Privacy and Security Policies

Table of Contents

Privacy and Security Policies

Privacy Policies

Security Policies

Privacy Policies

1 Policy Statement

HEALTHeLINK Participants must comply with applicable law and HEALTHeLINK Policies 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 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 agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized User;

D. 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

E. Has complied with other requirements described in HEALTHeLINK Policies.

3.2 Requirements for HEALTHeLINK's Personnel

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

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

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

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

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

E. Has complied with other requirements described in HEALTHeLINK Policies and Statewide Policy Guidance.

3.3 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.

4 References

- 45 CFR § 164.514(d)(2)(i).
- HEALTHeLINK Policy P04, *Patient Consent*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 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

A. 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.

B. An Affirmative Consent may be executed by an electronic signature that meets the requirements of the federal ESIGN statue, 15 USC § 7001 et seq., or any other applicable state or federal laws or regulations.

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

A. 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 3.8.7 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:
   1. To investigate suspected or confirmed cases of communicable disease (pursuant to PHL § 2(1)(l) and 10 N.Y.C.R.R. Part 2);
   2. To ascertain sources of infection (pursuant to 10 N.Y.C.R.R. Part 2);
   3. To conduct investigations to assist in reducing morbidity and mortality (pursuant to 10 N.Y.C.R.R. Part 2);
   4. 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;
   5. 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);
   6. For purposes allowed by PHL § 2(1)(n), Article 23 and 10 N.Y.C.R.R. Part 23 (STD).
   7. For purposes allowed by PHL § 2401 and 10 N.Y.C.R.R. § 1.31 (cancer);
   8. For the activities of the Electronic Clinical Laboratory Reporting System (ECLRS), the Electronic Syndromic Surveillance System (ESSS) and the Health Emergency Response Data System (HERDS);

[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.*

9. For purposes allowed by PHL § 2004 and 10 N.Y.C.R.R. Part 62 (Alzheimer's);
10. For purposes allowed by PHL § 2819 (infection reporting);
11. 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);
12. For purposes allowed under 10 N.Y.C.R.R. Part 22 (environmental diseases);
13. To investigate suspected or confirmed cases of lead poisoning (pursuant to 10 N.Y.C.R.R. Part 67);
14. For purposes allowed by 10 N.Y.C.R.R. Part 69 (including newborn disease screening, newborn hearing screening and early intervention);
15. For purposes allowed under 10 N.Y.C.R.R. § 400.22 (Statewide Perinatal Data System);
16. For purposes allowed under 10 N.Y.C.R.R. § 405.29 (cardiac data); or
17. 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. A patient's denial of consent for all Participants in HEALTHeLINK to Access the patient's Protected Health Information under Section 3.9.3 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.

D. HEALTHeLINK may Disclose the reports and information subject to 10 NYCRR §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 NYCRR §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:
   1. Patient name and other demographic information in a Record Locator Services and Other Comparable Directories;
   2. 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 3.9.3 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 (1) a Practitioner, (2) an Authorized User acting under the direction of a Practitioner; or (3) an Advanced Emergency Medical Technician and these individuals may Break the Glass if the following conditions are met:

1. Treatment may be provided to the patient without informed consent because, in the Practitioner's or Advanced 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
2. The Practitioner or Advanced Emergency Medical Technician determines, in his or her reasonable judgment, that information that may be held by or accessible via HEALTHeLINK may be material to emergency treatment.
3. 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 Advanced Emergency Medical Technician is affiliated.
4. 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.
5. The Practitioner, Advanced 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 PHI 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. 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.
    1. 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.

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

F. 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.

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 CFR § 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 Section 3.2.7 above.

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 NYSDOH Regarding Medicaid Beneficiaries

A. Affirmative Consent shall not be required for HEALTHeLINK to Disclose Protected Health Information of Medicaid beneficiaries to NYSDOH or Business Associate of NYSDOH to the extent such Disclosure is necessary to (i) calculate performance under quality measures adopted by the New York State Medicaid program; or (ii) determine payments to be made under the New York State Medicaid program.

3.2.11 Death Notifications

A. 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

A. 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:

1. The receiving Participant is a licensed physician or nurse practitioner whose professional responsibilities include determining the cause of death of a patient. Such Practitioners may include Medical Examiners and Coroners who are licensed as physicians or nurse practitioners.
2. HEALTHeLINK and the Participant abide by the minimum necessary standard set forth at P03 § 3.3.
3. 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.

3.3 Form of Patient Consent

3.3.1 Except as otherwise permitted by the Patient Consent Transition Rules, 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.

3.3.2 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 abuse, reproductive health, sexually-transmitted disease, and genetic testing information, if such categories of information may be Disclosed to the recipient;

B. The intended uses to which the information will be put by the Participant. 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 3.3.3(c), the signature need not appear on the same page as the language required under subsections (a), (b), and (c) above

3.3.3 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.

3.3.4 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.

3.3.5 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.

3.3.6 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.

3.4 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 CFR Part 2 that contains the language required by 42 CFR § 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 abuse 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 minors 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 NYSDOH 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

3.6.1 Disclosure of De-Identified Data for Specified Uses

A. Affirmative Consent is not required for HEALTHeLINK, to Disclose De-Identified Data for Research in accordance with Section 3.7 below.

B. Affirmative Consent is not required for HEALTHeLINK to Disclose De-Identified Data for Quality Improvement, provided that HEALTHeLINK's Research Committee reviews and approves the Quality Improvement activity in accordance with standards. Participants must make available to the committee the methodology of any proposed Quality Improvement project, which HEALTHeLINK will make accessible to other Participants and the general public. (See HEALTHeLINK Policy P13, *Release of Data for Research*.)

C. Affirmative Consent is not required for HEALTHeLINK, a Participant, or a government agency to Access or receive De-Identified Data for any purpose for which HEALTHeLINK, the Participant, or government agency may lawfully Access or receive PHI under the Policies and Procedures.

D. Affirmative Consent is not required for HEALTHeLINK to perform an evaluation of the economic or other value of HEALTHeLINK. The methodology and results of any such evaluation will be posted on HEALTHeLINK's website.

E. 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.

3.6.2 Creation of De-Identified Data for Specified Uses

HEALTHeLINK may Access PHI to create and validate the accuracy of De-Identified Data that is Used in accordance with Section 3.6.1.

3.6.3 Other Requirements

A. All other uses of De-Identified Data require Affirmative Consent.

B. A patient's participation in HEALTHeLINK will not be conditioned on the patient's decision to consent or deny Access to De-Identified Data for purposes other than those set forth in Section 3.6.1.

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

D. Any Use of De-Identified Data will be subject to adequate restrictions on the re- identification of such 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 toa researcher conducting Retrospective Research if (1) an Institutional Review Board has approved of such Disclosure; and (2) the HEALTHeLINK Research Committee has approved of such Disclosure; and (3) 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 Protection 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 2 Consent set forth in Section 3.3.3 even if the Protected Health Information is being Transmitted for a Level 1 Use, provided that the time limitation in Section 3.9.5 shall not apply if the Protected Health Information is being Transmitted for a Level 1 Use. For the avoidance of doubt, 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. 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 (A) issued a disability or life insurance policy to the patient; (B) received an application from the patient for such a policy; or (C) 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; and

iv. Represent that the recipient is not excluded, debarred, or otherwise ineligible from participating in any federal health care programs.

F. Special requirements applicable to Transmittals to life or disability insurers.

i. If the recipient is a life or disability insurer that is not a governmental entity, then the agreement specified above must also require such insurer to warrant that it has not, and will not in the future, condition the granting of a disability or life insurance policy, the continuation of such policy the payment of a claim or a particular premium rate on the patient's agreement to sign an Affirmative Consent that allows HEALTHeLINK to Transmit the patient's Protected Health Information to such insurer.

ii. When HEALTHeLINK receives a query from a life or disability insurer seeking a patient's Protected Health Information, HEALTHeLINK shall notify the applicable patient, via email or otherwise, of the patient's option to rescind his or her Affirmative Consent to the insurer and/or request a list of the Data Suppliers that are the sources of the patient's Protected Health Information. HEALTHeLINK shall abide by a patient's request to rescind Affirmative Consent or provide a list of Data Suppliers if such request is received within 72 hours of HEALTHeLINK's notification of the patient. If HEALTHeLINK does not receive a request from a patient to rescind Affirmative Consent within the 72-hour period, HEALTHeLINK may Transmit the patient's Protected Health Information to the life or disability insurer.

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 Section P15 § 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 forward a copy of the Consent to HEALTHeLINK within 3 business days of obtaining the Consent form if needed.

3.9.2 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.

A. The Participant will obtain a new HEALTHeLINK Consent form in which the patient denies Access to information contained in the health information exchange.

B. The Participant will change the patient's preference in the HEALTHeLINK software.

C. A copy of the new Consent form must be forwarded to HEALTHeLINK within 3 business days if needed.

3.9.3 Denial of Consent

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

A. Patient denial of consent must be in writing on a HEALTHeLINK Consent form with one of the denial of consent options checked:
    1. "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)(3).

    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.

3.9.4 Consents Covering Multiple Participants

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

A. The Participant 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 that Participant.

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 notifies patients that the list of Participants will be regularly updated on HEALTHeLINK's website and that patients have a right to obtain a hard copy of the list, free of charge, upon request, 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.

3.9.5 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.

3.9.6 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.

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

Provider Participants must ensure that a Payer Organization cannot 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.

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

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

3.10 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 NYSDOH.

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 NYSDOH.

4 References

- 45 CFR Part 164
- 42 CFR Part 2
- 42 CFR § 489.24
- 42 CFR § 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
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)* § 1

Patient Request for Restrictions or Confidential Communications

Privacy Policy
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 request 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 CFR § 164.522.

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*

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 CFR Subpart D
- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK* Privacy and Security Policies
- 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)
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 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
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 compliant/concern and action taken will be sent to the HEALTHeLINK Executive Director.

E. The HEALTHeLINK Executive Director 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*).

4 References

- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)*

Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies

Privacy Policy
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 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.

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

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.

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 the violation resulted 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*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)* §9

Workforce Training for HEALTHeLINK Privacy and Security Policies

Privacy Policy
Policy No. P10

1 Policy Statement

HEALTHeLINK's Privacy and Security Policies 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, 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 CFR § 164.530
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1).*

Workforce Access to and Termination from HEALTHeLINK

Privacy Policy
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 Users.

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 oftermination.

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*).

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 eventwithin 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*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)*

Release of Data for Research

Privacy Policy
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 Executive Director 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,* 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, 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 CFR § 164.514(a) and (b)
- 45 CFR § 164.512(i)
- HEALTHeLINK Policy P04, *Patient Consent*
- HEALTHeLINK Policy P09, *Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies*
- Privacy and Security Policies and Procedures for Qualified Entities and Their Participant in New York State Under 10 NYCRR § 300.3(b)(1)

Patient Engagement and Access

Privacy Policy
Policy No. P15

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

A. HEALTHeLINK shall facilitate the access of patients and their Personal Representatives to the patient's Protected Health Information. HEALTHeLINK shall inform patients or their Personal Representatives, as appropriate, about the means through which they may access their Protected Health Information and all material terms and conditions regarding such access.

   1. HEALTHeLINK may facilitate access to Protected Health Information in the SHIN-NY through its own web-based portal or through Participants' patient web-based portals, provided that each such portal enables access to information maintained by HEALTHeLINK on behalf of all of its Participants or all Protected Health Information in the SHIN-NY.

   2. HEALTHeLINK may facilitate access to Protected Health Information in the SHIN-NY through a web-based portal established by or maintained by a third party on behalf of a patient, provided, to the extent required by applicable law, the patient or his or her Personal Representative authorizes HEALTHeLINK to release Protected Health Information in the SHIN-NY to such portal.

3. HEALTHeLINK shall facilitate access to Protected Health Information by providing a paper or electronic copy of information maintained about the patient by HEALTHeLINK. Each patient shall have the right to indicate whether he or she prefers to receive information in paper or electronicform.

B. HEALTHeLINK and its Participants may (but are not required to) allow patients to grant access to their Protected Health Information to family members, informal caregivers and friends of the patient who are not Personal Representatives, provided such access is in accordance with any privacy and security standards.

C. Access of patients, their Personal Representatives, their family members, their informal caregivers and their friends who are not Personal Representatives to Protected Health Information must be in accordance with all applicable laws and regulations, including but not limited to, PHL §18, MHL § 33.16 and 10 NYCCR § 58-1.8, as well as, laws granting minors the right to keep Minor Consent Information confidential from their parents or guardians.

D. 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.

E. 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.

F. 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.

G. 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.

4 References

- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 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

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

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

C. Audit Logs shall, at a minimum, include the following information regarding each Transmittal of Protected Health Information via HEALTHeLINK:

1. The identity of the patient whose Protected Health Information was Transmitted;
2. The identity of the recipient of the Protected Health Information in the case of a Transmittal;
3. The type of Protected Health Information or record Transmitted (e.g., pharmacy data, laboratory data, etc.);
4. The date and time of Transmittal; and
5. 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).

D. Other Requirements Regarding Audit Logs and Access

1. 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.

2. 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.

E. Other Requirements Regarding Audit Logs and Transmittals

1. 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).

2. 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.

F. General Audit Log Requirements
   1. 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.

   2. 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 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 AuthorizedUser.

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*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)*

Security Policies

1 Introduction

The statements in this policy document establish HEALTHeLINK's expectations with respect to the security responsibilities of HEALTHeLINK participants.

2 Scope

This policy applies to HEALTHeLINK Participants including but not limited to those who access HEALTHeLINK applications and those who maintain hardware, software, or networks connected to HEALTHeLINK systems.

This policy applies to physical locations where HEALTHeLINK Participants use, access, or connect to HEALTHeLINK systems.

This policy applies to the information HEALTHeLINK creates, manages, processes, stores, or transmits and to the information systems developed, operated, managed, or provided 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 Responsibilities

3.1.1 Protect Information and Assets from Access and Loss

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

3.1.2 Comply with Laws and Regulations

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

3.2 General

3.2.1 Use for Authorized Purposes

HEALTHeLINK Authorized Users must use and administer HEALTHeLINK's information and assets in an ethical manner and for authorized purposes only. (SHIN-NY 3.3 §4.2)

3.2.2 Sharing of Login Credentials

HEALTHeLINK Authorized Users must not share or disclose HEALTHeLINK authentication credentials to another individual. (SHIN-NY 3.3 §4.1.5)

3.2.3 Unauthorized Testing

HEALTHeLINK Authorized Users must not attempt to access, modify, delete, or perform testing on HEALTHeLINK information systems or services.

3.2.4 Disabling Security Controls

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.

3.3 Information Handling

3.3.1 Protect Sensitive Information from Disclosure

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.

3.4 Credentials

3.4.1 Use Only Issued Accounts

HEALTHeLINK Authorized Users must use only the user IDs, network addresses, and network connections issued to them to access HEALTHeLINK's information systems. (SHIN-NY 3.3 §4.1.5)

3.4.2 Use Complex Passwords

HEALTHeLINK Authorized Users must use passwords that are complex, are difficult to guess, are not contained in a dictionary, and meet HEALTHeLINK's published guidelines. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D)) (SHIN-NY 3.3 §4.1.2)

3.4.3 Do Not Share Passwords

HEALTHeLINK Authorized Users must not share user IDs, passwords, remote access tokens, card keys, or other individually assigned credentials. (HIPAA §164.310) (SHIN-NY 3.3 §4.1.5)

3.5 Incident Reporting

3.5.1 Prompt Incident Reporting

HEALTHeLINK Authorized Users must promptly report any known or suspected security incident or weakness, including but not limited to known or suspected unauthorized access, use, or disclosure of protected health information, to the Help Desk.

3.5.2 Cooperation During Investigations

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

3.6 Access and Use

3.6.1 Complete Account Setup Form

HEALTHeLINK Authorized Users must complete and submit an account setup form prior to being granted access to HEALTHeLINK applications. (SHIN-NY 3.3 §4.7.3)

3.6.2 Verify Account Setup Form Before Submission

Participant Authorized Contacts must verify information submitted on an account setup form prior to submitting a new HEALTHeLINK Authorized User to the Help Desk.

3.6.3 Notify at Termination or Role Change

Participant Authorized Contacts must promptly notify the Help Desk when an Authorized User is terminated or changes roles in a way that changes the user's HEALTHeLINK application access requirements.

3.6.4 Acknowledge Terms of Use

HEALTHeLINK Authorized Users must acknowledge and accept terms of use of HEALTHeLINK applications prior to accessing the application. (SHIN-NY 3.3 §4.7.3)

3.7 Administration

3.7.1 Verify Access Need and Account Details

Participant Authorized Contacts must quarterly verify the accuracy of the user information of HEALTHeLINK Authorized Users and the need for access of each user. (SHIN-NY 3.3 §4.7.3)

3.8 Data Suppliers

3.8.1 Send Unfiltered Data

Data suppliers must send unfiltered data to HEALTHeLINK except when restricted by New York State laws or regulations.

3.9 Health Information Exchanges

3.9.1 Abide by Health Information Exchange Agreement Terms

HEALTHeLINK Authorized Users must abide by the terms of applicable health information exchange agreements. (SHIN-NY 3.3 §4.10.1)

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 participation. Under certain circumstances, violations of information security policy may give rise to civil and/or criminal liability.

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

1 Introduction

The statements in this policy document establish HEALTHeLINK's expectations with respect to security program design, planning, and operation.

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 Objectives

3.1.1 Protecting Sensitive Information

Directors must maintain a documented program to ensure the confidentiality, integrity, and availability of sensitive information. (HIPAA §164.306(a)(1))

3.1.2 Unauthorized Uses or Disclosures

Directors must implement safeguards to protect against unauthorized uses or disclosures of sensitive information. (HIPAA §164.306(a)(3))

3.1.3 Safeguards Against Threats

Directors must implement safeguards to protect against reasonably anticipated security threats. (HIPAA §164.306(a)(2))

3.1.4 Measures to Ensure Compliance

Directors must implement safeguards and practices to ensure that Authorized Users and workforce members comply with regulatory and contractual requirements. (HIPAA §164.306(a)(4))

3.1.5 Measures to Meet Regulatory Requirements

The Security Officer must ensure that security policies and practices are implemented to address regulatory requirements, directives, contracts, and applicable industry standards. (HIPAA §164.306(d)(1-3))

3.1.6 Report on Regulatory Requirements

The Security Officer must notify appropriate HEALTHeLINK management of non-compliance issues related to regulatory requirements, directives, and contracts.

3.1.7 Document Excluded Requirements

The Security Officer must document requirements from regulations and standards that are excluded from HEALTHeLINK's security program.

3.1.8 Workforce Collaboration

The Security Officer must communicate to the workforce the importance of cooperation and collaboration in complying with information security policies and identifying and addressing deviations.

3.2 Responsibilities

3.2.1 Protect Information and Assets from Access and Loss

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

3.2.2 Comply with Laws and Regulations

Workforce members 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.

3.2.3 Ensure Governance for Personnel Policies

The Security Officer must ensure that HEALTHeLINK's information security program's personnel-related policies, standards, procedures, and assessment processes address program purpose, scope, roles and responsibilities, and oversight.

3.2.4 Verify Delegated Security Tasks

Workforce members must ensure that assigned security tasks are correctly performed if delegated to another workforce member.

3.3 Oversight

3.3.1 Executive Oversight

Directors must actively support, maintain, and govern this information security program through allocation of appropriate funding and resources, assignment and acknowledgement of information security responsibility to workforce members, and participation in risk management and policy setting activities.

3.3.2 Security Committee

The Security 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.

3.3.3 Assess Overall Program

The Security Officer must, annually, direct an independent assessment of HEALTHeLINK's information security program covering executive oversight, communication to affected parties, resource allocation, conformance to regulatory and business requirements, security posture, suitability, adequacy, and effectiveness.

3.3.4 Security in Budgeting

Directors must establish discrete line item(s) for information security spending in program and budget planning.

3.4 Documentation

3.4.1 Security Program Documentation

The Security Officer must maintain HEALTHeLINK's policies, standards, and procedures in written form, which may be electronic. (HIPAA §164.316(b)(1)(i))

3.4.2 Policy Documentation

The Security Officer must document and maintain a record of changes to HEALTHeLINK's information security policies, standards, and procedures. (HIPAA §164.316(a))

3.4.3 Documentation Updates

The Security Officer must, annually, review information security documentation and update as needed based on environmental or operational changes. (HIPAA §164.316(b)(2)(iii))

3.4.4 Documentation Availability

The Security Officer must ensure that the individuals responsible for implementing the security program have access to policies, standards, and procedures. (HIPAA §164.316(b)(2)(ii))

3.4.5 Security Program Records

The Security Officer must maintain a written record of security actions, activities, or assessments performed to meet legal and regulatory requirements. (HIPAA §164.316(b)(1)(ii))

3.4.6 Documentation Retention

The Security Officer must retain information security documentation and records in accordance with HEALTHeLINK's document retention policies, and protect the documentation and records from unauthorized disclosure or modification. (HIPAA §164.316(b)(2)(i))

3.4.7 Provide Policies to Business Associates

The Operations Director must provide HEALTHeLINK's information security policies to business associates that handle HEALTHeLINK data, prior to providing system or data access.

3.4.8 Review Program Documentation for Clarity

The Security Officer must, annually, review information security documentation including policies, standards, and procedures to ensure that requirements are communicated clearly and address risk as intended.

3.4.9 Apply Frameworks

The Security Officer must incorporate appropriate industry framework(s) in the design and implementation of HEALTHeLINK's information security program.

3.4.10 Update Asset Management Processes

The Security Officer must, annually, review asset management processes and procedures and update, if necessary.

3.4.11 Required Procedures

The Security Officer must document and maintain formal procedures as required by regulatory requirements an applicable standards.

3.4.12 Maintain and Approve Procedures

The Security Officer must ensure that formal procedures are maintained with change control and an appropriate review and approval process.

3.4.13 Review Program Documentation based on Inputs

The Security Officer must incorporate specific feedback (e.g., audits, incidents, or corrective actions) subsequent to the prior review as an input to information security documentation reviews.

3.5 Program Assessment

3.5.1 Security Assessment

The Security Officer must, periodically, perform technical, physical, and administrative assessments of HEALTHeLINK's information security policies and practices, including when significant changes occur in HEALTHeLINK's environment or operations. (HIPAA §164.308(a)(8), 164.310(a)(2)(ii))

3.5.2 Assessment Documentation

The Security Officer must establish a process to document the findings, recommendations, and remediation decisions of each security program assessment. (HIPAA §164.308(a)(8))

3.5.3 Review Security Tools

The Security Officer must, periodically, review and update information security systems and tools, as appropriate.

3.5.4 Review Incident Response Processes

The Security Officer must, annually, conduct a review of incident response processes and update, if appropriate.

3.5.5 Align Security Responsibilities

The Security Officer must coordinate and align security roles between internal staff and external partners, including when using external services or systems.

3.6 Improvement

3.6.1 Security Program Maintenance

The Security Officer must, as needed, review implemented security measures to ensure that reasonable and appropriate protection is provided. (HIPAA §164.306(e))

3.6.2 Security Program Documentation Updates

The Security Officer must, as needed, update documentation when changes to security measures are made. (HIPAA §164.306(e))

3.6.3 Approval of Security Program Updates

The Security Officer must ensure that policies, standards, and procedures are appropriately approved when changes are made. (HIPAA §164.306(e))

3.7 Security Resources

3.7.1 Resources to Maintain Security

The Security Officer must identify and put in place additional resources, including maintenance and training, to ensure the proper operation of systems to prevent, detect, contain, and correct security violations. (HIPAA §164.308(a)(1)(i))

3.7.2 Acquiring Security Systems

The Security Officer must acquire and implement appropriate security systems to prevent, detect, contain, and correct security violations. (HIPAA §164.308(a)(1)(i))

3.7.3 Evaluating Security Systems

The Security Officer must evaluate security system requirements, based on the results of risk analysis, and identify appropriate acquisition requirements to prevent, detect, contain, and correct security violations. (HIPAA §164.308(a)(1)(i))

3.7.4 Inventory of Security Resources

The Security Officer must maintain an inventory of acquired security systems and resources. (HIPAA §164.308(a)(1)(i))

3.7.5 Threat Communication

The Security Officer must establish resources for communicating threat information to security personnel, management, and the workforce.

3.8 Identifying Exceptions

3.8.1 Identifying and Evaluating Policy Exceptions

The Security Officer must create a process for identifying, evaluating, and recording exceptions to HEALTHeLINK's information security policies.

3.9 Reviewing Exceptions

3.9.1 Reviewing Policy Exceptions

Directors must, regularly, review information security policy exceptions and validate that exceptions are only granted when appropriate.

3.10 Sanctions

3.10.1 Sanction Policy

Directors must apply appropriate sanctions against Authorized Users or, in accordance with HEALTHeLINK's human resources policies, against workforce members who do not comply with security policies. (HIPAA §164.308(a)(1)(ii)(C))

3.10.2 Disciplinary Actions

Directors must determine the appropriate disciplinary actions for policy violations, up to and including termination of employment and the pursuit of civil penalties and/or criminal liability.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to risk management.

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 General

3.1.1 Risk Management

Senior management must implement security measures to reduce risks and vulnerabilities to an acceptable level. (HIPAA §164.308(a)(1)(ii)(B))

3.2 Risk Analysis

3.2.1 Risk Analysis, Scope

The Security Officer must ensure that HEALTHeLINK's risk analyses identify and evaluate all systems that maintain sensitive information, including data moved with HEALTHeLINK and sent out of HEALTHeLINK. (HIPAA §164.308(a)(1)(ii)(A))

3.2.2 Risk Analysis, Periodic

The Security Officer must, annually, conduct an accurate and thorough risk assessment of potential security risks to sensitive information, considering likelihood and impact of a loss of confidentiality, integrity, and availability of sensitive information. (HIPAA §164.308(a)(1)(ii)(A))

3.2.3 Risk Analysis, Changes to Environment

The Security Officer must, as needed, conduct a risk analysis when changes occur within HEALTHeLINK's environment or operations, including after an incident or newly identified risk factor. (HIPAA §164.308(a)(1)(ii)(A))

3.2.4 Assess CMS-defined Controls

The Security Officer must, annually, 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.

3.2.5 Conduct Independent Assessments

The Security Officer must conduct an independent assessment of security and privacy controls every three years or with major system changes, aligned with a formal authorization to operate, if applicable.

3.2.6 Site Variability in Risk Analysis

The Security Officer must consider differences in threats, risks, physical and environmental hazards, data handling, and access factors for work locations, technologies, and third parties when assessing risk and selecting appropriate controls.

3.3 Review

3.3.1 Information System Activity Review

The Security Officer must, regularly, review records of information system, network, and physical activity such as audit logs, access reports, and incident reports and take appropriate actions when issues are found. (HIPAA §164.308(a)(1)(ii)(D))

3.3.2 Information System Activity Review, Record-keeping

The Security Officer must maintain a record of reviews of information system activity. (HIPAA §164.308(a)(1)(ii)(D))

3.3.3 Evaluate Threats of Adjacent Facilities

The Security Officer must consider threats associated with adjacent facilities and factors and threat including theft, fire, explosives, smoke, water, water supply failure, dust,

vibration, chemical effects, electrical supply interference, communications interference, electromagnetic radiation, vandalism, explosion, civil unrest, and other forms of natural or man-made disaster in HEALTHeLINK's risk management activities.

3.4 Vulnerability Management

3.4.1 Identify and Address Vulnerabilities

The Security Officer must implement a vulnerability identification, risk evaluation, and remediation process.

3.4.2 Collect Vulnerability Data

IT staff must ensure that vulnerability information is received and addressed commensurate with the potential level of risk.

3.4.3 Review Network Access Controls

IT staff must, annually, review all network access control rules to determine validity and use.

3.4.4 Test Security for Operational Changes

Directors must, as needed, require security testing of any new or substantially changed application or information processing facility prior to its deployment or putting it into operational mode.

3.5 Business Associates

3.5.1 Written Contract or Other Arrangement

The Executive Director must implement Business Associate Agreements to document that Business Associates safeguard sensitive information. (HIPAA §164.308(b)(3))

3.5.2 Inventory of Agreements

The Executive Director must maintain an inventory of HEALTHeLINK's Business Associate Agreements, including a record of security requirements addressed in each agreement. (HIPAA §164.308(b)(1))

3.5.3 Periodic Review of Agreements

The Executive Director must, periodically, review HEALTHeLINK's Business Associate Agreements to ensure that applicable requirements, appropriate to the nature and extent of system and information access, are addressed. (HIPAA §164.308(b)(1))

3.5.4 Business Associate Contracts, Compliance

The Executive Director must ensure that Business Associates are required to comply with applicable legal and regulatory requirements. (HIPAA §164.314(a)(2)(i)(A))

3.5.5 Business Associates, Breach Reporting

The Executive Director must ensure that Business Associates are required to promptly report security incidents and breaches of which they become aware. (HIPAA §164.314(a)(2)(i)(C))

3.5.6 Business Associates, Subcontractors

The Executive Director must ensure that subcontractors of Business Associates are required to comply with applicable legal and regulatory requirements. (HIPAA §164.314(a)(2)(i)(B))

3.5.7 Arrangements with Governmental Entities

The Executive Director must establish and maintain an inventory of HEALTHeLINK's arrangements with governmental entities. (HIPAA §164.314)

3.5.8 Assess Risk Before Granting Third-party Access

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

3.5.9 Validate Security Coverage in Statements of Work

The Operations Director must ensure that the security requirements of contracts and statements of work that involve sensitive or protected information conform with applicable regulatory requirements.

3.5.10 Validate Execution of Statements of Work

The Operations Director must ensure that contracts and statements of work that involve sensitive or protected information are executed by an authorized HEALTHeLINK representative.

3.6 Third Parties

3.6.1 Risk Assessment for Third Parties

Directors 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.

3.6.2 Evaluate Security Requirements Related to Third Parties

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.

3.6.3 Evaluate Security Practices of Third Parties when Necessary

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.

3.6.4 Evaluate Risk when Third Party Services Change

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.

3.6.5 Monitoring Third Parties

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

3.6.6 Notification of Third Party Service Changes

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

3.6.7 Coordinate Security Event Information with Third Parties

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

3.6.8 Define SLA Expectations

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

3.6.9 Identify System Locations

The Operations Director must require third party service providers of external information systems to identify the location of those systems.

3.6.10 Notify Third Parties of Security Program Changes

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

3.6.11 Monitoring Third Party Service Changes

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

3.7 Health Information Exchanges

3.7.1 Establish Health Information Exchange Agreements

The Executive Director 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.

3.7.2 Terms and Conditions in Agreements

The Executive Director 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.

3.7.3 Classification in Agreements

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

3.8 Service Delivery

3.8.1 Require Security Practices of Third-party Service Providers

The Operations Director must ensure that business associates implement appropriate information security controls, including policies, standards, and procedures, to protect HEALTHeLINK data.

3.9 Corrective Actions

3.9.1 Track Corrective Actions

The Security Officer must use an automated mechanism to track corrective actions.

3.10 Service Delivery

3.10.1 Avoid Use of Geographically Prohibited Facilities

The Security Officer must restrict the use of facilities used to process, transmit, or store HEALTHeLINK information based on geography in accordance with legal, regulatory, and contractual obligations.

3.11 Corrective Actions

3.11.1 Integrate Change and Risk Management

The Technology Director must integrate HEALTHeLINK's change and risk management processes to ensure that risks are addressed during changes to information systems, and that significant changes require a formal risk assessment and approval.

3.12 Insurance

3.12.1 Evaluation Insurance Coverage for Remote Work

The Operations Director must ensure that HEALTHeLINK maintains appropriate insurance coverage to address off-site equipment use and teleworking, if applicable.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to personnel security.

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 Official

3.1.1 Assign Security Responsibility

Directors must designate a security official with responsibility for the development and implementation of security policies. (HIPAA §164.308(a)(2))

3.1.2 Document the Security Officer's Job Duties

Directors must document the assigned responsibilities of the Security Officer and security staff and communicate those responsibilities to the entire organization. (HIPAA §164.308(a)(2))

3.2 Roles and Responsibilities

3.2.1 Document Workforce Security Responsibilities

The Operations Director must document significant security responsibilities and sensitive information access requirements in the job descriptions of workforce members, and communicate the security responsibilities during on-boarding. (HIPAA §164.308(a)(3))

3.2.2 Review Security in Job Descriptions

The Operations Director must, annually, review HEALTHeLINK's job descriptions to verify that security responsibilities are defined for appropriate roles.

3.2.3 Apply Separation of Duties for Security Activities

The Operations Director must apply the concept of 'separation of duties' when assigning security, testing, quality assurance, production, and auditing roles in job descriptions and access rights assignment.

3.2.4 Apply Separation of Duties if Collusion Risk

The Operations Director must apply the concept of 'separation of duties' in organizational processes to reduce the possibility of collusion.

3.2.5 Avoid Single Points of Failure

The Operations Director must assign multiple individuals to mission-critical and system support functions to avoid single points of failure.

3.2.6 Transfer Knowledge

The HR director must establish requirements for workforce members and third parties to transfer information important to ongoing HEALTHeLINK operations at the end of employment or services.

3.3 Workforce Verification

3.3.1 Experience Verification Requirements

Directors must establish requirements for verification of required experience and qualifications of workforce members who work with sensitive information. (HIPAA §164.308(a)(3))

3.3.2 Verification Records for Workforce Experience

The Operations Director must maintain a record of the verification of required experience and qualifications of workforce members who work with sensitive information. (HIPAA §164.308(a)(3))

3.3.3 Addressing Requirements

The HR director must review HEALTHeLINK's workforce verification process to confirm that security considerations are addressed, as indicated based on risk and regulatory factors, including as considered necessary character references, curriculum vitae accuracy, academic and and professional qualifications, employment history, residence, identity, and work eligibility.

3.3.4 Specialized Requirements

The Security Officer must review HEALTHeLINK's workforce verification process to determine if specialized screening is appropriate including health screening, drug screening, motor vehicle driving record screening, or criminal background checks.

3.3.5 Addressing Requirements in Role Changes

The Security Officer must confirm that HEALTHeLINK's workforce verification process includes consideration for changes in security-related requirements for current workforce members.

3.3.6 Third-party Workforce Screening

The Security Officer must review HEALTHeLINK's workforce verification process to confirm that non-employee workforce members receive appropriate screening in compliance with regulatory requirements.

3.3.7 Workforce Re-screening

The Security Officer must review HEALTHeLINK's workforce verification process and requirements to determine if periodic re-screening is appropriate (e.g., based on position criticality) and, if so, the criteria for rescreening.

3.3.8 Criteria and Limitations for Checks

The Security Officer must confirm that HEALTHeLINK's workforce verification process establishes the roles (e.g., single point-of-contact), circumstances, and both standard and role-specfic criteria for performing verification checks.

3.3.9 Screening Notification

The Security Officer must confirm that HEALTHeLINK's workforce verification process includes, if appropriate, notification steps to individuals prior to screening.

3.4 Employment Agreements

3.4.1 Address Policy in Employment Agreements

Directors must ensure that employee agreements are executed which contain language, appropriate to the nature and extent of system and information access, regarding adherence to HEALTHeLINK's security policy and expectations for safeguarding data during and following employment.

3.4.2 Clinical Access in Agreements

The Operations Director must ensure that employment agreements, if applicable to a clinical care position, specify rights of access to records and systems in the event of third-party claims.

3.4.3 Execute Agreements Before Access

Directors must ensure that employee agreements are executed before granting workforce members access to HEALTHeLINK systems and information.

3.5 Training and Awareness

3.5.1 Security Awareness and Training

The Security Officer must implement an initial and 'refresher' security awareness and training program for Authorized Users and the entire workforce, including management and technical staff, covering regulatory requirements as well as relevant current IT security topics. (HIPAA §164.308(a)(5)(i))

3.5.2 Security Reminders

The Security Officer must, regularly, provide security updates to the workforce, including regulatory requirements and specific information regarding the importance of protecting against malicious software. (HIPAA §164.308(a)(5)(ii)(A))

3.5.3 Specialized Security Training

The Security Officer must ensure that workforce members to whom additional security requirements apply receive additional, appropriate security training.

3.5.4 Participation in Security Forums

The Security Officer must identify and establish guidelines for participation in security, regulatory, and compliance relevant forums or professional associations to maintain information security knowledge, monitor threats, receive alerts and advisories, access specialist advice, and exchange information.

3.5.5 Training Record-keeping

The Operations Director must maintain a record of security training provided to a workforce member or Authorized User, and acknowledgment of the training where appropriate, for a minimum of seven years from the date of the member's termination from the workforce or the Authorized User's removal. (HIPAA §164.308(a)(5)(i))

3.5.6 Updating Security Awareness and Training Program

The Security Officer must review HEALTHeLINK's security awareness and training program, including testing and monitoring, and update as needed to address relevant and current information relating to security threats as well as workforce security responsibilities. (HIPAA §164.308(a)(5)(i))

3.5.7 Review of Security Awareness and Training Program

Directors must review and approve HEALTHeLINK's security awareness and training program. (HIPAA §164.308(a)(5)(i))

3.5.8 Provide Malware Awareness

The Security Officer must establish targeted security awareness to reduce HEALTHeLINK's exposure to malicious software.

3.5.9 Monitoring and Responding to Security Forums

The Security Officer must designate appropriate personnel to monitor relevant forums and information sources to identify and take appropriate action on newly discovered threats and vulnerabilities.

3.5.10 Automated Alert and Advisory Monitoring

IT staff must automate security alert and advisory monitoring and distribution where practical.

3.5.11 Review Security Forum Participation

The Security Officer must review and verify workforce participation in appropriate information security forums.

3.5.12 Distribute Security Advisories

The Security Officer must distribute security alerts, advisories, and directives to appropriate personnel.

3.5.13 Align Training with Risk Management

The Security Officer must validate that workforce security awareness and training aligns with HEALTHeLINK's risk management strategy and organizational priorities.

3.6 Prevention of Misuse of Information Assets

3.6.1 Notify Workforce of Monitoring

The Operations Director must notify workforce members that members' activities may be monitored for information security purposes.

3.6.2 Gain Consent Regarding Monitoring

The Operations Director must establish that workforce members have consented to monitoring for information security purposes.

3.6.3 Continued Security Obligations

The HR director must communicate HEALTHeLINK's expectations for continued safeguarding of sensitive information to workforce members at termination.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to physical security.

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 Facility Security

3.1.1 Facility Security Plan

The Operations Director must implement control and processes that limit physical access to HEALTHeLINK's information systems and facilities. (HIPAA §164.310(a)(2)(ii))

3.1.2 Access Control and Validation Procedures

The Security Officer must implement control and processes to validate access to HEALTHeLINK's facilities and information systems based on an individual's role or function. (HIPAA §164.310(a)(2)(iii))

3.1.3 Access Control and Validation Procedures, Visitors

The Security Officer must implement procedures to validate, monitor, and restrict access for visitors to HEALTHeLINK's facilities. (HIPAA §164.310(a)(2)(iv))

3.1.4 Access Control and Validation Procedures, Software Maintenance

The Security Officer must implement procedures to control access based on roles for testing and revision of software programs. (HIPAA §164.310(a)(2)(iv))

3.1.5 Maintenance Records

The Operations Director must create and retain documentation of security-related repairs and modifications to the facility. (HIPAA §164.310(a)(2)(iv))

3.1.6 Ensure Governance for Equipment Policies

The Security Officer must ensure that HEALTHeLINK's information security program's equipment maintenance-related policies, standards, and procedures address program purpose, scope, roles and responsibilities, and oversight.

3.1.7 Minimize Use of Secure Areas

Workforce members must avoid performing routine work in secure areas (e.g., data centers) when practical.

3.1.8 Recording in Secure Areas

Workforce members must not use photographic, video, or audio recording equipment in secure areas (e.g., data centers) unless authorized.

3.2 Workstation Security

3.2.1 Workstation Types

The Operations Director must establish a process to identify and classify workstations by type and location, with respect to access to sensitive information. (HIPAA §164.310(b))

3.2.2 Workstation Inventory

The Operations Director must, periodically, maintain an inventory of workstations classified by type and location. (HIPAA §164.310(b))

3.2.3 Workstation Use

The Operations Director must implement procedures for the configuration and use of workstations with access to sensitive information. (HIPAA §164.310(b))

3.2.4 Guidance for Workstation Security

The Operations Director must create and communicate guidance on how to maintain physical security for workstations with access to sensitive information. (HIPAA §164.310(b))

3.2.5 Guidelines for Food Near Workstations

The Operations Director must establish appropriate guidelines for eating and drinking in proximity to information assets.

3.3 Hardware and Media

3.3.1 Accountability

IT staff must maintain a record of the location of and persons responsible for hardware and electronic media containing sensitive information. (HIPAA §164.310(d)(2)(iii))

3.3.2 Device and Media Controls, Use Within Facilities

IT staff must monitor and control hardware and electronic media containing sensitive information as it is moved within HEALTHeLINK's facilities. (HIPAA §164.310(d)(1))

3.3.3 Device and Media Controls, Receipt and Removal

IT staff must monitor and control hardware and electronic media containing sensitive information as it enters and leaves HEALTHeLINK's facilities. (HIPAA §164.310(d)(1))

3.3.4 Disposal, Procedures

The Security Officer must implement procedures to securely destroy or erase hardware and electronic media containing sensitive information. (HIPAA §164.310(d)(2)(i))

3.3.5 Disposal, Recording

IT staff must maintain a record of the destruction or erasure of hardware and electronic media. (HIPAA §164.310(d)(2)(i))

3.3.6 Media Re-use

The Security Officer must implement procedures to securely erase sensitive information on hardware or electronic media prior to its reuse. (HIPAA §164.310(d)(2)(ii))

3.4 Protecting Against External and Environmental Threats

3.4.1 Ensure Governance for Physical Policies

The Security Officer must ensure that HEALTHeLINK's information security program's physical and environmental security-related policies, standards, and procedures address program purpose, scope, roles and responsibilities, oversight, and relevant health and safety regulations and standards.

3.5 Access and Identification

3.5.1 Require Visible Identification

The Operations Director must require visible identification for workforce members, visitors, and third parties and control distribution and return of temporary identification.

3.5.2 Review Physical Access Rights

The Operations Director must, quarterly, review physical access rights of workforce members.

3.6 Remote Work

3.6.1 Assess Remote Working Risks

The Security Officer must perform a risk analysis of the physical security of remote locations prior to authorizing teleworking.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to the acceptable use of information and information systems.

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 General

3.1.1 Use for Authorized Purposes

Workforce members must use and administer HEALTHeLINK's information and assets in an ethical manner and for authorized purposes only.

3.1.2 Sharing of Login Credentials

Workforce members must not share or disclose authentication credentials to another individual.

3.1.3 Unauthorized Testing

Workforce members must not attempt to perform unauthorized security testing including validating suspected weaknesses or accessing, modifying, or deleting information on information systems or services .

3.1.4 Disabling Security Controls

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

3.1.5 Accept Responsibility for Electronic Signatures

Workforce members must accept responsibility for actions taken under an assigned, unique electronic signature.

3.1.6 Avoid Access to Known Individuals

Workforce members must not access personal information of neighbors, colleagues, or relatives without a business need.

3.2 Information Handling

3.2.1 Protect Organizational Records

Senior management must ensure that organizational records are protected in accordance with applicable regulatory and contractual requirements.

3.2.2 Protect Sensitive Information from Disclosure

Workforce members 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.

3.2.3 Establish Classification Scheme

The Security Officer must establish a classification scheme for information resources based on the value of the resource, potential impact to HEALTHeLINK resulting from protection requirements including confidentiality, integrity, and availability and from adverse incidents, regulatory requirements, business needs and impacts, aggregation risk, and data form and technology factors.

3.2.4 Determine Classification

Senior management must determine the classification of information assets.

3.2.5 Roles and Classification Levels

The Security Officer must establish and communicate roles, responsibilities, and controls that safeguard information assets and processing facilities consistent with the associated classification level.

3.2.6 Safeguard According to Classification

Workforce members must be responsible for safeguarding information assets in accordance with HEALTHeLINK's information classification standard.

3.2.7 Review and Update Classifications

Senior management must, periodically, review and update the classification scheme and classification of information assets, including verifying asset responsibility based on process, activity, application, or data set and considering business changes, regulatory changes, changes from initial classification, and the impact of classification complexity on operations.

3.2.8 Methods of Handling Information

The Security Officer must enure that HEALTHeLINK's classification scheme addresses secure processing, storage, tranmission, declassification, and destruction.

3.2.9 List Approved Information Services

The Security Officer must maintain and communicate an inventory of HEALTHeLINK-approved information systems, external systems, network services, and networks for use and storage of HEALTHeLINK data, including any role- or condition-based criteria, limitations, or additional controls required.

3.2.10 Safeguard HIV-related Information

The Operations Director must establish appropriate requirements for labeling and handling of HIV-related information consistent with legal, regulatory, and industry guidelines.

3.2.11 Information Labeling

The Security Officer must establish printed, displayed, and electronically stored information labeling guidance aligned with HEALTHeLINK's information classification standard, including automated mechanisms and a process for formally documenting exempted media or hardware based on risk and location within a secure environment, if applicable.

3.2.12 Review Sensitive Output Labeling

The Security Officer must review the outputs of systems processing sensitive information to verify that outputs are labeled according to HEALTHeLINK's information classification standard.

3.2.13 Evaluate Third Party Classification Labels

Workforce members must safeguard information assets of third parties in accordance with HEALTHeLINK's information classification standard, taking care to interpret differences in classification labeling.

3.2.14 Unapproved External Systems

Workforce members must not store HEALTHeLINK data on unapproved external systems or use unapproved external systems for HEALTHeLINK data processing.

3.3 Mobile and Remote Access

3.3.1 Establish Security Requirements for Mobile Devices

Directors must establish and communicate requirements around the use of mobile devices and communications.

3.3.2 Mobile and Remote Access Security

Directors must establish and communicate requirements for remote access and workforce members working remotely.

3.3.3 Restrictions on Mobile Device Sharing

Workforce members must not allow an unauthorized individual to use a laptop or any other organization-provided mobile device.

3.3.4 Report Loss or Theft of Mobile Devices

Workforce members must immediately report the loss, theft, or exchange of any mobile device that may contain organization information.

3.3.5 Protect Equipment Off-Premises

Workforce members must protect HEALTHeLINK-provided laptops and other devices by avoiding leaving devices unattended, following manufacturer recommendations for protection, and, where practical, obscuring the identity of devices in luggage and carrying as hand luggage when travelling.

3.3.6 Use Only Authorized Equipment

Workforce members must not remove equipment or use systems and applications to remotely access HEALTHeLINK information and systems, without HEALTHeLINK authorization .

3.4 Data Protection and Privacy of Covered Information

3.4.1 Avoid Storing Sensitive Data

Workforce members must avoid storing sensitive information when not necessary.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to technical security.

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 Inventory of Assets

The Technology Director must identify and maintain a list of information assets, including classification and asset ownership, if applicable, and an indication of assets deemed critical to HEALTHeLINK or at a high risk of loss or theft.

3.1.2 Verify Installed Software

The Technology Director must establish procedures to periodically verify that only approved software is installed on HEALTHeLINK's systems.

3.1.3 Review and Authorize Technologies

IT staff must establish a review and authorization process for new or changed information technologies, communications, or services.

3.1.4 Security Involvement in System Evaluation

IT staff must notify the Security Officer of information technologies, communications, or services either planned or under evaluation.

3.1.5 Monitor System Performance

IT staff must monitor the utilization, performance, and stability of information technology resources to support capacity management and incident response.

3.1.6 Document Systems and Connections

The Technology Director must maintain documentation of authorized HEALTHeLINK information systems and both internal and external interconnections, including interface characteristics (e.g., protocol), security requirements, and type of data transmitted as well as business or security implications.

3.1.7 Inventory External Systems

The Technology Director must maintain an inventory of authorized external information systems.

3.1.8 Document Use of External Systems

The Technology Director must document the limitations and requirements for use of authorized external information systems, and the classifications of data permitted on each.

3.1.9 Review and Update Inventory

The Technology Director must, annually, review and update the asset inventory and, if applicable, update the asset ownership when a listed owner is no longer responsible for an asset.

3.1.10 Investigate Inventory Discrepancies

The Technology Director must evaluate changes identified in an asset inventory review and investigate discrepancies, if found.

3.1.11 Consider Capacity in Planning

The Technology Director must consider outputs of utilization, performance, and stability monitoring including current use, logging storage requirements, trends, anticipated business changes, and tuning to improve availability and performance in planning for new and existing systems and services.

3.1.12 Review Capacity Monitoring

The Technology Director must, regularly, review storage capacity to avoid impacts to system performance and availability.

3.1.13 Recording Off-site Asset Authorization

The Technology Director must maintain a record of off-site asset authorizations and/or restrictions, including time limits and returns if applicable, for the workforce and applicable third parties.

3.2 Authentication

3.2.1 Review of Authentication Methods

The Technology Director must, periodically, review the implemented authentication methods for systems maintaining sensitive information and evaluate alternative authentication methods. (HIPAA §164.312(d))

3.2.2 Person or Entity Authentication

The Technology Director must select and implement mechanisms to authenticate individuals or entities accessing sensitive information stored on information systems. (HIPAA §164.312(d))

3.2.3 Testing of Authentication Methods

The Technology Director must, periodically, ensure that the authentication methods used by systems maintaining sensitive information are tested. (HIPAA §164.312(d))

3.3 Passwords

3.3.1 Password Management, Set Standards

The Security Officer must implement standards for Authorized Users and workforce members to securely create, modify, and safeguard passwords. (HIPAA §164.308(a)(5)(ii)(D))

3.3.2 Password Management, Follow Standards

Workforce members must follow password standards when creating, changing, and safeguarding passwords. (HIPAA §164.308(a)(5)(ii)(D))

3.3.3 Password Management, System Configuration

IT staff must configure systems to require and enforce passwords that conform to HEALTHeLINK's password standards. (HIPAA §164.308(a)(5)(ii)(D))

3.4 Encryption

3.4.1 Encryption and Decryption of Stored Data

IT staff must configure information systems to encrypt sensitive information when stored electronically. (HIPAA §164.312(a)(2)(iv))

3.4.2 Documentation of Encryption Mechanisms

The Security Officer must document the configuration of encryption components including type(s) of encryption used, protection of keys (i.e., to avoid modification, loss, or destruction), access to keys, and key management. (HIPAA §164.312(a)(2)(iv))

3.4.3 Limit Term of PKI Certificates

The Technology Director must ensure that PKI-based certificates are configured to be valid for no more than a three years.

3.4.4 Validate Token Security

The Technology Director must ensure that hardware token-based authentication mechanisms, if used, meets generally acceptable minimum security requirements.

3.4.5 Encryption of Media

IT staff must configure removable media, where approved, to encrypt sensitive information when stored.

3.5 Transmission

3.5.1 Encryption of Transmitted Data

The Technology Director must implement mechanisms to encrypt sensitive information when it is transmitted over a network not controlled by HEALTHeLINK. (HIPAA §164.312(e)(2)(ii))

3.5.2 Transmission Security, Integrity Controls

The Technology Director must implement mechanisms to ensure that electronically transmitted sensitive information is not modified without detection. (HIPAA §164.312(e)(2)(i))

3.5.3 Session Authenticity

The Technology Director must ensure that encryption mechanisms for transimitting sensitive information protect the integrity and authenticity of network sessions using industry-accepted algorithms.

3.6 Data Integrity

3.6.1 Integrity

The Technology Director must implement procedures to prevent improper alteration or destruction of sensitive information stored on information systems. (HIPAA §164.312(c)(1))

3.6.2 Mechanism to Authenticate Sensitive Data

The Technology Director must implement mechanisms to validate that sensitive information is not altered or destroyed without authorization. (HIPAA §164.312(c)(2))

3.7 Malicious Software

3.7.1 Protection from Malicious Software, Detection

The Security Officer must implement systems that detect and provide alerts when malicious software is detected. (HIPAA §164.308(a)(5)(ii)(B))

3.7.2 Protection from Malicious Software, Prevention

The Security Officer must implement systems and processes to prevent compromise by malicious software. (HIPAA §164.308(a)(5)(ii)(B))

3.7.3 Detect and Remediate Malware

IT staff must establish mechanisms on systems attacked by malware that detect and remediate malicious software.

3.7.4 Review Use of Anti-Malware Defenses

The Security Officer must, periodically, review malware threats to determine if changes to anti-malware defenses are needed, including use of anti-malware defenses on systems not previously vulnerable to malware attack.

3.8 Monitoring

3.8.1 Log-in Monitoring, Recording Log-ins

IT staff must create a record of successful and attempted log-ins. (HIPAA §164.308(a)(5)(ii)(C))

3.8.2 Log-in Monitoring, Reviewing Log-in Records

The Security Officer must review the records of log-in attempts and assess any identified discrepancies. (HIPAA §164.308(a)(5)(ii)(C))

3.8.3 Monitor Continuously

The Security Officer must implement continuous monitoring mechanisms for HEALTHeLINK's information systems, including security and logging systems.

3.9 Security Audit

3.9.1 Audit Controls, Select Activities to Audit

The Security Officer must determine security-related activities that must be tracked or audited. (HIPAA §164.312(b))

3.9.2 Audit Controls, Recording of Activities

IT staff must implement mechanisms that record security-related activities in information systems maintaining sensitive information. (HIPAA §164.312(b))

3.9.3 Privileged Account Auditing

The Security Officer must implement controls to monitor and record the use of system and privileged accounts and the actions taken by Authorized Users and workforce members with elevated privileges.

3.9.4 Audit Controls, Review of Activities

The Security Officer must implement automated or manual processes to examine security-related activities in information systems maintaining sensitive information. (HIPAA §164.312(b))

3.9.5 Communication of Audit Activities

The Security Officer must communicate the audit policy and approach to workforce members and Authorized Users. (HIPAA §164.312(b))

3.9.6 Maintenance of Logging Data

The Executive Director must establish a defined period of time (reference “SP-013 Record Retention”) for which audit logs must be retained to support incident and risk management activities.

3.9.7 Integrity of Logging Data

IT staff must ensure the generation and integrity of audit logs recording user activity and information security events by information systems including but not limited to servers, workstations and endpoints, networking devices, and applications.

3.10 Certified Applications

3.10.1 Authorization for Certified Applications

IT staff must ensure that access to sensitive information by Certified Applications is permitted in accordance with SHIN-NY encryption and other authorization requirements.

3.10.2 Authentication for Certified Applications

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

3.10.3 Access Control for Certified Applications

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

3.11 Control of Operational Software

3.11.1 Restrict Unapproved Software

IT staff must prevent the installation of unapproved software on HEALTHeLINK systems.

3.11.2 Check for Unauthorized Software

IT staff must inspect HEALTHeLINK's systems for unauthorized software.

3.12 Electronic Commerce Services

3.12.1 Maintain Security for E-commerce

The Technology Director must take appropriate steps to maintain the confidentiality and integrity of electronic commerce transactions.

3.13 Electronic Messaging

3.13.1 Avoid Faxing

Workforce members must refrain from sending sensitive information via facsimile when delivery by more secure channels is practical.

3.14 Inventory of Assets

3.14.1 Review Inventories to Avoid Duplication

The Technology Director must review HEALTHeLINK's inventories to confirm that information is not unnecessarily duplicated in multiple inventories.

3.14.2 Review Inventories for Consistency

The Technology Director must review HEALTHeLINK's inventories to validate that information is consistent across inventories.

3.14.3 Manage Assets Assigned to Third Parties

The Operations Director must define the process for assigning, monitoring, tracking, and returning assets assigned to third parties in the agreements with third parties.

3.14.4 Manage Assets Assigned to Volunteers

The Operations Director must define the process for assigning, monitoring, tracking, and returning assets assigned to volunteers in the agreements with volunteers.

3.14.5 Define Data Erasure Process

The Technology Director must document the process for erasing data from magnetic media prior to transfer, exchange, or disposal.

3.14.6 Update Asset Inventory

The Technology Director must, annually, direct an inventory of information assets and update the list of information assets, if necessary.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to access control.

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 General

3.1.1 Configure Controls to Restrict Access

IT staff must establish technical access controls for electronic information systems that store, process, or transmit sensitive data including sensitive information to allow access only to those persons or software programs that have been granted access rights. (HIPAA §164.312(a)(1))

3.1.2 Document Workforce Access Levels

The Security Officer must establish and formally document that levels of access of Authorized Users and workforce members are appropriately approved and communicated. (HIPAA §164.308(a)(3))

3.1.3 Review and Approve Workforce Access Levels

IT staff must establish a document identifying appropriate levels of access for Authorized Users and workforce members, based on roles, to information systems that house sensitive information. (HIPAA §164.308(a)(3))

3.1.4 Periodic Review of Access Control Processes

The Security Officer must periodically review user access procedures and practices and update as needed to ensure that access controls are consistent with policy. (HIPAA §164.312(a)(1))

3.2 Role Based Access Control

3.2.1 Define Roles and Responsibilities in Job Descriptions

The Operations Director must define information security roles and responsibilities in job descriptions and correlate with job function. (HIPAA §164.308(a)(3))

3.2.2 Establish Role-based Categories

The Operations Director must establish role-based categories of Authorized Users and workforce members to be used in setting access rights to sensitive data including sensitive information. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.2.3 Correlate Roles to Access Levels

IT staff must determine the standard level of access to sensitive information for each category of Authorized User or workforce member, to implement role-based access control in order to restrict access to only authorized users and uses. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.2.4 Assign Access Categories to Each User

The Operations Director must assign a role-based security category to each Authorized User or workforce member. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.3 Need to Know

3.3.1 Evaluate User Needs

Senior management must perform an analysis of user needs and workloads to establish appropriate access controls. (HIPAA §164.312(a)(1))

3.3.2 Document Business Needs for Access

The Security Officer must determine and formally document that levels of access are granted based on business need. (HIPAA §164.308(a)(3))

3.3.3 Grant No More Access than Required

IT staff must grant only appropriate levels of access to sensitive information to Authorized Users and workforce members, and no more access than is required for an Authorized User's work duties. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.3.4 Configure Access Based on Need to Know

IT staff must allow Authorized Users and workforce members to have appropriate access to data (e.g., sensitive information) to perform work duties, based on "need to know". (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.3.5 Assign Access Based on Job Duties

The Security Officer must implement a process to ensure that Authorized Users and workforce members are assigned appropriate level of access to sensitive data including sensitive information based on job duties. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.3.6 Restrict Access When Not Required

IT staff must prevent Authorized Users and workforce members from gaining access to data that is not necessary to work duties. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.3.7 Authorization and/or Supervision by Need

Senior management must evaluate business requirements to determine and approve appropriate security and access levels based on an Authorized User's or workforce member's job function. (HIPAA §164.312(a)(1), 164.308(a)(3)(ii)(A))

3.4 Credentials

3.4.1 Use Only Issued Accounts

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

3.4.2 Use Complex Passwords

Workforce members must use passwords that are complex, are difficult to guess, and are not contained in a dictionary. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.4.3 Do Not Share Passwords

Workforce members must not share user IDs, passwords, remote access tokens, card keys, or other individually assigned credentials or authentication tools. (HIPAA §164.310)

3.5 Information Access Management

3.5.1 Establish Access Controls for Information Systems

The Security Officer must establish procedures for granting access to sensitive information through a workstation, transaction, program, process, or other mechanisms. (HIPAA §164.308(a)(3), 164.308(a)(4)(ii)(b))

3.5.2 Establish Procedures for Access Controls

The Security Officer must establish procedures to authorize access and to document, review, and modify a user's right of access to a workstation, transaction, program, or process. (HIPAA §164.308(a)(4)(ii)(c))

3.5.3 Communicate Role Changes

The Operations Director must promptly communicate the change to the Help Desk, whenever a workforce member changes roles or is terminated. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.5.4 Review Access Rights when Roles Change

IT staff must ensure that the allocation of access to workforce members is reviewed and updated when members change positions, including removing access when it is no longer required. (HIPAA §164.312(a)(1))

3.5.5 Deactivate Access on Termination

IT staff must deactivate a workforce member's unique user ID promptly upon the member's termination, including voluntary and involuntary termination, to prevent further access to sensitive data including sensitive information by the member. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e), 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.5.6 Recover Access Mechanisms on Termination

IT staff must recover access control devices and deactivate computer access upon termination of employment. (HIPAA §164.308(a)(3)(ii)(c))

3.5.7 Maintain a Record of Access Rights Changes

IT staff must maintain a record of the user and privileged access grants, changes, and removals and perform regular reviews that such changes have been appropriately made.

3.5.8 Termination Process

The Operations Director must establish appropriate guidance for the termination process for workforce members including addressing security-related topics, return of property, revocation of access, knowledge and information transfer, and provision of access to records.

3.5.9 Responsibilities After Termination

The Operations Director must establish appropriate guidance for communication to workforce members during the termination process regarding ongoing security requirements and legal responsibilities, confidentiality requirements, and continuing terms and conditions.

3.6 Records

3.6.1 Maintain a Record of Access Approval

IT staff must maintain a record of approval or verification of access to sensitive information. (HIPAA §164.308(a)(3))

3.7 Audit and Review

3.7.1 Restrict Access to Audit Logs

IT staff must restrict access to audit logs and tools to only those explicitly authorized personnel with an operational requirement to access the logs.

3.7.2 Document Audit Authorizations

The Security Officer must document that personnel authorized to access audit logs are authorized by applicable system owners.

3.7.3 Assess Audit Logging Systems

The Security Officer must, annually, perform a risk analysis of audit logging systems.

3.8 Access Reports

3.8.1 Document Access Report Requests

The Security Officer must document requests from consumers or third parties for Access Reports permitted by applicable laws and regulations.

3.8.2 Create and Maintain Access Report Records

The Security Officer must create and maintain records of requests for and processing of Access Reports.

3.8.3 Report on Access Report Requests to Operating Committee

The Executive Director must, periodically, report to the Operating Committee on Access Report requests and processing.

3.9 Control of Operational Software

3.9.1 Restrict Support Provider Access

Directors must provide physical or logical access for support providers only when required for support.

3.9.2 Gain Approval of Support Provider Access

IT staff must obtain management approval prior to granting physical or logical access to support providers.

3.9.3 Monitor Support Providers

IT staff must monitor support providers when provided physical or logical access to HEALTHeLINK systems or facilities.

3.10 Privilege Management

3.10.1 Assign Normal-use IDs to Administrators

The Technology Director must assign user IDs with elevated privileges, separate from IDs provided for normal use, to system and application administrators.

3.10.2 Avoid Use of Elevated-privilege Accounts

IT staff must refrain from using user IDs with elevated privileges for normal use.

3.10.3 Provide Guidance for Information Sharing

The Security Officer must provide guidance for authorized workforce members to share information with business partners, where discretion is allowed.

3.11 User Identification and Authentication

3.11.1 Verify the Identity of Individuals

Help Desk staff must identify individuals prior to performing activities that have information security implications (e.g., password resets).

3.11.2 Verify Identities when Issuing Electronic Signatures

The Technology Director must verify the identify of an individual before establishing, assigning, or certifying the individual's electronic signature.

3.11.3 Use Multi-factor for Remote Access

The Technology Director must implement multi-factor authentication for remote access to HEALTHeLINK's internal network.

3.11.4 Use Multi-factor for Administrator Access

The Technology Director must implement multi-factor authentication for administrative access to privileged accounts of HEALTHeLINK's information systems.

3.11.5 Use Multi-factor for High-security Systems

The Technology Director must implement multi-factor authentication for access to HEALTHeLINK systems storing or processing sensitive or protected information.

3.12 User Authentication for External Connections

3.12.1 Encrypt Dial-up Connections

The Technology Director must restrict the use of unencrypted dial-up connections.

3.13 User Password Management

3.13.1 Acknowledge Password Receipt

IT staff must require acknowledgment of password receipt when receipt of a password cannot otherwise be confirmed.

3.13.2 Change Default Passwords at Setup

IT staff must change the passwords to default accounts during system configuration.

3.13.3 Require New Password at First Login

IT staff must configure systems to require a new password at first login after a password reset.

3.13.4 Change Password if Compromised

IT staff must change an account's password if the account is known or suspected to be compromised.

3.13.5 Protect PINs

Workforce members must protect PINs and other ID codes similarly to passwords.

3.13.6 Reuse Only if Authorized

Workforce members must not use the same password on multiple HEALTHeLINK systems except where single sign-on (SSO) is enabled or authorized to use the same quailty password on HEALTHeLINK systems of a similar security level.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to IT acquisition, development, and maintenance.

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 Documentation

3.1.1 Document Management

The Technology Director must establish a document management system that enables controlled access to information technology and operational documentation, and provide access to the system to workforce members as appropriate.

3.1.2 Maintain System Guidance

The Technology Director must maintain information technology documentation (e.g., user and administrator guides) for information systems, where available and not readily available online.

3.1.3 Document Unavailable Guidance

The Technology Director must maintain links to online information technology documentation, as appropriate, and keep a record of systems for which documentation is not available.

3.1.4 Manage Documentation Access

The Security Officer must review access lists for the document management system for information technology and operational documentation and verify that the access list is appropriate and aligned with data classification requirements.

3.2 Change Management

3.2.1 Change Approval Process

IT staff must implement a change management approval process for changes to information processing facilities, systems, and software, and changes to the standards and guidelines supporting these technologies.

3.2.2 Security Review of Changes

IT staff must request a review from the Security Officer for any changes to the standards and guidelines that may affect the security of an information system.

3.2.3 Review Software Deployment for Authorization

The Security Officer must, periodically, review software deployment processes to verify that risks related to unauthorized access or changes are addressed.

3.3 Application Development

3.3.1 Employ Security Throughout Development Life Cycle

The Technology Director must establish and incorporate information security requirements and controls throughout all phases of the deployment and maintenance lifecycle for new information processing facilities and applications as well as those undergoing revisions.

3.3.2 Follow Policies in Application Development

IT staff must ensure that applications implement HEALTHeLINK's policies and standards to preserve the integrity and prevent unauthorized disclosure of sensitive information.

3.3.3 Separate System Environments

IT staff must maintain separate development, testing, and production environments and supporting information services and resources, including controls to address security (e.g., segregated networks) and operational issues.

3.3.4 Security Guidance for Application Development

The Security Officer must establish security requirements and guidance for applications that support the processing or facilitate access to sensitive information.

3.3.5 Security Guidance for Data Storage and Transmission

The Security Officer must establish standards and guidelines for the protection of stored and transmitted information including confidentiality, integrity, availability, and non-repudiation.

3.3.6 Restrict Data in Test Environments

The Security Officer must restrict the storage and use of sensitive and protected information in test environments.

3.4 Networks

3.4.1 Authentication Standards

IT staff must implement an authentication standard for all remote connections including workforce members and third parties.

3.4.2 Configure Electronic Messaging to Prevent Malware

IT staff must ensure that electronic messaging systems are configured to detect and protect against malicious software.

3.4.3 Information Exchange Standards

The Technology Director must establish and communicate requirements for the secure exchange of information both internally and with third parties, including in third party exchange agreements where applicable.

3.5 Systems

3.5.1 Implement Baseline Configurations for Systems

IT staff must establish and implement standards for baseline configuration for deployed information processing technology including workstations, servers, network devices, applications, and mobile computing devices.

3.5.2 Configure Systems Securely when Deployed

IT staff must ensure that documented standard configurations are applied when information systems are deployed.

3.5.3 Restrict Access to System Settings

IT staff must establish and implement controls to restrict access to system programs or configuration files.

3.5.4 Protect Network Devices

IT staff must establish and implement physical and logical controls to protect the configuration of network infrastructure devices.

3.5.5 Data Loss Prevention

IT staff must implement processes to identify and prevent leakage of sensitive information.

3.5.6 Validate Secure Configuration During Assessments

The Security Officer must review the results of technical assessments to validate that HEALTHeLINK's secure configuration standards are applied to information systems.

3.5.7 Manage Secure Baselines

IT staff must maintain automated mechanisms to centrally manage, apply, and verify secure configuration settings.

3.5.8 Validate Secure Baselines to HHS Requirements

The Security Officer must, annually, validate that HEALTHeLINK's secure configuration standards conform with HHS secure configuration guidelines.

3.5.9 Communicate Baseline Configuration Requirements

IT staff must communicate HEALTHeLINK's standards for baseline configuration to third parties connecting to HEALTHeLINK networks.

3.5.10 Test Third Party Device Security

IT staff must evaluate the security of third party systems, via a vulnerability scan or similar method, prior to allowing connection to a HEALTHeLINK network.

3.5.11 Assess Risk for Third Party Devices

IT staff must perform a risk analysis and document risk treatment decisions, if applicable, for third party systems prior to connection to a HEALTHeLINK network.

3.5.12 Maintain Authority to Connect

The Security Officer must maintain required aspects of any CMS-granted Authority to Connect including updates at three years or significant change, change in sensitivity, change in regulations, violations or incidents, and update on expiration.

3.6 Control of Operational Software

3.6.1 Plan Migration for Unsupported Systems

IT staff must establish a migration plan for systems that are no longer supported by a vendor.

3.6.2 Review Unsupported System Migration Plans

The Security Officer must review and approve migration plans developed to migrate from systems when vendor support ends.

3.6.3 Define Roll-back Plans

IT staff must document roll-back plans before making changes that may affect the security or availability of HEALTHeLINK systems.

3.6.4 Log Updates

IT staff must maintain an audit log of updates to operating systems and applications.

3.7 Equipment Maintenance

3.7.1 Meet Vendor-recommended Intervals for Maintenance

The Operations Director must ensure that maintenance personnel and providers perform maintenance at vendor-recommended intervals.

3.7.2 Meet Insurance Requirements for Maintenance

The Operations Director must ensure that maintenance personnel and providers perform maintenance as required by insurance policies and HEALTHeLINK's business requirements.

3.7.3 Prevent Data Storage on Maintenance Equipment

The Operations Director must restrict the unauthorized storage or removal of sensitive or protected information on maintenance equipment.

3.7.4 Clear Data Before Maintenance

IT Staff must clear sensitive or protected information from equipment prior to maintenance, unless authorized.

3.7.5 Verify Security After Maintenance

IT Staff must verify the operation of security controls following information system maintenance.

3.7.6 Maintain Maintenance Records

IT Staff must maintain records of information system maintenance activities.

3.8 Input Data Validation

3.8.1 Document Input Validation and Error Checking

IT staff must document the input validation and error checking features of HEALTHeLINK-developed applications.

3.8.2 Review Security in Application Development Processes

The Security Officer must, periodically, review and update, if appropriate, HEALTHeLINK application development processes and standards .

3.9 Security Requirements Analysis and Specification

3.9.1 Align Security with Risk Impact

The Security Officer must ensure that applied safeguards are aligned with the value of, and the potential for adverse impact to, information assets.

3.9.2 Include Security in Acquisition

The Security Officer must establish appropriate security requirements as part of a formal acquisition process for commercial products and services.

3.9.3 Include Security in Third-party Agreements

The Security Officer must include appropriate security requirements in agreements associated with purchased commercial products and services.

3.9.4 Evaluate Risk During Acquisition

The Security Officer must evaluate the risk associated with security gaps identified during the acquisition process for commercial products, prior to purchase.

3.9.5 Disable Risky Functionality in Products

IT staff must disable or mitigate additional functionality included in purchased commercial products, if the functionality increases risk.

3.9.6 Separate User and Management Functions

IT staff must maintain a separation between user functionality and information systems management functionality.

3.9.7 Include Security in Service Provider Contracts

The Operations Director must include appropriate contractual requirements related to security and privacy when engaging information system providers.

3.9.8 Prevent User-to-user Data Exposure

The Technology Director must ensure that system acquisition and design processes address requirements to prevent information accessed by one user from being accessed by a subsequent user.

3.9.9 Review Security in System Design

The Security Officer must obtain and evaluate control design and implementation information from the developers of HEALTHeLINK's information systems.

3.9.10 Incorporate Availability during Acquisition

The Technology Director must incorporate availability and redundancy requirements in information systems development and acquisition processes.

3.9.11 Consider Security in System Requirements

The Technology Director must consider information security and data classification when developing system requirements, obtaining appropriate management approvals.

3.9.12 Define Enterprise Architecture

The Technology Director must establish an enterprise architecture for HEALTHeLINK's information systems, taking into account information security plans and risk, and update the enterprise architecture or security program as changes occur.

3.9.13 Review and Approve Plans

The Security Officer must review and approve information security plans for HEALTHeLINK's systems prior to system implementation.

3.10 Outsourced Software Development

3.10.1 Establish Source Code Ownership and Security

The Operations Director must establish agreements covering source code ownership and security when outsourcing software development.

3.10.2 Cover Security in Outsourced Software Agreements

The Operations Director must include appropriate contractual requirements related to security, change management, flaw tracking and resolution, and reporting to HEALTHeLINK when outsourcing software development.

3.11 Software Licensing

3.11.1 Maintain Licensing Agreements

The Technology Director must ensure that appropriate software licensing is acquired and maintained for information systems and applications.

3.11.2 Comply with Licensing

The Technology Director must ensure that information systems and applications are used in compliance with applicable software licensing.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to incident reporting.

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 Reporting

3.1.1 Prompt Incident Reporting

Workforce members must promptly report any known or suspected security incident, security weakness, or system fault to the Help Desk.

3.1.2 Cooperation During Investigations

Workforce members must cooperate with Management and members of the Incident Response Team (IRT) during reporting and incident response activities.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to incident management.

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 Response Authority

3.1.1 Single Point of Authority for Incident Response

Senior management must designate a single point of authority responsible for incident response.

3.2 Incident Assessment and Escalation

3.2.1 Prompt Review of Reports

The Security Officer must review each security event promptly to determine if it constitutes a security incident.

3.2.2 Identify Root Causes

The Security Officer must evaluate each security event to determine if the event should be consolidated with other events related to a suspected threat, attack, vulnerability, or malware.

3.2.3 Classify and Declare Incidents

The Security Officer must formally declare a security incident for any security event that is determined to have an adverse impact. (HIPAA §164.308(a)(6)(ii))

3.3 Incident Response

3.3.1 Convene an Incident Response Team

The Security Officer must convene an IRT composed of members appropriate to the scale and nature of the incident promptly following declaration of a security incident.

3.3.2 Promptly Contain Incidents

Incident Response Team members must make a prompt determination of the scope and impact of a security incident and direct the isolation of computers, networks, or applications as appropriate in order to minimize the adverse impact of an incident.

3.3.3 Contain Incidents and Identify Resolutions

Incident Response Team members must coordinate the response to security incidents, verify that the response is effective, escalate response if appropriate, and make a recommendation to the Security Officer for remediation of the event.

3.3.4 Engage Third Parties if Appropriate

Incident Response Team members must involve third parties for forensic examinations in order to ensure the courtroom admissibility of evidence or to otherwise assist in the resolution of an incident, including for internal disciplinary action, when appropriate or when required by applicable laws, regulations, or standards.

3.3.5 Notify Appropriate Parties

Incident Response Team members must notify appropriate personnel and, if applicable, external parties such as law enforcement or other entities in accordance with applicable laws, regulations, and standards.

3.3.6 Preserve Evidence During Investigation

Incident Response Team members must evaluate the nature of the security incident and, if appropriate, direct the preservation of information or systems related to the

incident, in accordance incident response procedures, internal disciplinary processes, and applicable laws, regulations, and standards.

3.3.7 Avoid Unauthorized Disclosures Regarding Incidents

Incident Response Team members must not provide information related to a security incident to any individual not specified in the incident response procedures without explicit authorization from the Security Officer.

3.3.8 Maintain Response Team Contacts

The Security Officer must, annually, review and update key contact information for HEALTHeLINK's incident response plans.

3.3.9 Maintain Law Enforcement Contacts

The Security Officer must maintain a list of law enforcement contacts for use in incident response, investigation, and reporting including known or suspected violations of law.

3.3.10 Verify Evidence Preservation

The Security Officer must verify that HEALTHeLINK's incident response processes conform with applicable standards regarding management of admissible evidence.

3.4 Incident Resolution

3.4.1 Close Security Events when Resolved

The Security Officer must declare security incidents closed following verification and update records associated with the incident to reflect resolution. (HIPAA §164.308(a)(6)(ii))

3.4.2 Implement Remediation when Appropriate

Incident Response Team members must identify actions to remediate security incidents, refer the actions to the appropriate personnel, and monitor remediation activity to ensure that the actions are promptly and effectively applied. (HIPAA §164.308(a)(6)(ii))

3.4.3 Review Incident Response Results

The Security Officer must review results to ensure that a security incident has been resolved when remediation actions related to a security incident are complete.

3.5 Detection Systems

3.5.1 Configure Systems to Detect Incidents

The Security Officer must ensure that security systems with the capability to detect potential security incidents are configured to report the event in accordance with this policy and appropriate standards related to recording of admissible evidence.

3.5.2 Validate False Positives in Malware Alerts

The Security Officer must validate that security events are not 'false positives' to avoid adverse impacts to system availability.

3.6 Incident Reporting

3.6.1 Maintain Record of Incident Reports

Help Desk staff must record each security event using an Operational Incident Report (OIR) form and shall review the reported event according to defined procedures in order to determine if the event should be referred for incident response.

3.6.2 Allow Anonymous Event Reporting

The Operations Director must establish and communicate a mechanism for anonymous security event reporting.

3.6.3 Facilitate Event Reporting

The Operations Director must establish mechanism(s) for security event reporting that are easy-to-use, available, and accessible to internal and appropriate external parties.

3.7 Incident Response Management

3.7.1 Reporting and Escalation

The Security Officer must ensure that there is a method, including policies, standards, and procedures, for reporting and escalating security event reports promptly. (HIPAA §164.308(a)(6)(i))

3.7.2 Consistent Incident Response Processing

Help Desk staff must process all reported or identified security events (i.e., known or suspected security incident, security weakness, or system fault) in accordance with HEALTHeLINK's processes. (HIPAA §164.308(a)(6)(ii))

3.7.3 Test Incident Response

The Security Officer must ensure that the incident reporting and response processes are tested at least annually.

3.7.4 Forensic Analysis Capability

The Security Officer must establish a forensic capability, composed of workforce members and/or third parties, to support incident response.

3.7.5 Evidence Management

The Security Officer must ensure that staff, processes, and training are in place to maintain a chain of evidence during investigations.

3.7.6 Log Controls Used to Protect Evidence

The Security Officer must ensure that records are kept of the controls used to protect evidence during an investigation including during collection, storage, and processing.

3.7.7 Creating Forensic Copies of Evidence

The Security Officer must ensure that investigative evidence is protected, copying of evidence is supervised, forensic analysis is done only on copies of evidence, and a log of copying activities is kept.

3.7.8 Confirm Authorization for Corrective Actions

Help Desk staff must verify that a corrective measure taken to address a system fault is authorized and will not compromise required security controls.

3.7.9 Verify Security After Corrective Actions

Help Desk staff must verify that corrective measures taken to address system faults have not compromised required security controls.

3.8 Management Reporting

3.8.1 Evaluate Responses Following Resolution

The Security Officer must develop a post mortem report that details the actions taken during the security incident after each incident has been closed, and review the post mortem report with the IRT to verify the actions taken during the event, support future incident response activities, and determine appropriate corrective actions. (HIPAA §164.308(a)(1)(ii)(D))

3.8.2 Provide Incident Reporting

The Security Officer must, regularly, provide a report related to security incident response activities to Management.

3.9 Training

3.9.1 Provide Incident Reporting Training

The Security Officer must ensure that workforce members are instructed on incident reporting in information security training and awareness.

3.9.2 Provide Incident Response Training

The Security Officer must ensure that periodic training is provided to workforce members who are tasked with incident response.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to security requirements related to business continuity.

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 Contingency Planning

3.1.1 Contingency Plan Development

The Technology Director must establish a formally documented contingency plan, consistent with HEALTHeLINK's business objectives and workforce roles and responsibilities, for responding to emergencies or other situations that damage systems containing sensitive information. (HIPAA §164.308(a)(7)(i))

3.1.2 Emergency Mode Operation Plan

The Security Officer must implement processes, including documentation in contingency and disaster recovery plans, to ensure that sensitive information is secured when operating in emergency mode. (HIPAA §164.308(a)(7)(ii)(C))

3.1.3 Contingency Plan Review and Approval

Directors must, annually, review and approve HEALTHeLINK's contingency plan. (HIPAA §164.308(a)(7)(i))

3.1.4 Include Network Service Outages in Continuity Plans

The Operations Director must ensure that business continuity plans address the impact of a loss of network service.

3.1.5 Contingency Plan Contacts

The Technology Director must, annually, review and update key contact information for HEALTHeLINK's business continuity plans.

3.2 Backup and Recovery

3.2.1 Data Backup Documentation

The Technology Director must document the backup processes for information systems that maintain sensitive data. (HIPAA §164.308(a)(7)(ii)(A))

3.2.2 Data Backup

IT staff must create and maintain exact backup copies of sensitive information in encrypted format. (HIPAA §164.308(a)(7)(ii)(A))

3.2.3 Disaster Recovery Plan

IT staff must implement and document processes to restore sensitive information if required. (HIPAA §164.308(a)(7)(ii)(B))

3.2.4 Data Recovery Strategy

The Technology Director must develop a recovery strategy to ensure that contingency plans and procedures are secured and available in the event of an emergency or disaster. (HIPAA §164.308(a)(7)(ii)(A))

3.2.5 Data Backup Prior to Moves

IT staff must, as needed, create backups of sensitive information before equipment containing the sensitive information is moved. (HIPAA §164.310(d)(2)(iv))

3.2.6 Backup Prior to Update

IT staff must ensure that systems are adequately backed up prior to the deployment of a patch, update, or upgrade.

3.2.7 Backup Testing

IT staff must, regularly, test backups to verify that sensitive information can be successfully restored. (HIPAA §164.310(d)(2)(iv))

3.2.8 Secure Protection of Backups

IT staff must store backups securely and in a location protected from the elements. (HIPAA §164.310(d)(2)(iv))

3.2.9 Record of Backup Media

IT staff must maintain a record of the location and disposition of backups. (HIPAA §164.310(d)(2)(iv))

3.2.10 Define Workforce Backup Requirements

The Technology Director must communicate requirements, if applicable, for workforce members to backup data on HEALTHeLINK-issued devices under their control.

3.2.11 Define Backup Requirements for BYOD

The Technology Director must communicate requirements, if applicable, for workforce members to backup data on personally-owned devices used for HEALTHeLINK work.

3.2.12 Backup Critical Data

The Technology Director must ensure that critical data is backed up regularly, at least daily, and that steps are taken to ensure the integrity of each backup.

3.2.13 Maintain Generations of Backups

The Technology Director must ensure that at least three generations of backups are maintained such that the backups are not vulnerable to damage if the backed-up systems are impacted.

3.2.14 Verify Backup Integrity

IT Staff must, annually, verify the integrity of archived backups.

3.2.15 Backup Cloud Environments

The Technology Director must establish adequate backups for cloud environments that consider the data to be covered, verification of backups, and periodic monitoring.

3.3 Testing and Review

3.3.1 Applications and Data Criticality Analysis

The Technology Director must, annually, assess the criticality of information and information systems, operations, and processes to support business continuity activities, including development of the contingency plan. (HIPAA §164.308(a)(7)(ii)(E))

3.3.2 Preventive Measures

The Technology Director must evaluate and document the measures in place for critical information systems and facilities, including information security controls and suitable insurance, to prevent or minimize impact from emergencies or disasters. (HIPAA §164.308(a)(7)(i))

3.3.3 Testing and Revision Procedures

The Technology Director must, annually, test each element of business continuity plans including coordination with testing of related plans and, if necessary, revise HEALTHeLINK's contingency plans based on the results of testing. (HIPAA §164.308(a)(7)(ii)(D))

3.3.4 Implement Corrective Actions

The Technology Director must implement corrective actions for gaps identified during business continuity plan testing and reviews.

3.3.5 Testing Schedule

The Technology Director must indicate the technique and timing of plan elements within test plans.

3.3.6 Coordinate Tests

The Technology Director must ensure that business continuity tests, including partial or component-level testing, take into account prior test activities and future test plans.

3.3.7 Incorporate Testing Techniques

The Technology Director must incorporate varying techniques in business continuity testing, as appropriate, including tabletop exercises, simulations, alternate site recovery, supplier response, rehearsals, and technical tests covering application installation and setup, system parameters and configuration, patching, access to documentation, and data restores.

3.3.8 Awareness of Business Continuity Responsibilities

The Technology Director must ensure that business continuity testing maintains workforce awareness of roles and responsibilities for business continuity and security when contingency plans are invoked.

3.4 Business Continuity and Risk Assessment

3.4.1 Review Business Continuity Plans for Applicability

The Security Officer must review business continuity plans to verify that security aspects of the plans are based on reasonable events and scenarios.

3.4.2 Ensure Business Continuity Plans Considers Impact

The Security Officer must review business continuity plans to verify that a risk analysis evaluates events based on duration, impact, and recovery period.

3.4.3 Ensure Business Continuity Plans Align with Risk Analysis

The Security Officer must verify that business continuity plans address security aspects of business continuity in alignment with HEALTHeLINK's risk analysis.

3.4.4 Confirm Management Approval of Business Continuity Plans

The Security Officer must verify that security aspects of business continuity are approved by management and put into practice during planning activities.

3.4.5 Resources for Business Continuity

Directors must ensure that financial, organizational, technical, and environmental resources are available to address the information security requirements of HEALTHeLINK's business continuity plans.

3.5 Business Continuity Planning Framework

3.5.1 Ensure Business Continuity Plans Address Minimum Expectations

The Security Officer must ensure that business continuity plans providing an approach to availability and security have a defined owner, escalation plan, activation terms, and identified individuals responsible for executing plan components.

3.5.2 Update Business Continuity Plans when Needed

Directors must update business continuity plans, if appropriate, as new requirements or changes to business arrangements, personnel, facilities, resources, business processes, risk, or regulatory requirements are identified.

3.5.3 Designate Business Continuity Responsibilities

Directors must designate appropriate individuals with responsibility for emergency, manual fall-back, and resumption procedures.

3.5.4 Ensure Third Parties Plan Business Contuity Fall-back

The Technology Director must ensure that the individuals or third parties responsible make adequate fall-back arrangements for technical resources, systems, and facilities.

3.5.5 Establish Security Requirements for Business Continuity

The Security Officer must establish specific, minimum information security controls, including preventive and detective controls, as a component of HEALTHeLINK's business continuity framework.

3.5.6 Ensure Safety and Asset Protection

The Security Officer must ensure that information security controls applied to HEALTHeLINK's business continuity framework support personnel safety and protection of HEALTHeLINK information assets and property.

3.6 Developing and Implementing Continuity Plans Including Information Security

3.6.1 Distribute Business Continuity Plans

The Security Officer must distribute business continuity plans to individuals with emergency response.

3.7 Equipment Maintenance

3.7.1 Confirm Access to Spare Parts for Third Parties Involved in Business Continuity

The Technology Director must ensure that HEALTHeLINK can obtain support and spare parts in alignment with the recovery time objectives defined in its business continuity plan.

3.8 Facility Resiliency

3.8.1 Separate Primary and Secondary Sites

The Operations Director must identify alternative storage and processing sites sufficiently separate from primary sites with equivalent security measures in place.

3.8.2 Ensure Backup Power and Telecommunications

The Operations Director must ensure that appropriate emergency power and backup telecommunications infrastructure is available to support critical processing at HEALTHeLINK sites.

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 statements in this policy document establish HEALTHeLINK's expectations with respect to retaining records to meet business and regulatory requirements.

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 Clinical/Medical Records

3.1.1 Retain Records to Meet Regulatory Requirements

Workforce members 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.

3.1.2 Archive Older Retained Data

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

3.1.3 Store Archives in Secure Areas

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

3.1.4 Maintain Backups of Archived Data

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

3.1.5 Protect Retained Records

The Operations Director 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.

3.1.6 Retain Records of Notice

The Operations Director 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.

3.1.7 Retain Records of Restrictions

The Operations Director 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 accountsings of disclosure are retained for a period of six years.

3.2 Audit Logs

3.2.1 Maintain Accessible Audit Logs

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

3.2.2 Archive Audit Logs

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.

3.3 Information Assets

3.3.1 Consider Classification in Data Retention

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.

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 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.

ADVANCED EMERGENCY MEDICAL TECHNICIAN

A person certified pursuant to the New York State Emergency Services Code at 10 NYCRR § 800.3(p) as an emergency medical technician-intermediate, an emergency medical technician-critical care, or an emergency medical technician-paramedic.

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 useable 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 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 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 CFR § 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 CFR § 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. Care Management does not include utilization review or other activities carried out by a Payer Organization to determine whether coverage should be extended or payment should be made for a health care service.

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).

CONSENT IMPLEMENTATION DATE

The date by which the NYSDOH requires QEs to begin to utilize an Approved Consent. In establishing such date, NYSDOH shall take into account the time that will be required for individual QEs 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 CFR § 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 SUPPLIER

An individual or entity that supplies Protected Health Information to or through HEALTHeLINK. Data Suppliers include both Participants and entities that supply but do not Access Protected Health Information via the SHIN-NY governed by HEALTHeLINK (such as clinical laboratories and pharmacies).

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 (i) it satisfies the requirements of 45 CFR § 164.514(b) and (ii) does not contain DNA variation information derived from sequencing genotyping or other such technologies.

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 CFR § 164.501.

DIRECTOR

An executive-level manager of HEALTHeLINK.

DISASTER RELIEF AGENCY

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)

Means information that comes within paragraphs 1(i) or 1(ii) of the definition of "Protected Health Information", as defined in 45 CFR § 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.

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.

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 CFR 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 CFR 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 CFR 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 CFR § 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 CFR Part 160 and Subparts A and E of Part 164

HIPAA SECURITY RULE

The federal regulations at 45 CFR 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 NYCRR § 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 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 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, 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 CFR § 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).

MALWARE

Malicious software

MARKETING

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 abuse 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 business.

NEW YORK EHEALTH COLLABORATIVE (NYEC)

The New York not-for-profit corporation organized for the purpose of (1) convening, educating and engaging key constituencies, including health care and health IT leaders across New York State, QEs, and other health IT initiatives; (2) developing common health IT policies and procedures, standards, technical requirements and service requirements through a transparent governance process and (3) evaluating and establishing accountability measures for New York State's health IT strategy. NYeC is under contract to the NYSDOH to administer the SCP and through it develop Statewide 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.

NYSDOH

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 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 CFR § 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 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 CARE 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.

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 CFR § 164.501.

PERFORMING PROVIDER SYSTEM (PPS)

A Performing Provider System that has received approval form NYSDOH to implement projects and receive funds under New York's Delivery System Reform Incentive Payment Program

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 NYSDOH 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 NYSDOH.

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 CFR § 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 NYCRR 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.

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 abuse, 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 PORTAL

The secure online website that gives patients and their Personal Representatives access to the Protected Health Information about them that is available through the SHIN-NY

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

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 COLLABORATIVE 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 Statewide Policy Guidance as provided in 10 NYCRR Section 300.3.

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 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 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 NYSDOH as provided in 10 NYCRR Section 300.3, including the statewide policy guidance incorporated by reference in subdivision (c) of that section.

TECHNICAL SAFEGUARDS

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

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.

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 17932(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.

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).

HEALTHeLINK™

Revision History

Privacy Policies

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

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
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

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

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
Policy P09
Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 05/14/09, 04/01/10, 04/25/13, 06/01/13, 06/30/16, 07/29/19

Participant Workforce Training for HEALTHeLINK Privacy and Security Policies
Policy P10
Effective Date: 06/29/08
Review Dates: 05/26/16, 10/26/17, 05/24/18, 06/27/19, 05/28/20
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
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
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20

Alerts
Policy P14
Effective Date: 06/30/16
Review Dates: 10/26/17
Revision Effective Dates: ARCHIVED 11/27/17

Patient Engagement
Policy P15
Effective Date: 11/27/17
Review Dates: 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 07/29/19

Audit
Policy P16
Effective Date: 11/27/17
Review Dates: 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 07/29/19

Security Policies

Participant Requirements
Policy SP-001
Effective Date: 09/13/07

Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/25/10, 01/15/15, 06/30/16, 07/01/18

Security Program
Policy SP-002
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Risk Management
Policy SP-003
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Personnel Security
Policy SP-004
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Physical Security
Policy SP-005
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Acceptable Use
Policy SP-006
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Technical Security
Policy SP-007
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

Access Control
Policy SP-008
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 07/29/19, 06/29/20

System Development Life Cycle (SDLC)
Policy SP-009
Effective Date: 01/15/15
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20

Incident Reporting
Policy SP-010
Effective Date: 09/16/11
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18, 06/29/20

Incident Management
Policy SP-011
Effective Date: 01/15/15
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20

Business Continuity
Policy SP-012
Effective Date: 01/15/15
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20

Record Retention
Policy SP-013
Effective Date: 01/15/15
Review Dates: 01/15/15, 05/19/16, 05/24/18, 06/27/19, 05/28/20
Revision Effective Dates: 06/30/16, 07/01/18, 07/29/19, 06/29/20