency medical technician-intermediate, an emergency medical technician-critical care, or an emergency medical technician-paramedic.

EMPLOYEES

Employees, students/trainees, volunteers, consultants and other individuals under the direct control of HEALTHeLINK or a HEALTHeLINK 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.

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.

FAILED ACCESS ATTEMPT

An instance in which an Authorized User or other individual attempting to Access HEALTHeLINK is denied Access due to use of an inaccurate log-in, password, or other security token.

FNAME

Patient First Name.

HEALTH CARE OPERATIONS

Has the meaning ascribed to this term in HIPAA, 45 C.F.R. 164.501. Health care operations means any of the following activities of the covered entity to the extent that the activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 C.F.R. 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;

(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non- health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to:

(i) Management activities relating to implementation of and compliance with the requirements of this subchapter;

(ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer.

(iii) Resolution of internal grievances;

(iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
(v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

HEALTH HOME

An entity that is enrolled in New York's Medicaid Health Home program and that receives Medicaid reimbursement for providing care management services to participating enrollees.

HEALTH HOME MEMBER

An entity that contracts with a Health Home to provide services covered by New York's Medicaid Health Home program.

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.

HEALTH INFORMATION EXCHANGE ORGANIZATION

An entity that facilitates and oversees the exchange of Protected Health Information among Covered Entities, Business Associates, and other individuals and entities.

HEALTH INFORMATION TECHNOLOGY FOR ECONOMIC AND CLINICAL HEALTH ACT (HITECH)

The Health Information Technology for Economic and Clinical Health (HITECH) Act is legislation enacted under the American Recovery and Reinvestment Act of 2009 (ARRA) to promote and expand the adoption of health information technology.

HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The Health Insurance Portability and Accountability Act of 1996, as amended from time to time, and its implementing regulations set forth at 45 C.F.R. Parts 160 and 164.

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.

HHS

Department of Health and Human Services.

HIPAA PRIVACY RULE

The federal regulations at 45 C.F.R. Part 160 and Subparts A and E of Part 164.

HIPAA SECURITY RULE

The federal regulations at 45 C.F.R. Part 160 and Subpart C of Part 164.

INCIDENTAL DISCLOSURE

A secondary use or disclosure that cannot reasonably be prevented, is limited to demographic information other than any elements of a social security number except the last four digits thereof, occurs as a by-product of an otherwise permitted use or disclosure, and occurs notwithstanding the implementation by HEALTHeLINK and/or its Participants of reasonable safeguards to limit disclosures.

INDEPENDENT PRACTICE ASSOCIATION (IPA)

An entity that is certified as an independent practice association under 10 N.Y.C.R.R. § 98- 1.5(b)(6)(vii).

INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION (IIHI)

A subset of health information, including demographic information collected from an individual, that is created or received by a health care provider or plan, employer, or healthcare clearinghouse, and relates to the past, present, or future physical or mental health or condition or TO payment for healthcare and that identifies or can be used to identify the individual.

INFORMATION BLOCKING RULES

The requirements and exceptions related to information blocking established by The Office of the National Coordinator for Health Information Technology set forth at 45 C.F.R. Part 171.

INFORMATION SECURITY EVENT

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

INFORMATION SECURITY INCIDENT

That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. NOTE: The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

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.

INSURANCE COVERAGE REVIEW

The use of information by a Participant (other than a Payer Organization) to determine which health plan covers the patient or the scope of the patient’s health insurance benefits.

INTEGRITY

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

LEVEL 1 CONSENT

A consent permitting Access to and receipt of Protected Health Information for Level 1 Uses.

LEVEL 1 USES

Treatment, Quality Improvement, Care Management, Utilization Review, and Insurance Coverage Reviews.

LEVEL 2 CONSENT

A consent permitting Access to and receipt of Protected Health Information for a Level 2 Use.

LEVEL 2 USES

Any uses of Protected Health Information other than Level 1 Uses, including but not limited to Payment, Research and Marketing.

LIMITED DATA SET

Protected Health Information that excludes the 16 direct identifiers set forth at 45 C.F.R. § 164.514(e)(2) of an individual and the relatives, employers, or household members of such individual.

LNAME

Patient Last Name.

MALICIOUS SOFTWARE (MALWARE)

Software designed to damage or disrupt a system (e.g., a virus).

MARKETING

Has the meaning ascribed to this term under the HIPAA Privacy Rule as amended by Section 13406 of HITECH (42 USC § 17936).

MASTER PATIENT INDEX (MPI)

An index in which patient demographic data is stored.

MEDICAL EXAMINER

A licensed physician who serves in a county medical examiner's office in accordance with New York State County Law § 400, and shall include physicians within the New York City Office of Chief Medical Examiner.

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, STD, 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.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) CYBERSECURITY FRAMEWORK

The set of industry standards and best practices to help organizations manage cybersecurity risks that has been developed by the National Institute of Standards and Technology. The NIST Cybersecurity Framework uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses.

NEW YORK EHEALTH COLLABORATIVE (NYEC)

The New York not-for-profit corporation organized for the purpose of (i) convening, educating and engaging key constituencies, including health care and health IT leaders across New York State, QEs, and other health IT initiatives; (ii) developing common health IT policies and procedures, standards, technical requirements and service requirements through a transparent governance process and (iii) evaluating and establishing accountability measures for New York State's health IT strategy. NYeC is under contract to the NYS DOH to administer the SCP and through it develop SHIN-NY Policy Guidance.

NON-REPUDIATION

To ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

NYS DOH

New York State Department of Health.

ONE-TO-ONE EXCHANGE

A Transmittal of Protected Health Information originating from a Participant which has a relationship with a patient to one or more other Participants with the patient's knowledge and implicit or explicit consent where no records other than those of the Participants jointly providing health care or social services to the patient are Transmitted. Examples of a One-to-One Exchange include, but are not limited to, information provided by a primary care provider to a specialist when referring to such specialist, a discharge summary sent to where the patient is transferred, lab results sent to the Practitioner who ordered the laboratory test, or a claim sent from a Participant to the patient's health plan.

ORGAN PROCUREMENT ORGANIZATION (OPO)

A regional, non-profit organization responsible for coordinating organ and tissue donations at a hospital that is designated by the Secretary of Health and Human Services under section 1138(b) of the Social Security Act (see also 42 C.F.R. § 121).

PARTICIPANT

A Provider Organization, Payer Organization, Practitioner, Independent Practice Association, Accountable Care Organization, Public Health Agency, Organ Procurement Organization, Health Home, Health Home Member, PPS Partner, PPS Lead Organization, PPS Centralized Entity, Social Services Program, a Community-Based Organization, or Disaster Relief Agency that has directly or indirectly entered into a Participation Agreement with HEALTHeLINK and Accesses Protected Health Information via the SHIN-NY governed by HEALTHeLINK.

PARTICIPANT AUTHORIZED CONTACT

A person within a practice, facility, or organization who is responsible for communication, administration, and other duties related to an entity's role as a Participant.

PARTICIPATION AGREEMENT

The agreement made by and between HEALTHeLINK and each of its Participants, which sets forth the terms and conditions governing the operation of HEALTHeLINK and the rights and responsibilities of the Participants and HEALTHeLINK with respect to HEALTHeLINK.

PASSWORD

Confidential authentication information composed of a string of characters.

PATIENT APP

An application on a patient's smart phone, laptop, tablet, or other technology that collects Protected Health Information about the patient and makes such Protected Health Information accessible to the patient.

PATIENT CARE ALERT ("ALERT")

An electronic message about a development in a patient's medical care, such as an emergency room or inpatient hospital admission or discharge, a scheduled outpatient surgery or other procedure, or similar event, which is derived from information maintained by HEALTHeLINK and is Transmitted by HEALTHeLINK to subscribing recipients but does not allow the recipient to Access any Protected Health Information through HEALTHeLINK other than the information contained in the message. Patient Care Alerts may contain demographic information such as patient name and date of birth, the name of the Participant from which the patient received treatment, and limited information related to the patient's complaint or diagnosis but shall not include the patient's full medical record relating to the event that is the subject of the electronic message.

PATIENT CONSENT TRANSITION RULES

The rules set forth in P04 § 3.10.

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.

PAYER ORGANIZATION

An insurance company, health maintenance organization, employee health benefit plan established under ERISA or any other entity that is legally authorized to provide health insurance coverage.

PAYMENT

The activities undertaken by (i) a health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan or (ii) a health care provider or health plan to obtain or provide reimbursement for the provision of health care. Examples of payment are set forth in the HIPAA regulations at 45 C.F.R. § 164.501.

PERFORMING PROVIDER SYSTEM (PPS)

A Performing Provider System that had received approval from NYS DOH to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program. Note: the DSRIP program ended March 31, 2020.

PERSONAL REPRESENTATIVE

A person who has the authority to consent to the Disclosure of a patient's Protected Health Information under Section 18 of the New York State Public Health Law and any other applicable state and federal laws and regulations.

PHYSICAL SAFEGUARDS

Physical measures, policies, and procedures to protect a covered entity's or business associate's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

PPS CENTRALIZED ENTITY

An entity owned or controlled by one or more PPS Partners that has been engaged by a PPS to perform Care Management, Quality Improvement or Insurance Coverage Reviews on behalf of the PPS.

PPS LEAD ORGANIZATION

Entity that has been approved by NYS DOH and CMS to serve as designated organization that has assumed all responsibilities associated with Delivery System Reform Incentive Payment ("DSRIP") program per their project application and DSRIP award.

PPS PARTNER

A person or entity that is listed as a PPS Partner in the DSRIP Network Tool maintained by NYS DOH.

PRACTITIONER

A health care professional licensed under Title 8 of the New York Education Law, or an equivalent health care professional licensed under the laws of the state in which he or she is practicing or a resident or student acting under the supervision of such a professional.

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.

PRIVILEGED ACCOUNT

A system or application account, such as a system administrator's account, that has more privileges than a normal user account.

PROTECTED HEALTH INFORMATION (PHI)

Individually identifiable health information (e.g., any oral or recorded information relating

to the past, present, or future physical or mental health of an individual; the provision of health care to the individual; or the payment for health care) of the type that is protected under the HIPAA Privacy Rule.

PROVIDER ORGANIZATION

An entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services.

PUBLIC HEALTH AGENCY

An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, the New York State Department of Health, a New York County Health Department, or the New York City Department of Health and Mental Hygiene, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate and that has signed a Participation Agreement with HEALTHeLINK and Accesses Protected Health Information via the SHIN-NY governed by HEALTHeLINK.

PUBLIC HEALTH AUTHORITY

An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

QUALIFIED ENTITY PARTICIPATION AGREEMENT (QEPA)

The agreement between each of the QEs and the State Designated Entity entered into in April 2014 that sets forth the terms and conditions for HEALTHeLINK participation in the SHIN-NY including providing HEALTHeLINK Participants Access to and use of the SHIN-NY.

QUALIFIED HEALTH IT ENTITY (QE)

A not-for-profit entity that has been certified as a QE under 10 N.Y.C.R.R. Section 300.4 and has executed a contract to which it has agreed to be bound by SHIN-NY Policy Standards.

QUALITY IMPROVEMENT

Activities designed to improve processes and outcomes related to the provision of health care services. Quality Improvement activities include but are not limited to outcome evaluations; development of clinical guidelines; population based activities relating to improving health or reducing health care costs; clinical protocol development and decision support tools; case management and care coordination; reviewing the

competence or qualifications of health care providers, but shall not include Research. The use or Disclosure of Protected Health Information for quality improvement activities may be permitted provided the Accessing and Disclosing entities have or had a relationship with the individual who is the subject of the Protected Health Information.

RECORD LOCATOR SERVICE OR OTHER COMPARABLE DIRECTORY

A system, queryable only by Authorized Users, that provides an electronic means for identifying and locating a patient's medical records across Data Suppliers.

REGISTRATION APPLICATION

The application submitted by a person or entity that wishes to become a Participant.

RESEARCH

A systematic investigation, including research development, testing and evaluation designated to develop or contribute to generalizable knowledge, including clinical trials.

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.

RETROSPECTIVE RESEARCH

Research that is not conducted in connection with Treatment and involves the use of Protected Health Information that relates to Treatment provided prior to the date on which the Research proposal is submitted to an Institutional Review Board.

RHIO

Regional Health Information Organization.

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.

SENSITIVE HEALTH INFORMATION

Any information subject to special privacy protection under state or federal law, including but not limited to, HIV/AIDS, mental health, alcohol and substance use, reproductive health, sexually-transmitted disease, and genetic testing information.

SHIN-NY ENTERPRISE

The information technology (IT) infrastructure inclusive of the Qualified Entities (QEs) and the Statewide SHIN-NY Hub that supports the electronic exchange of patient health information across New York State.

SHIN-NY HUB

The information technology (IT) infrastructure operated by the State Designated Entity that allows for the exchange of information between QEs.

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.

SOCIAL SECURITY NUMBER (SNN)

The nine-digit number issued by the Social Security Administration to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act.

SOCIAL SERVICES PROGRAM

A program within a social services district (as defined by New York Social Services Law, § 2) which has authority under applicable law to provide “public assistance and care” (as defined by New York Social Services Law § 2), Care Management, or coordination of care and related services.

STAKEHOLDER

A Charter Member.

STATE DESIGNATED ENTITY (SDE)

The public/private partnership in New York State that has been designated by the New York State Commissioner of Health as eligible to receive federal and state grants to promote health information technology.

STATEWIDE CHIEF INFORMATION SECURITY OFFICER (CISO)

The senior-level executive employed by the State Designated Entity who has authority over the SHIN-NY Enterprise in order to establish and maintain the vision, strategy, and

security program to ensure the SHIN-NY Enterprise's information assets and technologies are adequately protected.

STATEWIDE COLLABORATION PROCESS (SCP)

An open, transparent process to which multiple SHIN-NY stakeholders contribute, that is administered by the State Designated Entity for the development of SHIN-NY Policy Guidance as provided in 10 N.Y.C.R.R. Section 300.3.

STATEWIDE CONSENT DATE

The date on which NYS DOH requires Participants to offer to patients a Statewide Form of Consent.

STATEWIDE FORM OF CONSENT

The proposed community-wide Level 1 Consent that (i) at minimum, allows for disclosure of Protected Health Information to all current and future Participants who provide Treatment to a patient, regardless of which QE such Participants have contracted with; and (ii) has been approved and issued by NYS DOH.

STATEWIDE HEALTH INFORMATION NETWORK OF NEW YORK (SHIN-NY)

The technical infrastructure (SHIN-NY Enterprise) and the supportive policies and agreements that make possible the electronic exchange of clinical information among QEs, Participants, and other individuals and entities for authorized purposes, including both the infrastructure that allows for exchange among Participants governed by the same QE and the infrastructure operated by the State Designated Entity that allows for exchange between different QEs. The goals of the SHIN-NY are to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting patient privacy and ensuring data security.

STATEWIDE PATIENT RECORD LOOKUP (sPRL)

A system under which Protected Health Information or other information may be accessed across QE systems for disclosure to a Participant or other person who is permitted to receive such information under the terms of these Policies and Procedures.

TECHNICAL SAFEGUARDS

The technology and the policy and procedures for its use that protect electronic Protected Health Information and control access to it.

TELEHEALTH

The use of electronic information and two-way, real-time communication technologies to deliver health care to patients at a distance. Such communication technologies include both audio-video and audio-only (e.g., telephonic) connections.

TRANSMITTAL

HEALTHeLINK's transmission of Protected Health Information, a Limited Data Set, or De-identified Data to a recipient in either paper of electronic form, other than via the display of such information through HEALTHeLINK's electronic health information system or through a Certified Application.

TREATMENT

The provision, coordination, or management of health care and related services among health care providers or by a single health care provider, and may include providers sharing information with a third party. Consultation between health care providers regarding a patient and the referral of a patient from one health care provider to another also are included within the definition of Treatment.

UNAUTHORIZED USE

(i) any attempt at or any action that results in circumventing the access controls or access policies of the HIE; (ii) use in violation of intellectual property, privacy, publicity, proprietary information rights and policies of others; and/or (iii) use other than in accordance with the express terms of these Terms and Conditions, the Policies and Procedures, the SHIN-NY Policy Guidance, or applicable law.

UNSECURED PROTECTED HEALTH INFORMATION

Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the U.S. Department of Health and Human Services in guidance issued under section 13402(h)(2) of HITECH (42 USC 1793.2[h][2]).

USE

With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

UTILIZATION REVIEW

An activity carried out by a Payer Organization to determine whether a health care item or service that has been provided to an enrollee of such Payer Organization, or which has been proposed to be provided to such an enrollee, is medically necessary.

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.

VENDOR AGREEMENT

Each agreement between HEALTHeLINK and a Vendor respecting that Vendor's provision of software or hardware and/or performance of related 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.

WORKSTATION

Electronic computing device, or any other device that performs similar functions, and electronic media stored in its immediate environment (e.g., a laptop or desktop computer).

Revision History

Privacy Policies and Procedures

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
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

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
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

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
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19

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
Revision Effective Dates: 05/14/09, 04/01/10, 09/16/11, 04/25/13, 06/01/13, 06/30/16, 07/29/19

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
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/30/23

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
Revision Effective Dates: 05/14/09, 04/01/10, 04/25/13, 06/01/13, 06/30/16, 07/29/19, 06/27/22

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
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19

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
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/29/19

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
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20, 06/27/22, 06/30/23

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
Revision Effective Dates: 07/29/19, 06/28/21, 06/27/22, 06/30/23

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
Revision Effective Dates: 07/29/19, 06/27/22, 06/30/23

Security Policies

Governance
Policy SP-001
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Identify Risks and Threats
Policy SP-002
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Cybersecurity Protection
Policy SP-003
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Threat Detection
Policy SP-004
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Incident Response
Policy SP-005
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Incident Recovery
Policy SP-006
Effective Date: 05/23/24
Review Dates:
Revision Effective Dates: 06/28/24

Participant Requirements
Policy SP-007
Effective Date: 05/23/24
Review Dates:
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)