HEALTHeLINK™

Privacy and Security Policies

Table of Contents

Privacy and Security Policies

Privacy Policies

Security Policies

Privacy Policies

Amendment of Data

Privacy Policy
Policy No. P02

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 amendment and/or correction of PHI.

2 Scope

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

3 Procedure

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

B. If a patient makes a request for an Amendment of Data directly to HEALTHeLINK:
    1. Within 3 business days, HEALTHeLINK will provide the patient directions on how to make such request of the applicable Data Supplier including the contact information of the Privacy Officer of the Data Supplier.
    2. Within 3 business days of such request, HEALTHeLINK will also notify the Data Supplier Participant of the request and will cooperate with the Participant so the Participant may respond to the patient.

C. Participants must notify HEALTHeLINK if, in response to a request by a patient, the Participant makes any corrections to the patient's erroneous information.

D. Upon 10 days' written notice by the Data Supplier Participant, HEALTHeLINK will make, or make available for, amendment(s) to PHI in a Designated Record Set to which the Participant agrees.

E. HEALTHeLINK will make reasonable efforts to provide its Participants with information indicating which other Participants have accessed erroneous information that the Participant has corrected at the request of the patient.

4 References

- 45 CFR § 164.526.
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1).*
- HEALTHeLINK: *Terms and Conditions for Health Information Exchange Participation Agreement*

Authorized User Access

Privacy Policy
Policy No. P03

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:

1. Has completed training provided or approved by HEALTHeLINK;
2. 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;
3. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized User;
4. 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
5. 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:

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

2. Will be permitted to use the HIE only as reasonably necessary for the performance of HEALTHeLINK's activities;
3. Has agreed not to disclose to any other person any passwords and/or other security measures issued to the Authorized Users;
4. 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;
5. 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 provide, 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, a Participant may not access a patient's PHI via HEALTHeLINK unless the patient has provided an Affirmative Consent authorizing the Participant to access 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 is not required under the circumstances set forth below. Access to 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 accessed or disclosed without Affirmative Consent unless 42 C.F.R Part 2 specifically allows for such access or disclosure.

3.2.1 One-to-One Exchanges

A. Affirmative Consent (as defined in the definitions section) shall not be required for a Participant to access a patient's Protected Health Information via the SHIN-NY governed by a QE from another Participant if such access meets all the requirements of in a One-to-One Exchange (including the requirements that the access 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 provided 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. A Public Health Agency may access Protected Health Information through a QE's clinical viewer or portal 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.

B. A patient's denial of consent for access of the patient's PHI under Section 3.8.3 will not prevent or otherwise restrict a Public Health Agency from accessing the patient's PHI for the purposes stated above.

C. 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.

3.2.3 Access for Disaster Tracking

A. For the purpose of locating patients during an Emergency Event, a Disaster Relief Agency is allowed to access 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. Access to information under this Section may begin when the Emergency Event begins and will cease when the Emergency Event ceases.

C. Information accessed under this Section will not reveal the nature of the medical care received by the patient who is the subject of the access request 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 to access the patient's PHI under Section 3.8.3 does not restrict a Disaster Relief Agency from accessing information as permitted by this Section.

3.2.4 Emergency Access to PHI When Treating a Patient with an Emergency Condition or "Break the Glass"

A. Affirmative Consent is not required for (1) a Practitioner, (2) an Authorized User acting under the direction of a Practitioner; or (3) an Advanced Emergency Medical Technician to "Break the Glass" and access PHI 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 exist; **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 the patient's information is currently in effect with respect to the Participant with which the 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 access.

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 access to PHI via Breaking the Glass terminates upon the completion of the emergency treatment.

D. Upon a patient's discharge from a Participant's emergency room, if emergency access to 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 accessed 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 accessed through Break the Glass.

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

3.2.5 Converting Data

Affirmative Consent is not 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 HEALTHeLINK is serving as the Data Supplier's Associate (as defined in 45 CFR § 160.103) and (ii) HEALTHeLINK does not make the information accessible to Participants 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 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 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 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 PHI for the purpose of evaluating and improving HEALTHeLINK operations.

3.2.7 De-Identified Data

Affirmative Consent is not required for access to De-Identified Data for specified Authorized Users as set forth in Section 3.6.

3.2.8 Organ Procurement Organization Access

Organ Procurement Organization may access PHI without Affirmative Consent solely for the purposes of facilitating organ, eye or tissue donation and transplantation. A patient's denial or Affirmative Consent for all Participants in HEALTHeLINK to access the patient's PHI under Section 3.8.3 will not prevent or otherwise restrict an Organ Procurement Organization from accessing 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 provided 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 sent 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 sent 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.

3.3 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.

A QE 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. QEs are 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, the QE 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 information via the SHIN-NY governed by a QE for Level 1 Uses shall be obtained using a Level 1 Consent or an Alternative Consent approved by a QE under this section, which shall include the following information:

A. A description of the information to which the patient is granting the Participant access, 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 information via the SHIN-NY governed by a QE for the purposes of Level 2 Uses shall be obtained using a Level 2 Consent or an Alternative Consent approved by a QE 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 accessed;

B. Whether the QE and/or its Participants will benefit financially as a result of the use/disclosure of the information to which the patient granting access;

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 a QE website or other means; the consent form shall also identify whether the QE 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 a QE 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 a QE.

If a QE 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 PHI via the SHIN-NY governed by a QE for the purpose of Marketing, the QE 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 will authorize Participants to access all the patient's PHI, including Sensitive Health Information.

3.4.2 Re-disclosure Warning

A. HEALTHeLINK will place a warning statement that is viewed by Authorized Users whenever they are obtaining access to 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.

B. HEALTHeLINK will include a warning statement that is viewed by Authorized Users whenever they are obtaining access to 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 3.4.2(A) or on the log-in screen that Authorized Users must view before logging into HEALTHeLINK.

C. HEALTHeLINK will include a warning statement that contains language that notifies Authorized Users they may be accessing 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 and 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 3.4.2(A) or on the log-in screen that Authorized Users must view before logging into HEALTHeLINK.

3.4.3 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 through HEALTHeLINK the 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 Minor Consent Information through HEALTHeLINK 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 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 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.

3.6 De-Identified Data

3.6.1 Access of De-Identified Data for Specified Uses

A. Affirmative Consent is not required for HEALTHeLINK, a Participant, or a government agency to access De-Identified Data for Research in accordance with Section 3.7 below.

B. Affirmative Consent is not required for a Participant to access 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 De-Identified Data for any purpose for which HEALTHeLINK, the Participant, or government agency may lawfully access 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 disclose 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.

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.

C. De-Identified Data will 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 Use of De-Identified Data for Research

Affirmative Consent shall not be required to access De-Identified Data in order to conduct Research approved or deemed exempt by an Institutional Review Board organized and operating in accordance with 45 CFR § 164. The Researcher seeking to perform the Research must obtain approval from the Research Committee. (See HEALTHeLINK Policy P13, *Release of Data for Research*.)

3.7.2 Use of Limited Data Set for Research

Affirmative Consent shall not be required for HEALTHeLINK or a Participant to access a Limited Data Set in order to conduct Research approved or deemed exempt by an Institutional Review Board organized and operating in accordance with 45 CFR § 164.

3.7.3 Other Requirements Relating to Research

HEALTHeLINK will not permit a Participant to opt out of having its PHI de-identified or converted into a Limited Data Set and used for Research that complies with Section 3.7.1 or Section 3.7.2.

3.8 Other Policies and Procedures Related to Consent

3.8.1 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.

C. HEALTHeLINK will maintain copies of all the patients' written consents.

3.8.2 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 must be forwarded to HEALTHeLINK within 3 business days.

3.8.3 Denial of Consent

Patients may deny consent to the access of their health information 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. "No, Except in an Emergency" or
    3. "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).

C. 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.

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

3.8.4 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. An Affirmative Consent may apply to Participants who join the QE after the date the patient signs the consent form, provided that:
    1. the QE 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. the QE 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 the QE'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.

3.8.5 Durability

A. An Affirmative Consent for Level 1 Uses is not time-limited. Affirmative Consents remain in effect until revoked by the patient.

B. An Affirmative Consent for Level 2 Uses is time-limited and will 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.

3.8.6 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.

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

Provider Participants must ensure that a Payer Organization cannot access 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's Organization 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.

3.8.8 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.

3.9 Patient Consent Transition Rules

3.9.1 Use of Approved Consents.

Except as set forth in Section 3.9.2, 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.

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

Each QE that obtained patient consent utilizing a patient consent substantially similar to a Level 1 Consent prior to the Consent Implementation Date (an "Existing Consent Form") 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.

3.9.3 Use of Existing Consent After Consent Implementation Date

A QE 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*
- 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).*

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 provide, 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 transport 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, 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, 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 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 as appropriate in accordance with 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).*
- 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 provide, 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, 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 provide, make available or access health information through HEALTHeLINK.

3 Procedures

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

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

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

D. 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.

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

4. whether the violation resulted in harm to a patient or other person.

F. 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; and
   4. suspending or terminating a Participant's participation in HEALTHeLINK.

G. With the exception of sanctions temporarily restricting an Authorized User's access to HEALTHeLINK or requiring Authorized Users to undergo additional training in the use of HEALTHeLINK, any sanction applied by HEALTHeLINK to a Participant must first be presented to the HEALTHeLINK Operating Committee for 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).*

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 provide, 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 provide, 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 use 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 of termination.

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

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

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

4 References

- 45 C.F.R. § 164.530
- HEALTHeLINK Policy P09, *Sanction for Failure to Comply with HEALTHeLINK Privacy and Security Policies*
- 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 release data to third party researchers for scholarly research purposes. The data subject to release 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 release 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.
    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. PHI will not be accessed through HEALTHeLINK for Research purposes unless the patient has provided an Affirmative Consent (i.e., Level 2 Consent for Research)

authorizing the access of such PHI for Research. (See HEALTHeLINK Policy P04, *Patient Consent*.)

1. Affirmative Consent shall not be required for HEALTHeLINK or a Participant to access De-Identified Data in order to conduct Research approved or deemed exempt by an Institutional Review Board (IRB) organized and operating in accordance with 45 CFR § 164.
2. Affirmative Consent shall not be required for HEALTHeLINK or a Participant to access a Limited Data Set in order to conduct Research approved or deemed exempt by an IRB organized and operating in accordance with 45 CFR § 164.

C. If the proposed Research using De-Identified Data or a Limited Data Set 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.

D. 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.

E. 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 released 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)

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 provide, 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. A QE 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 the QE on behalf of all of its Participants or all Protected Health Information in the SHIN-NY.

   2. A QE 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 the QE 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 electronic form.

B. HEALTHeLINK may 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 deny Personal Representatives of minors under the age of 18 access to the minor's Protected Health Information.

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

G. Each QE shall make reasonable efforts to provide its Participants with information indicating which other QE Participants have accessed 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)*

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 access of Protected Health Information via HEALTHeLINK.

B. Audit Logs shall, at a minimum, include the following information:
   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 Participate 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. 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.

D. 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. 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.

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

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 accessed via HEALTHeLINK, other than in Break the Glass situations;
   2. That Authorized Users who access Protected Health Information via the SHIN-NY governed by HEALTHeLINK do so for Authorized Purposes; and
   3. That applicable requirements were met where Protected Health Information was accessed 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 using a statistically significant sample size.

E. 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 accessed via the SHIN-NY governed by HEALTHeLINK:
   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 access; and

3. The type of Protected Health Information or record that was accessed (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 the patient's Protected Health Information in up to the prior 6-year period;
   2. The time and date of such access; and
   3. The type of Protected Health Information or record that was accessed (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 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 Users were consistent with the terms of these Policies and Procedures (based upon a listing sent by the HEALTHeLINK).

3.8 Additional Requirements Related to Auditing of Public Health Access

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

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

B. The name of the particular Public Health Agency shall be listed in the patient audit logs.

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

4 References

- HEALTHeLINK Policy P06, *Breach Response*
- NYSDOH: *Privacy and Security Policies and Procedures for Qualified Entities and Their Participants in New York State Under 10 NYCRR § 300.3(b)(1)*

HEALTHeLINK™

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 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 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. (HIPAA §164.306(d)(1-3))

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 and regulations 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, and procedures address program purpose, scope, roles and responsibilities, and oversight.

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.

3.4 Documentation

3.4.1 Security Program Documentation

The Security Officer must maintain HEALTHeLINK's policies 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 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 and procedures. (HIPAA §164.316(b)(2)(ii)) (SHIN-NY 3.3 §4.7(1))

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. (HIPAA §164.316(b)(2)(i))

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 Scope of Assessments

The Security Officer must define the scope of technical and non-technical assessments of HEALTHeLINK's information security policies and practices to ensure that appropriate regulatory requirements are addressed. (HIPAA §164.308(a)(8))

3.5.3 Assessment Preparation

The Security Officer must establish a process to prepare and provide information necessary to an assessment of HEALTHeLINK's security policies and practices in a timely manner. (HIPAA §164.308(a)(8))

3.5.4 Review of Assessor Credentials

The Security Officer must evaluate and select the parties performing information security assessments, whether qualified internal staff or external consultants, and document the verification of the assessor's credentials and experience. (HIPAA §164.308(a)(8))

3.5.5 Agreements with Assessors

The Security Officer must ensure that an appropriate agreement is in place with any party performing an assessment of HEALTHeLINK's information security policies and practices. (HIPAA §164.308(a)(8))

3.5.6 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))

3.6 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 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)) (SHIN-NY 3.3 §4.7(1))

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))

3.8 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)) (SHIN-NY 3.3 §4.8.3)

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. (SHIN-NY 3.3 §4.8)

3.11 Certification

3.11.1 Provide Security Control Certification or Attestation

The Security Officer must must provide to Participants, as requested, proof of certification or attestation of appropriate data security controls in place to safeguard and protect the Participants' PHI and Personally Identifiable Information. Such certification or attestation may be in the form of a SOC 2 Type 2 report, HITRUST certification, or as established by the HEALTHeLINK Operating Committee.

3.12 Management Commitment to Information Security

3.12.1 Retain Security Program Responsibility

The Executive Director must retain responsibility for HEALTHeLINK's cybersecurity program if a third party serves as HEALTHeLINK's information security officer.

3.12.2 Establish Oversight of Third Party Security Officer

The Executive Director must designate a senior manager to provide oversight if a third party serves as HEALTHeLINK's information security officer.

3.12.3 Require Program Third Party Security Officer

The Executive Director must require a third party to maintain its own information security program if the third party serves as HEALTHeLINK's information security officer.

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. (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. (HIPAA §164.308(a)(1)(ii)(A))

3.3 Review

3.3.1 Information System Activity Review

The Security Officer must regularly review records of information system 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))

3.4 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)) (SHIN-NY 3.3 §4.10.1)

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 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.

3.6 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 a third party service provider.

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 that establish each signatory's obligations, responsibilities, and expectations.

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 and procedures, to protect HEALTHeLINK data.

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 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. (HIPAA §164.308(a)(3))

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)) (SHIN-NY 3.3 §2.1.5)

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)) (SHIN-NY 3.3 §2.1.5)

3.4 Employment Agreements

3.4.1 Address Policy in Employment Agreements

Directors must ensure that employee agreements are executed which contain language regarding adherence to HEALTHeLINK's security policy.

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)) (SHIN-NY 3.3 §2.1.5, 4.7.1, 4.7.2, 4.7.4)

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. (SHIN-NY 3.3 §2.1.5)

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.

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)) (SHIN-NY 3.3 §4.7.2, 4.7.3)

3.5.6 Updating Security Awareness and Training Program

The Security Officer must review HEALTHeLINK's security awareness and training program 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.

3.6 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.

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 procedures 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 procedures 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 document 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.

3.2 Protecting Against External and Environmental Threats

3.2.1 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, and oversight.

3.3 Service Delivery

3.3.1 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.

3.4 Workstation Security

3.4.1 Workstation Security

The Operations Director must implement physical safeguards to restrict access to only Authorized Users for workstations where sensitive information is accessed, including limiting unauthorized viewing of data and providing for secure disposal of sensitive documents. (HIPAA §164.310(c))

3.4.2 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))

3.4.3 Workstation Inventory

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

3.4.4 Workstation Use

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

3.4.5 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))

3.5 Hardware and Media

3.5.1 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))

3.5.2 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))

3.5.3 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))

3.5.4 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))

3.5.5 Disposal, Recording

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

3.5.6 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))

3.6 Secure Disposal or Re-Use of Equipment

3.6.1 Securely Store Spare Equipment

IT staff must store surplus equipment securely when not in use.

3.7 Emergency Access

3.7.1 Contingency Operations

The Technology Director must implement procedures to allow and control emergency access to authorized individuals, including workforce members and third parties, for data restoration and incident response. (HIPAA §164.310(a)(2)(i))

3.8 Equipment Maintenance

3.8.1 List Maintenance Providers

The Operations Director must maintain a list of authorized maintenance organizations or personnel.

3.8.2 Establish Access for Maintenance Providers

The Operations Director must establish access authorizations for non-escorted maintenance personnel prior to maintenance.

3.8.3 Supervise Escorted Maintenance Providers

The Operations Director must designate authorized and appropriately skilled individuals to supervise maintenance personnel who do not have prior access authorization.

3.8.4 Monitor Service Providers

The Operations Director must monitor remote maintenance and diagnostic activities.

3.8.5 Restrict Report Maintenance

The Operations Director must restrict remote maintenance and diagnostic activities without prior, written management approval.

3.9 Protecting Against External and Environmental Threats

3.9.1 Verify Fire Protection Installation

The Operations Director must verify that fire extinguishers and detectors are installed in accordance with regulatory requirements.

3.9.2 Verify that Fire Alarms Notify Authorities

The Operations Director must verify that installed fire alarm systems are configured to automatically notify appropriate authorities when activated.

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. (SHIN-NY 3.3 §4.2)

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 access, modify, delete, or perform testing 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.

3.2 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 or potential impact to HEALTHeLINK resulting from adverse incidents.

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 the classification of information assets and update as needed.

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.

3.4 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 an indication of assets deemed critical to HEALTHeLINK.

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.

3.2 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)) (SHIN-NY 3.3 §3.2.3)

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)) (SHIN-NY 3.3 §3.1, 3.2.1, 4.1.1)

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)) (SHIN-NY 3.3 §3.2.1(a), 4.1.2)

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)) (SHIN-NY 3.3 §3.2.1(a))

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)) (SHIN-NY 3.3 §3.2.1(a), 4.1.2)

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, access to keys, and key management. (HIPAA §164.312(a)(2)(iv))

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))

3.6 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.

3.8 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)) (SHIN-NY 3.3 §6.1, 6.1.1)

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)) (SHIN-NY 3.3 §2.1.5)

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. (SHIN-NY 3.3 §2.1.5)

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)) (SHIN-NY 3.3 §6.2)

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. (SHIN-NY 3.3 §6.1.5)

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. (SHIN-NY 3.3 §6.1.1, 6.1.2, 6.1.3, 6.1.4)

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. (SHIN-NY 3.3 §2.1.6)

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. (SHIN-NY 3.3 §3.5)

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. (SHIN-NY 3.3 §4.9)

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 Maintain Software with Support

IT staff must maintain vendor-supplied software installed on HEALTHeLINK systems at a level that is supported by the vendor.

3.11.3 Maintain Web Browsers

IT staff must maintain web browsers installed on HEALTHeLINK systems at current and supported levels.

3.11.4 Blacklist Risky Software

IT staff must configure systems to prevent unauthorized (i.e., blacklisted) software from executing.

3.11.5 Follow Software Terms and Conditions

IT staff must configure systems to prevent software from executing if not authorized based on the software's terms and conditions.

3.11.6 Check for Unauthorized Software

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

3.11.7 Maintain Software Blacklist

The Security Officer must annually review and update, if appropriate, the list of unauthorized software that is blacklisted from HEALTHeLINK systems.

3.12 Mobile Computing and Communications

3.12.1 Issue Special Devices for High-risk Travel

IT staff must issue mobile devices with additional controls or limited access to workforce members traveling to high-risk locations.

3.12.2 Check Devices After High-risk Travel

IT staff must inspect the mobile devices issued for travel to high-risk locations upon return to detect malware or tampering.

3.13 Electronic Commerce Services

3.13.1 Maintain Security for E-commerce

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

3.14 Electronic Messaging

3.14.1 Avoid Faxing

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

3.15 Input Data Validation

3.15.1 Implement Input Validation

IT staff must implement input validation for accuracy, completeness, validity, and authenticity for HEALTHeLINK applications as close to the point of origin as practical.

3.15.2 Implement Error Checking

IT staff must implement error checking for input size, data type, acceptable ranges, and acceptable formats for HEALTHeLINK applications.

3.16 Inventory of Assets

3.16.1 Review Inventories to Avoid Duplication

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

3.16.2 Review Inventories for Consistency

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

3.16.3 Include Wireless Access Points in Inventory

IT staff must list authorized wireless access points in HEALTHeLINK's asset inventory.

3.16.4 Record Wireless Access Point Justification

IT staff must specify the business justification for wireless access points in HEALTHeLINK's asset inventory.

3.16.5 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.

3.16.6 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.

3.16.7 Define Data Erasure Process

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

3.17 Network Controls

3.17.1 Update Network Diagrams After Changes

IT staff must update HEALTHeLINK's wired and wireless network diagrams when significant changes to the network occur.

3.17.2 Update Network Diagrams Periodically

The Technology Director must bi-annually review and update, if appropriate, HEALTHeLINK's wired and wireless network diagrams.

3.17.3 Test Wireless Networks

The Security Officer must test for unauthorized wireless networks devices connected to HEALTHeLINK's networks.

3.17.4 Validate Wireless Access Point Requests

The Technology Director must review and approve, if appropriate, requirements for wireless access points on HEALTHeLINK's networks.

3.17.5 Keep Devices Under Asset Management

IT staff must ensure that devices connected to HEALTHeLINK networks are covered under HEALTHeLINK's asset management processes.

3.18 On-line Transactions

3.18.1 Check E-commerce Transactions for Sensitive Data

The Technology Director must check electronic commerce transactions to identify covered information contained therein.

3.18.2 Protect E-commerce Transactions

The Technology Director must maintain security throughout the electronic commerce transaction lifecycle.

3.18.3 Use Encryption for E-commerce Transactions

The Technology Director must use encryption to protect electronic commerce transactions between all parties.

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)) (SHIN-NY 3.3 §2.1.5)

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)) (SHIN-NY 3.3 §2.1.2)

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)) (SHIN-NY 3.3 §2.1.1(a), 2.1.3)

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)) (SHIN-NY 3.3 §2.1.1(b), 2.1.1(c), 2.1.2, 2.1.3)

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)) (SHIN-NY 3.3 §2.1.4)

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)) (SHIN-NY 3.3 §2.1.1(c), 2.1.2)

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)) (SHIN-NY 3.3 §4.5)

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 Assign Unique User IDs

IT staff must ensure that user accounts for information systems and applications are provisioned with a unique user ID. (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)) (SHIN-NY 3.3 §4.1, 4.1.3)

3.4.2 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.

3.4.3 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)) (SHIN-NY 3.3 §4.1.2)

3.4.4 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) (SHIN-NY 3.3 §4.1.5)

3.4.5 Configure Systems to Require Secure Passwords

IT staff must configure systems to require complex passwords that are difficult to guess and ensure that system and network passwords are securely created, expired, changed, and reset. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.4.6 Configure Systems to Expire Passwords

IT staff must configure information systems to expire passwords after 90 days. (HIPAA §164.310, 164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D)) (SHIN-NY 3.3 §4.1.4)

3.4.7 Configure Systems to Prevent Password Re-use

IT staff must configure systems to prevent password re-use. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D)) (SHIN-NY 3.3 §4.1.4)

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)) (SHIN-NY 3.3 §4.8, 4.8.1, 4.8.2)

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)) (SHIN-NY 3.3 §4.8.1)

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 access grants, changes, and removals and perform regular reviews that such changes have been appropriately made.

3.6 System

3.6.1 Configure Time-outs

IT staff must configure all information systems that store, process, or transmit sensitive data including sensitive information such as computers, mobile devices, and network equipment to include automated inactivity time-out features after a predetermined time of inactivity. (HIPAA §164.312(a)(1), 164.312(a)(2)(iii)) (SHIN-NY 3.3 §4.4)

3.6.2 Prevent Unauthorized Login Attempts

IT staff must configure information systems to restrict access to only authorized individuals, to limit the number of login attempts by a connecting user, and to limit the number of attempts that may be made to login to an individual account. (HIPAA §164.308(a)(4)(ii)(b)) (SHIN-NY 3.3 §4.3)

3.7 Administrative Access

3.7.1 Limit Access Administrators

The Security Officer must restrict the ability to add, modify, or delete user access to only authorized personnel and maintain a record of the individuals granted the ability. (HIPAA §164.312(a)(1)) (SHIN-NY 3.3 §2.1.5)

3.7.2 Monitor Use of Administrative Privileges for Access Control

IT staff must maintain an audit log of individuals using administrative accounts and regularly review access rights to administrative accounts. (HIPAA §164.308(a)(4)(ii)(B), 164.312(a)(1)) (SHIN-NY 3.3 §2.1.5)

3.7.3 Document and Control Generic Accounts

IT staff must document the generic and/or system IDs used or created and maintain a record of the approval of each ID. (HIPAA §164.312(a)(1))

3.7.4 Restrict Generic Account Use

IT staff must establish procedures governing the creation of and use of generic and system IDs to prevent unauthorized use. (HIPAA §164.312(a)(1))

3.8 Vendor Accounts

3.8.1 Change Default Vendor Passwords

IT staff must configure hardware and software such that default passwords and other passwords set by vendors are changed and/or disabled prior to implementing a system. (HIPAA §164.312(a)(1))

3.8.2 Restrict Vendor Accounts

IT staff must ensure that each vendor account is configured to provide only the access to systems, applications, and information that is required for each vendor’s responsibilities, and that access to sensitive information by vendor's is only permitted when required.

3.9 Emergency Access

3.9.1 Document Emergency Access Processes

Senior management must establish a documented process to allow facility access for restoration and recovery in the event of an emergency. (HIPAA §164.310(a)(2)(i))

3.9.2 Enable Emergency Access

IT staff must establish methods for accessing sensitive data including sensitive information during an emergency, as required for business purposes, if normal access controls are disabled or inoperable or in a clinical emergency situation. (HIPAA §164.312(a)(2)(ii), 164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.9.3 Restrict Emergency Access Initiation

Senior management must restrict the ability to initiate emergency access processes to only appropriate personnel. (HIPAA §164.312(a)(2)(ii))

3.10 Records

3.10.1 Document Roles and Systems

The Security Officer must maintain a cross-reference of systems that process, store, or transmit sensitive data including sensitive information to the departments and roles that require access to the system. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.10.2 Document Role Assignments

IT staff must maintain a record of the category assignments of workforce members and supporting details including name, job title, date of hire, date of transfer, transfer category, and termination date. (HIPAA §164.312(a), 164.312(c)(2), 164.312(d), 164.312(e))

3.10.3 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))

3.11 Audit and Review

3.11.1 Maintain an Audit Log of Access Attempts

IT staff must establish an audit logging process to record attempts to access information systems, secure areas, and facilities. (SHIN-NY 3.3 §6.1, 6.1.1)

3.11.2 Protect Audit Log Data from Unauthorized Access

The Security Officer must ensure that audit log data is protected against unauthorized access, disruption of collection or delivery, and modification. (SHIN-NY 3.3 §6.1.4)

3.11.3 Restrict Access to Audit Logs

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

3.11.4 Review Access Rights by Individual

Senior management must annually review workforce members' access rights to systems. (HIPAA §164.312(a)(1))

3.11.5 Review Access Rights by Role

The Security Officer must annually perform regular reviews of granted access levels to determine that granted access is appropriate. (HIPAA §164.308(a)(3), 164.308(a)(4), 164.308(a)(5)(ii)(D))

3.11.6 Review Physical Access Logs

The Security Officer must perform regular reviews of the physical access logs of facilities and secure areas for inappropriate activity.

3.12 Access Reports

3.12.1 Document Access Report Requests

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

3.12.2 Create and Maintain Access Report Records

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

3.12.3 Report on Access Report Requests to Operating Committee

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

3.13 Control of Operational Software

3.13.1 Restrict Support Provider Access

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

3.13.2 Gain Approval of Support Provider Access

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

3.13.3 Monitor Support Providers

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

3.14 Privilege Management

3.14.1 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.

3.14.2 Avoid Use of Elevated-privilege Accounts

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

3.14.3 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.

3.15 Session Time-out

3.15.1 Deploy Idle Lockout

IT staff must configure and enforce HEALTHeLINK-issued devices to use an automatic idle-time screen lockout.

3.15.2 Require Idle Lockout for BYOD

IT staff must require and enforce BYOD devices to use an automatic idle-time screen lockout.

3.16 User Identification and Authentication

3.16.1 Avoid Electronic Signature Re-use

The Technology Director must ensure that unique electronic signatures cannot be reused or reassigned to other individuals.

3.16.2 Verify PKI Certificate Paths

The Technology Director must ensure that PKI-based authentication is configured to validate certificates by verifying a certificate path to an accepted trust anchor and checking certificate status.

3.16.3 Enforce PKI Access to Corresponding Keys

The Technology Director must ensure that PKI-based authentication is configured to enforce access to the corresponding private key.

3.16.4 Map PKI Identities to Corresponding Accounts

The Technology Director must ensure that PKI-based authentication is configured to map identities to corresponding individual or group accounts.

3.16.5 Use Local PKI Revocation Cache if Not Networked

The Technology Director must ensure that PKI-based authentication is configured to use a local cache of revocation data if network-based validation is unavailable.

3.16.6 Implement Biometric-based Electronic Signatures

The Technology Director must implement biometric-based electronic signatures so that the signatures can only be used by their owners.

3.16.7 Link Signatures to Applicable Electronic Records

The Technology Director must implement mechanisms to link electronic and handwritten signatures to their respective electronic records.

3.16.8 Provide Human-readable Electronic Signature Data

The Technology Director must enable information regarding electronically signed records to be human-readable.

3.16.9 Verify the Identity of Individuals

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

3.16.10 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.

3.17 User Authentication for External Connections

3.17.1 Encrypt Dial-up Connections

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

3.18 User Password Management

3.18.1 Acknowledge Password Receipt

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

3.18.2 Change Default Passwords at Setup

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

3.18.3 Require New Password at First Login

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

3.18.4 Change Password if Compromised

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

3.18.5 Change Privileged Passwords

IT staff must changed privileged account passwords no less than every 60 days.

3.18.6 Protect PINs

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

3.18.7 Require ID for Electronic Signatures

The Technology Director must require non-biometric electronic signatures to use two distinct identification components.

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.

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.

3.3 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.

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.

3.4 Networks

3.4.1 Restrict Inbound Network Traffic

IT staff must ensure that all inbound traffic from external networks including the Internet and third parties is restricted based on documented business requirements.

3.4.2 Restrict Outbound Network Traffic

IT staff must ensure that all outbound traffic is restricted based on documented business requirements.

3.4.3 Segregate Internal Networks

IT staff must implement and enforce isolation and segregation of networks, systems, services, and devices between development, test, and production environments.

3.4.4 Configure Internal Networks using RFC 1918

IT staff must configure internal network to use an RFC 1918 addressing scheme.

3.4.5 Authentication Standards

IT staff must implement an authentication standard for all remote connections including workforce members and third parties. (SHIN-NY 3.3 §2.1.6)

3.4.6 Configure Electronic Messaging to Prevent Malware

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

3.4.7 Information Exchange Standards

The Technology Director must establish and communicate requirements for the secure exchange of information both internally and with third parties.

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 Maintain Technical Countermeasures

IT staff must ensure that technical countermeasures are deployed, operational, and are using signatures or updates that are current according to organizational standards.

3.5.4 Restrict Access to System Settings

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

3.5.5 Protect Network Devices

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

3.5.6 Synchronize Time on Systems and Devices

IT staff must establish and implement time synchronization to support time-based correlation of events and logs.

3.5.7 Data Loss Prevention

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

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.

3.8 Controls Against Malicious Code

3.8.1 Control Access and Changes to Prevent Malware

IT staff must ensure that system access and change management processes are deployed to help detect and prevent the spread of malicious software.

3.9 Input Data Validation

3.9.1 Document Input Validation and Error Checking

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

3.9.2 Review Security in Application Development Processes

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

3.10 Security Requirements Analysis and Specification

3.10.1 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.

3.10.2 Include Security in Acquisition

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

3.10.3 Include Security in Third-party Agreements

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

3.10.4 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.

3.10.5 Disable Risky Functionality in Products

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

3.11 Outsourced Software Development

3.11.1 Establish Source Code Ownership and Security

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

4 Procedures

Procedures to implement these policies are documented separately.

5 Enforcement

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

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

Incident Reporting

Information Security Policy
Policy No. SP-010

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 or weakness 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.

3.3 Incident Response

3.3.1 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.

3.4 Incident Assessment and Escalation

3.4.1 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))

3.5 Incident Response

3.5.1 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.

3.5.2 Contain Incidents and Identify Resolutions

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

3.5.3 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, when appropriate or when required by applicable laws, regulations, or standards.

3.5.4 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.

3.5.5 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 and applicable laws, regulations, and standards.

3.5.6 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.

3.6 Incident Resolution

3.6.1 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))

3.6.2 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))

3.6.3 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.

3.7 Detection Systems

3.7.1 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.

3.8 Incident Reporting

3.8.1 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.

3.9 Incident Response Management

3.9.1 Reporting and Escalation

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

3.9.2 Consistent Incident Response Processing

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

3.9.3 Test Incident Response

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

3.10 Management Reporting

3.10.1 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 and to support future incident response activities. (HIPAA §164.308(a)(1)(ii)(D))

3.10.2 Provide Incident Reporting

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

3.11 Training

3.11.1 Provide Incident Reporting Training

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

3.11.2 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 review and approve HEALTHeLINK's contingency plan. (HIPAA §164.308(a)(7)(i))

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. (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.

3.3 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 information systems and facilities 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 and, if necessary, revise HEALTHeLINK's contingency plans. (HIPAA §164.308(a)(7)(ii)(D))

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.

3.5 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 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 as a component of HEALTHeLINK's business continuity framework.

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.

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.

3.2 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 7 years on digital storage media stored in secure areas. (SHIN-NY 3.3 §6.1.5)

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

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.

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.

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.

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 access of information via the SHIN-NY governed by a QE, such as, for example, queries made by Authorized Users, type of information accessed, information flows between the QE and Participants, and date and time markers for those activities.

AUTHORIZED PURPOSES

QEs and their Participants shall permit Authorized Users to access Protected Health Information of a patient via the SHIN-NY governed by a QE 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 to access patient data via the HIE in accordance with the Terms and Conditions and the 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 QE 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; (ii) 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 a QE or 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 a QE or Participant to another person authorized to access Protected Health Information at the same QE 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 a QE 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 a QE that is used by a Participant to access Protected Health Information from the QE on an automated, system-to-system basis without direct access to the QE'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.

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.

DATA INTEGRITY

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

DATA SUPPLIER

Data Supplier means an individual or entity that supplies Protected Health Information to or through a QE. Data Suppliers include both Participants and entities that supply but do not access Protected Health Information via the SHIN-NY governed by a QE (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 it satisfies the requirements of 45 CFR § 164.514(b).

DEMOGRAPHIC INFORMATION

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

DESIGNATED RECORD SET

The same meaning as the term "Designated Record Set", as defined in 45 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.

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 or the NewYork 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 a QE 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.

HEALTHELINK INFORMATION

Information for which HEALTHeLINK fulfills the role of Information Owner.

HEALTH INFORMATION EXCHANGE (HIE)

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

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. Department of Health and Human Services.

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

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 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 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 direct identifiers of the individual or of relatives, employers, or household members of the individual. Data may be considered a limited data set only if it satisfies the requirements of 45 CFR § 164.514(e3).

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.

MINOR

A person under eighteen (18) years of age.

MINOR CONSENTED SERVICES

Healthcare services provided to a minor that generate Minor Consent Information

MINOR CONSENT INFORMATION

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.

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

NYSDOH means the New York State Department of Health.

ONE-TO-ONE EXCHANGE

A disclosure of Protected Health Information by 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 exchanged. 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 a QE and accesses Protected Health Information via the SHIN-NY governed by a QE.

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 a QE and each of its Participants, which sets forth the terms and conditions governing the operation of the QE and the rights and responsibilities of the Participants and the QE with respect to the QE.

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 a QE and is sent by the QE to subscribing recipients but does not allow the recipient to access any Protected Health Information through the QE 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.

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

Privacy Officer is 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, 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 a QE and accesses Protected Health Information via the SHIN-NY governed by a QE.

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 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 Guidance.

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, queriable 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

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.

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

A set of agreements (and the transactions, relations and data that are created by and through such set of agreements) between the NYSDOH, its contractors, QEs and Participants to make possible the exchange of clinical information among Participants for authorized purposes to improve the quality, coordination and efficiency of patient care, reduce medical errors and carry out public health and health oversight activities, while protecting privacy and security. Pursuant to such agreements, the QEs and the Participants agree to be bound by policy and technical requirements in SHIN-NY Policy Standards that has been created through the Statewide Collaboration Process.

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 single entity that: (1) has been designated by the Governor as eligible to receive from the federal government state grants to promote health information technology and conforms to federal requirements to receive such awards, or that has been certified by the Commissioner of Health as meeting the requirements of 10 NYCRR Part 300; (2) is a not-for-profit entity that includes on its board of directors representation from a broad range of SHIN-NY stakeholders; (3) demonstrates that its principal purpose is to serve the people of the State of New York by using information technology to create and maintain the SHIN-NY; and (4) adopts nondiscrimination and conflict of interest policies that demonstrate a commitment to open, fair, and nondiscriminatory participation by SHIN-NY stakeholders.

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 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.

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)).

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).

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
Revision Effective Dates: 06/25/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16, 07/01/18

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
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
Revision Effective Dates: 10/14/10, 04/25/13, 06/01/13, 06/30/16, 11/27/17, 07/01/18

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

Breach Response
Policy P06
Effective Date: 06/29/08
Review Dates: 05/26/16, 10/26/17, 05/24/18

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

Privacy Complaints/Concerns
Policy P07
Effective Date: 09/13/07
Review Dates: 05/26/16, 10/26/17, 05/24/18
Revision Effective Dates: 05/14/09, 07/13/09, 04/25/13, 06/01/13, 06/30/16

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

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

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

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
Revision Effective Dates: 06/30/16, 07/01/18

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

Audit
Policy P16
Effective Date: 11/27/17
Review Dates: 05/24/18

Security Policies

Participant Requirements
Policy SP-001
Effective Date: 09/13/07
Review Dates: 01/15/15, 05/19/16, 05/24/18
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
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18

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

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

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

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

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

Access Control
Policy SP-008
Effective Date: 09/13/07

Review Dates: 01/15/15, 05/19/16, 05/24/18
Revision Effective Dates: 01/15/15, 06/30/16, 07/01/18

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

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

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

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

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