



HEALTHeLINK™

HEALTHeLINK POLICIES

HEALTHeLINK Policies
Table of Contents

Privacy	Policy Name	Policy #	Policy Manual Page
	Compliance with Law and HEALTHeLINK Policies	P01	2
	Amendment of Data	P02	4
	Minimum Necessary Access	P03	5
	Patient Consent	P04	7
	Request for Restrictions or Confidential Communications	P05	13
	Breach Response	P06	14
	Privacy Complaints/Concerns	P07	17
	Use and Disclosure of Protected Health Information (PHI)	P08	18
	Sanctions for Failure to Comply with HEALTHeLINK Privacy & Security Policies	P09	20
	Participant Workforce Training for HIPAA Privacy & Security Standards	P10	22
	Workforce, Agent and Contractor Access to and termination from HEALTHeLINK	P11	23
	Accounting of Disclosures	P12	25
Security	Policy Name	Policy #	Policy Manual Page
	Elysium User Access Request and Standard Elysium User License Agreement/Confidentiality Agreement	S01	27
	Records Retention	S02	30
	Audit Reporting	S03	31
	Data Maintenance and Filtering	S04	33
	Secure Transport	S05	35
	Physical Security Policy	S06	36
	Data Security Policy	S07	38
	Elysium Application Security	S08	41
	Disaster Recovery/Business Continuity Plan	S09	45
	Access Via External Networks	S10	46
Glossary	Policy Name		
	Glossary	PGL	48



PRIVACY POLICIES



Title of Policy: Compliance with Law and HEALTHeLINK Policies	Policy # P01
Effective Date: 09-13-07	Revision Effective Date: 07-13-09

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

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.

II. Who Should Know This Policy

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.

III. Definitions

N/A

IV. Procedures

A. Law

1. Each Participant will, at all times, comply with all applicable federal, state, and local laws and regulations, including, but not limited to, those protecting the confidentiality and security of individually identifiable health information and establishing certain individual privacy rights.
2. Each Participant will use reasonable efforts to stay abreast of any changes or updates to, and interpretations of such laws and regulations to ensure compliance.

B. HEALTHeLINK Policies

1. Each Participant will, at all times, comply with all applicable HEALTHeLINK policies and procedures (“HEALTHeLINK Policies”).
2. HEALTHeLINK Policies may be revised and updated from time to time upon reasonable written notice to Participant. Each Participant is responsible for ensuring it has, and is in compliance with, the most recent version of these HEALTHeLINK Policies.

C. Participant Policies

1. Each Participant is responsible for ensuring that it has the requisite, appropriate, and necessary internal policies for compliance with applicable laws and HEALTHeLINK Policies.

2. In the event of a conflict between HEALTHeLINK Policies and an institution's own policies and procedures, the Participant will comply with the policy that is more protective of individual privacy and security.

V. References

- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Amendment of Data		Policy # P02
Effective Date: 09-13-07	Revision Effective Date: 07-13-09	

Review Date:							
Revision Date:	06/25/09						
Policy Replacing:							

I. Statement of Policy

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 protected health information.

Who Should Know This Policy

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.

II. Definitions

N/A

III. Procedure

- A. All requests for amendments and/or correction must go through the data source Participants, not through HEALTHeLINK.
- B. If an individual requests, and the Participant accepts, an amendment to the health information about the individual, the Participant shall make reasonable attempts to inform other Participants that accessed or received such information through the Clinical Information Exchange.
- C. The fact that there is an amendment must be flagged in the Axolotl software so all providers will be aware of the change.

IV. References

- 45 CFR 164.526.
- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation



Title of Policy: Minimum Necessary Access		Policy # P03	
Effective Date: 09-13-07		Revision Effective Date: 07-13-09	

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

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.

II. Who Should Know This Policy

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.

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedure

A. Uses

1. Each Participant will use only the minimum amount of health information obtained through HEALTHeLINK as is necessary to accomplish the intended purpose for which the information was accessed.
2. Each Participant will share health information obtained through HEALTHeLINK with and allow access to such information by only those workforce members, agents, and contractors who need the information in connection with their job function or duties.
3. Each Participant must identify that person or class of persons as appropriate, in its workforce, including physicians and their staff, who need access to PHI to carry out their duties.

B. Disclosures by HEALTHeLINK for Public Health Reporting

HEALTHeLINK will disclose only the minimum amount of health information necessary for the purpose of meeting reporting requirements.

C. Access

Each Participant will access only the minimum amount of health information through HEALTHeLINK as is necessary for the intended purpose.

D. Entire Medical Record

1. A Participant will not use, disclose, or access an individual's entire medical record except where specifically justified as the amount that is reasonably necessary to accomplish the purpose of the use, disclosure, or access.
2. This limit does not apply to disclosures to or request by a health care provider for treatment purposes or disclosures required by law.

V. References

- 45 CFR 164.514(d)(2)(i). *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Patient Consent		Policy # P04	
Effective Date: 09-25-08		Revision Effective Date: 8/23/2010	

Review Date:	10/13/2010						
Revision Date:	10/14/2010						
Policy Replacing:							

I. Statement of Policy

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

II. Who Should Know This Policy

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.

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedure

A. General Considerations

1. Unless an exception applies (see Section IV-D, E, F, and G below), affirmative consent of the patient must be obtained before a Participant may access a patient’s health information. This is done by utilizing a HEALTHeLINK Consent form for either Level 1 uses or Level 2 uses.
 - a. Level 1 uses are uses for treatment, quality improvement, care management and insurance coverage (pre-authorization) reviews. (See the HEALTHeLINK Policy Glossary for definition of terms.)
 - b. Level 2 uses are for uses other than Level 1 uses, including but not limited to payment, research, and marketing. (See the HEALTHeLINK Policy Glossary for definition of terms.)

2. HEALTHeLINK Level 1 and Level 2 consent forms must be approved by the New York State Department of Health prior to implementation.

3. Patients need to be aware that, once they give consent, **all** of their health information will be available through HEALTHeLINK. No partial or filtered data will be available through HEALTHeLINK.
4. If a patient consents, the information accessible through HEALTHeLINK will include the following sensitive information:
 - a. HIV-related Information (New York State Public Health Law, Article 27-F)
 - b. Mental health information (New York State Mental Hygiene Law §33.13)
 - c. Genetic testing information (New York State Civil Rights Law §79-1)
 - d. Sexually transmitted disease and abortion information (New York State Public Health Law §17)
 - e. Reproductive health information (New York State Public Health Law §2305 and 2504)
 - f. Alcohol and substance abuse information (42 CFR Part 2).
5. All patient consents must be in writing on a HEALTHeLINK Consent form and flagged in the HEALTHeLINK software. HEALTHeLINK Consents include:
 - a. *Patient Consent to Participate in HEALTHeLINK Health Information Exchange – Level 1 Multi-Payer/Multi-Provider Consent*
 - b. (Level 2 consents to be developed.)
6. HEALTHeLINK will maintain copies of all patients’ written consents.
7. Patients may withdraw their consent at any time upon written request.
 - a. The HEALTHeLINK “Withdrawal of Consent to Participate in HEALTHeLINK Health Information Exchange” form may be used to provide withdrawal request; or
 - b. A new HEALTHeLINK Consent form may be completed in which the patient denies access to information contained in the health information exchange.
 - c. Changes in Consent status must be flagged in the HEALTHeLINK software.
8. Patients may refuse to consent to the access of their health information through HEALTHeLINK (“deny consent”).
 - a. Patient denial of consent must be in writing on a HEALTHeLINK Consent form with one of the “Deny Consent” options (either “No Except” or “No Never”) checked and flagged in the HEALTHeLINK software.
 - b. Patients may deny consent “except in a medical emergency” or they may deny consent “including in a medical emergency.”
 - c. A patient’s decision not to sign a consent form will not be construed as a denial of consent.

N.B.: 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 health information except in an emergency.

9. Providers/Payers must not condition treatment/coverage on the patient's willingness to consent to the access of their health information through HEALTHeLINK.
10. Patients will be provided, or instructed on where to obtain, a list of HEALTHeLINK Participants and data suppliers at the time they give consent authorizing access of their protected health information through HEALTHeLINK.

B. Patient Consent

1. Unless an exception applies (see Section IV-D, E, F, and G below), the Participant will be unable to access a patient's health information through the HEALTHeLINK clinical information exchange until the individual patient has been given an opportunity to consent, in writing, to the exchange.
2. The Participant will document the patient's consent on the HEALTHeLINK Consent form and indicate the patient's consent in the HEALTHeLINK software.
3. The Participant will forward a copy of the Consent to HEALTHeLINK within three (3) business days of obtaining the Consent.
4. If the patient wishes to withdraw his/her consent, the Participant will obtain the patient's written request to withdraw consent, change the patient's preference in the HEALTHeLINK software, and forward a copy of the written withdrawal to HEALTHeLINK.
5. If a patient withdraws his/her consent, data that has been accessed by the Participant up to the time of withdrawal will remain as part of the Participant's records.

C. Consent for Minors

1. In New York State, a minor is anyone under the age of 18.
2. Minors under ten years of age:
 - a. Unless an exception applies (see Section IV-D, E, F, and G below), Participants may access the health information of a minor **under ten years of age** based on a HEALTHeLINK Consent executed by the minor's parent or legal guardian.
 - b. Parents that share joint custody of the minor have equal authority to provide written consent for the minor.
 - a. If a court order clearly permits one parent to make health care decisions for a minor, that parent has the authority to provide written consent for the minor. If the court order is not clear as to which parent has the authority to make health care decisions, either parent may provide written consent for the minor.

- b. Foster parents or other individuals who have legal custody (but not guardianship) must provide written documentation to evidence their legal authority to consent before the Participant accepts their written consent to access the health information of the minor.
3. Minors ten years of age or older:
 - a. If the minor's parent or legal guardian consented, in writing, to the access of the minor's health information through HEALTHeLINK prior to the minor turning ten (i.e., the minor was age 0 to 10), access to the minor's health information will be terminated by the software on the minor's tenth birthday.
 - b. Status of the consent will become "No Except" which will allow for access to the minor's information in a medical emergency.
 - c. No access to a minor's health information will be permitted between the minor's tenth and eighteenth birthdays except in an emergency
4. When the patient reaches the age of majority (18th birthday), the Participant must obtain the written consent of the (adult) patient in order to access his/her health information through HEALTHeLINK.

D. Exception: Up-Loading Data

1. HEALTHeLINK holds patient data solely as a custodian of the Participants. HEALTHeLINK, as a business associate of the Participants, does not make patient information accessible to other Participants until patient consent is obtained.
2. Since the storage of data is not treated as a "disclosure" to a third party requiring consent under New York law, Participants may upload patient information to HEALTHeLINK without patient consent.

E. Exception: "One-To-One" Electronic Health Information Exchange.

1. Participant practitioners receiving one-to-one information will be notified via the HEALTHeLINK software of the availability of the information through the clinical information exchange. (See the HEALTHeLINK Policy Glossary for definition of terms.)
2. Each one-to-one exchange is understood and predictable to the patient, and information is limited in scope to that of the two exchanging providers. Therefore, affirmative patient consent is not needed for one-to-one exchange of health information. However, if a patient requests limitations on the disclosure of his/her information electronically through the HEALTHeLINK clinical information exchange, the practitioner may comply with this request. (See HEALTHeLINK policy PO5, *Request for Restrictions or Confidential Communications*.)

3. NYS laws requiring written consent for the disclosure and re-disclosure of sensitive information as identified in Section IV-A-4 above still apply to the one-on-one exchange of health information. Providers should utilize their own consent forms for this purpose as applicable.

F. Exception: Access to Patient Health Information in an Emergency Situation

1. Affirmative consent is not required for a practitioner to access patient health information in an emergency. An “emergency condition” means a medical or behavioral condition, the onset of which is sudden, that manifests itself by symptoms of sufficient severity, including severe pain, that a prudent layperson, possessing an average knowledge of medicine and health, could reasonably expect the absence of immediate medical attention to result in:
 - a. Placing the health of the person afflicted with such condition in serious jeopardy, or in the case of a behavioral condition, placing the health of such person or others in serious jeopardy; or
 - b. Serious impairment to such person’s bodily functions; or
 - c. Serious dysfunction of any bodily organ or part of such person; or
 - d. Serious disfigurement of such person.
2. Patient information will be accessible through HEALTHeLINK to Participant practitioners without patient consent in an emergency situation in which the patient’s condition meets the definition of “emergency condition” as defined above (Section IV-F-1), the patient has not denied consent “including in an emergency” and:
 - a. The patient is unconscious or other wise unable to give or withhold consent, **and**
 - b. The treating practitioner determines that information that may be held by HEALTHeLINK may be material to treatment.

NOTE: “Unable to give or withhold consent” means that the patient’s condition is such that he/she is unable to make a rational and competent decision regarding the use and disclosure of his/her health information, or to communicate such decision by any means. The patient’s condition could result from illness, the influence of alcohol or some other substance, physical or psychological disabilities, or some other cause.

3. The treating practitioner must attest in the HEALTHeLINK software that **both** of the above (Section IV-F-2-a and b) conditions apply. He/She will then be allowed to “break the glass” and access the patient’s information.
4. The right to “break the glass” terminates with the completion of the emergency treatment. If the practitioner seeks to access the patient’s health information after the emergency has ended, he/she must comply with patient consent requirements (Section IV-A through F).
5. HEALTHeLINK will maintain a record of “break the glass” access.

G. Exception: Public Health Reporting

If a data supplier is permitted to disclose protected health information to a government agency for the purposes of public health reporting without patient consent under applicable state and federal laws and regulations, HEALTHeLINK may make that disclosure on behalf of the data supplier without the patient's affirmative consent. (See the HEALTHeLINK Policy Glossary for definition of terms.)

- NOTE:** (1) **Patient consent must be in compliance with state and federal Limited English Proficiency requirements.**
- (2) **Conflicts between a patient's right to privacy and a Participant's need to know should be resolved in favor of patient privacy, except where that would result in serious health hazard or harm to the patient or others.** (AMA Policy H-140.989, Informed Consent and Decision-Making in Health Care)

V. References

- 45 CFR Part 164
- 42 CFR Part 2
- 42 CFR §489.24
- 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
- American Medical Association Policy H-140.989
- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation.
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 2*



Title of Policy: Request for Restrictions or Confidential Communications	Policy # P05
Effective Date: 09-13-07	Revision Effective Date: 07-13-09

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

HEALTHeLINK Participants who agree to individuals’ request for restriction or request for confidential communications due to endangerment, or use of their PHI must comply with such request with regard to the release of information to HEALTHeLINK.

II. Who Should Know This Policy

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.

III. Definitions

N/A

IV. Procedure

- H.** All requests for restrictions or request for confidential communications must go through the Participants, not through HEALTHeLINK.
- I.** If a Participant agrees to an individual’s request for restrictions or confidential communications, the Participant shall ensure that it complies with the restrictions or confidential communications when releasing information obtained through HEALTHeLINK.

V. References

- 45 CFR 164.522.
- HEALTHeLINK Data Maintenance and Filtering Security Policy
- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation



Title of Policy: Breach Response		Policy # P06	
Effective Date: 06/29/08		Revision Effective Date: 09/16/11	

Review Date:							
Revision Date:	05/14/09	04/01/10	9/16/11				
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to provide notification of breaches of unsecured protected health information (PHI) in accordance with the procedures set forth herein and in compliance with the HITECH Act. The breach notification provisions of the HITECH Act apply to HIPAA covered entities and their business associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, use, or disclose unsecured protected health information.

HEALTHeLINK is the business associate of the covered entities participating in the clinical information exchange.

II. Who Should Know This Policy

HEALTHeLINK and its Participants including but not limited to those who access the HEALTHeLINK system and/or transport protected health information contained therein, as well as those who maintain the HEALTHeLINK hardware and software.

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedures

- A. HEALTHeLINK will use appropriate administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of protected health information.
- B. **Periodic Audits to be conducted by HEALTHeLINK**
 - 1. Audits are useful oversight tools for recording and examining access to information through HEALTHeLINK and are necessary for verifying compliance with access controls developed to prevent/limit inappropriate access to information.
 - 2. HEALTHeLINK must conduct audits at least annually and submit audit reports, including identification of breaches, to the Board.
- C. HEALTHeLINK will implement reasonable and appropriate technologies and methodologies designed to prevent the unauthorized disclosure of unsecured PHI. "Unsecured PHI" means protected health information that is not secured through the use of approved technologies or methodologies. To be approved, technologies and

methodologies must render PHI unusable, unreadable, or indecipherable to unauthorized individuals, as described in **Procedure D** below.

If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not “unsecured PHI.”

- D.** Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals:
1. **Encryption.** HEALTHeLINK will implement and maintain reasonable and appropriate encryption technologies and methodologies to enhance the protection of PHI.
 2. **Destruction.** HEALTHeLINK will implement destruction techniques that render PHI unusable and/or unreadable in any format.
- E. HEALTHeLINK Personnel Reporting Requirements**
1. HEALTHeLINK personnel, 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 Security Officer/designee.
 2. The HEALTHeLINK Security Officer/designee will report the breach or suspected breach to the effected Data Supplier(s), in writing, within twenty-four (24) hours of HEALTHeLINK becoming aware of such breach.
 - a. HEALTHeLINK will include in the report, or provide to the Data Supplier(s) as promptly thereafter as the information becomes available, the following:
 - 1.) Identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, used or disclosed;
 - 2.) A brief description of what happened, including the date of the breach and the date of the discovery of the breach.
 - b. HEALTHeLINK will not contact any individuals suspected to be affected by the breach without prior written approval of the effected Data Supplier(s).
 3. HEALTHeLINK will:
 - a. Investigate the scope and magnitude of the breach.
 - b. Identify the root cause of the breach
 - c. Mitigate, to the extent possible, damages caused by the breach.
 - d. If applicable, request the party who received such information to return and/or destroy the impermissibly disclosed information.
 - e. Apply sanctions as appropriate.
 4. If the breach includes patient information contained in the nationwide health information network ("NwHIN"), HEALTHeLINK will comply with the breach notification requirements of NwHIN participants contained in the Data Use and Reciprocal Support Agreement ("DURSA") signed by HEALTHeLINK.
 5. If applicable, HEALTHeLINK will report security breaches as required by the New York State Information Security Breach and Notification Act.
 6. HEALTHeLINK will notify the HEALTHeLINK Operating Committee and the HEALTHeLINK Board of Directors of the breach.

V. References

HEALTHeLINK Error Handling Policy

N.Y. State Information Security Breach and Notification Act (NY General Business Law §899-aa)

HEALTHeLINK Policy # P07, Privacy Complaint/Concerns

HEALTHeLINK Policy # P09, Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies

NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*

Restatement I of the Data Use and Reciprocal Support Agreement (DURSA). Version Date: May 3, 2011

HITECH Act



Title of Policy: Privacy Complaints/Concerns		Policy # P07
Effective Date: 09-13-07	Revision Effective Date: 07-13-09	

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

Each HEALTHeLINK Participant shall have a mechanism for, and shall encourage all workforce members, agents, and contractors to report any non-compliance with these policies to the Participant. Each Participant also shall 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.

II. Who Should Know This Policy

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.

III. Definitions

N/A

IV. Procedures

- A. Any complaints/concerns about confidentiality will be reported to the affected entity’s HIPAA Privacy Officer for standard follow-up.
- B. On completion of the investigation, a summary of complaint/concern will be sent to the HEALTHeLINK Executive Director.
- C. Steps to mitigate could include, among other things, data source Participant notification to the individual of the disclosure of information about them, or Participant requests to the party who received such information to return and/or destroy the disclosed information.
- D. The HEALTHeLINK Executive Director will archive the summaries of the complaints/reports for later reporting and discussion.

V. References

- HEALTHeLINK Policy # P06, Breach Response
- HEALTHeLINK Policy # P09, Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Use and Disclosure of Protected Health Information (PHI)	Policy # P08
Effective Date: 06/29/08	Revision Effective Date: 07-13-09

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to protect health information of its patients and to use and disclose protected health information as permitted and required.

II. Who Should Know This Policy

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

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedures

- 1) All access to protected health information (PHI) through HEALTHeLINK will be consistent with applicable federal, state and local laws and regulations. If applicable law requires that certain documentation exists or that other conditions be met prior to accessing PHI for a particular purpose, the Participant will ensure that the required documentation has been obtained or the requisite conditions have been met and be able to provide evidence of such as applicable.
- 2) All Participants will use appropriate safeguards to prevent unauthorized use or disclosure of PHI, including administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of that PHI.
- 3) PHI may be used to create de-identified information. De-identified information created in accordance with the HIPAA Privacy Rule (45 CFR §164.514(a)) is not subject to the requirements of this policy unless it is re-identified. Disclosure of a key or mechanism that could be used to re-identify such information is considered disclosure of protected health information and as such would be subject to the requirements of this policy.
- 4) HEALTHeLINK will not use or disclose PHI in any manner that violates HEALTHeLINK’s business associate agreements.

- 5) HEALTHeLINK, acting under the authority of a business associate agreement with its Participants, may disclose PHI to vendors that assist in carrying out HEALTHeLINK's authorized activities provided:
 - i. HEALTHeLINK requires the vendors to protect the confidentiality of PHI in accordance with HEALTHeLINK's business associate agreements with its Participants, **and**
 - ii. The vendor does not make such information available to Participants without the patient's affirmative consent.

- 6) HEALTHeLINK will make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of the United States Department of Health and Human Services, or any other regulars as required, for purposes of determining the Participant's compliance with its legal obligations.

V. References

- 45 CFR Part 164
- 45 CFR Part 46
- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation.
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Sanctions for Failure to Comply with HEALTHeLINK Privacy and Security Policies		Policy # P09
Effective Date: 09-13-07	Revision Effective Date: 04/01/10	

Review Date:							
Revision Date:	05/14/09	04/01/10					
Policy Replacing:							

I. Statement of Policy

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 protected health information except as permitted by the HEALTHeLINK Privacy and Security policies and that they comply with these policies.

II. Who Should Know This Policy

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

III. Definitions

N/A

IV. Procedures

- A. Any breach of confidentiality reported to the individual HEALTHeLINK Participant (see Privacy Complaints/Concerns Policy #P07 and Breach Response Policy #P06) will be handled according to the individual Participant’s HIPAA Privacy and Security Policies.
- B. Any breach of confidentiality reported to HEALTHeLINK (see Privacy Complaints/Concerns Policy #P07 and Breach Response Policy #P06) 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. Such sanctions may include, but not be limited to, verbal or written warnings, required retraining, suspension without pay, and termination of contract or employment.
- 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. Such sanctions may include, but not be limited to, verbal and written warnings, termination of individual user access, and termination of participation in HEALTHeLINK.

V. References

- HEALTHeLINK Policy #P06, Breach Response
- HEALTHeLINK Policy # P07, Privacy Complaints/Concerns
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Participant Workforce Training for HIPAA Privacy and Security Standards	Policy # P10
Effective Date: 06/29/08	Revision Effective Date: 07-13-09

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

It is required that HEALTHeLINK Participants’ workforce be trained regarding the HEALTHeLINK privacy and security policies/standards. The HEALTHeLINK Participant/consumer education standards conform to the consumer education program standards approved by the New York State Department of Health. Once initial training is completed by HEALTHeLINK, the Participants are responsible for ensuring that the training information is communicated to new members of their workforce, as well as any consultants and vendors who work with them and use HEALTHeLINK.

II. Who Should Know This Policy

- HEALTHeLINK Participants and their respective workforces
- HEALTHeLINK administrators
- Axolotl workforce managing/working with the HEALTHeLINK network

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedures

1. To support HEALTHeLINK’s commitment to information privacy and security, both new and existing members of the workforce of each HEALTHeLINK Participant will be trained on all HEALTHeLINK privacy and security policies, including but not limited to those related to user access, use, transmission and/or disclosure of information, as well as patient/consumer consent.
2. Each Authorized user will sign a certificate that he/she has received training and will comply with all HEALTHeLINK policies and procedures. This certification will be kept on file by the training organization for at least six (6) years.

V. References

- 45 C.F.R. §164.530
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Workforce, Agent and Contractor Access to and Termination from HEALTHeLINK	Policy # P11
Effective Date: 09-13-07	Revision Effective Date: 07-13-09

Review Date:							
Revision Date:	05/14/09						
Policy Replacing:							

I. Statement of Policy

In accordance with the requirements of the Health Insurance Portability and Accountability Act (HIPAA) with respect to privacy principles of use limitation, security safeguards and controls, accountability and oversight, data integrity and quality, and remedies, HEALTHeLINK participants shall comply and make reasonable efforts to limit or determine access as needed and use of protected health information (PHI) available through the HEALTHeLINK System.

In doing so, the HIPAA requirements for workforce training, sanctions for privacy/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/security practices, and the prompt identification of and undertaking of remedial action for privacy/security violations.

II. Who Should Know This Policy

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.

III. Definitions

See HEALTHeLINK Policy Glossary

IV. Procedures

E. 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.

F. Access Control

1. Each Participant shall monitor and allow access to the HEALTHeLINK System only by those workforce members, agents, and contractors who have a legitimate and appropriate need to use the HEALTHeLINK System and/or release or obtain information through the HEALTHeLINK System.
2. Each Participant is responsible to oversee the activities of its Authorized Users.

3. Each Participant shall 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 one business day of termination.
4. Any violation, by an Authorized User or any other individual who accesses the HEALTHeLINK system either through the Participant or by use of any log-on, password, etc., received or obtained from the Participant or the Participant's Authorized Users, will be cause for suspension or termination of access to the HEALTHeLINK system.
5. HEALTHeLINK will terminate access in the following situations:
 - a. Immediately or as promptly as reasonably practicable but in any event within one business day of termination of a Participant's Participation Agreement with HEALTHeLINK; and/or
 - b. Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an authorized user's employment or affiliation with the Participant.

V. References

- 45 C.F.R. § 164.530
- HEALTHeLINK Policy #P09, Sanction for Failure to Comply with HEALTHeLINK Privacy & Security Policies
- *The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange*, ©2006, Markle Foundation
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



Title of Policy: Accounting of Disclosures		Policy # P12	
Effective Date: 09-13-07		Revision Effective Date: 04/01/10	

Review Date:							
Revision Date:	06/25/09	04-01-10					
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to provide information needed by a HEALTHeLINK Participant in order to respond to an individual’s request for an accounting of disclosures of his/her protected health information.

II. Who Should Know This Policy

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.

III. Definitions

N/A

IV. Procedure

- a. All patient requests for an accounting of disclosures must be made to the Participant that supplied the data (“Data Supplier”), not to HEALTHeLINK.
- b. HEALTHeLINK will provide disclosure information collected to the Data Supplier, in a time and manner reasonably designated by such Data Supplier, which will permit the Data Supplier to respond to a request by an individual for an accounting of disclosure.
- c. Individuals who contact HEALTHeLINK directly for an accounting of disclosure of their protected health information will be given information on contacting HEALTHeLINK Data Suppliers with their request.
- d. Any disclosure of patient information that is not in compliance with HEALTHeLINK Policy P08, Use and Disclosure of Protected Health Information, must be treated as a Breach. (See HEALTHeLINK Policy P06, Breach Response.)

V. References

- 45 CFR. § 164.528
- The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange, ©2006, Markle Foundation
- NYSDOH: *Privacy and Security Policies and Procedures for RHIOs and Their Participants in New York State. Version 1.0*



HEALTHeLINK™

SECURITY POLICIES



Title of Policy: Elysium User Access Request and Standard Elysium User License Agreement/Confidentiality Agreement		Policy # S01
Effective Date: 09-13-07	Revision Effective Date: 01-25-2010	

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

Each user of the HEALTHeLINK’s Elysium application will need to complete HEALTHeLINK Elysium Account Setup form before being granted a logon and password to access the application. The Participant Authoritative Source (PAS) will verify the information on the form based on authentication parameters setup by HEALTHeLINK and forward it to the HEALTHeLINK Help Desk to be setup. Users will be required to accept the ‘**Standard Elysium User License Agreement/Confidentiality Statement**’ within form in order to be granted access to the application. Users will also be required to acknowledge their acceptance of this statement when logging onto the application. If a user does not acknowledge their acceptance they will be denied access to the Elysium application.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

N/A

IV. Procedures

- a. User requesting access to HEALTHeLINK’s Elysium application must complete a HEALTHeLINK Elysium Account Setup form and sign off on the Standard Elysium Users License Agreement. Both the form and the agreement must be submitted to the Participant’s Authoritative Source (PAS) and forwarded to the Elysium Help Desk.

- b. The PAS will verify the information based on authentication parameters setup by HEALTHeLINK on the form and forward it to HEALTHeLINK Help Desk to be setup.
- c. The HEALTHeLINK Help Desk will directly issue each user a logon and password upon validation of DOB by that user, and communicate that all accounts have been established and furnished to the PAS.
- d. The HEALTHeLINK Help Desk will maintain a database of user information.
- e. Periodically the HEALTHeLINK Help Desk will verify the accuracy of the user information and the need for the user access.
- f. Users must accept the ‘**Standard Elysium User License Agreement/Confidentiality Statement**’ within Elysium in order to launch into a session. If a user does not ‘accept’ the statement, they are immediately logged off of Elysium. Note: a user will be unable to conduct any activity within Elysium until/unless they accept the electronic statement.

V. References

HEALTHeLINK Elysium Account Setup form

Confidentiality Acknowledgement

As a condition to your access and use of the HEALTHeLINK System, you must read this Confidentiality Acknowledgment and click to confirm your agreement below.

The HEALTHeLINK System will provide you access to Protected Health Information (PHI) submitted to HEALTHeLINK by participating providers. You or your employer have already signed a participation agreement that imposes certain restrictions on your use and disclosure of PHI from the HEALTHeLINK System. This acknowledgment is a reaffirmation of the participation agreement, and shall in no way be interpreted as limiting the restrictions set forth therein.

I acknowledge and agree as follows:

- I am an Authorized User of the HEALTHeLINK System, authorized by HEALTHeLINK and my employer and granted a distinct user name and password. I will safeguard this password and not allow others to use it.
- I will access through the HEALTHeLINK System information relating only to individuals with whom I have a health care treatment or health care payer

relationship. I will not disclose such information to any third party without the consent of HEALTHeLINK.

- I will undertake a reasonable and professional degree of care to protect the confidential nature of any information accessed from the HEALTHeLINK System.
- I have received training on HEALTHeLINK's Policies and Procedures, and agree to comply fully therewith. I will notify HEALTHeLINK immediately of any breach of such Policies and Procedures of which I become aware.
- I will comply with all applicable federal, state and local laws, rules and regulations with regard to access, use and disclosure of PHI.
- I acknowledge that any breach of this Confidentiality Acknowledgment may result in modification, suspension or revocation of my access to the HEALTHeLINK System, and/or disciplinary measures by my employer, up to and including termination of employment.



Title of Policy: Records Retention				Policy # S02			
Effective Date: 09-13-07				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to govern the historical time period that electronic clinical/medical records (Medical data) will be retained within the HEALTHeLINK/Elysium infrastructure, as well as data source databases. The policy establishes controls to ensure the proper management of electronic medical records, which are the property of HEALTHeLINK, and are required to satisfy both federal and New York State regulatory requirements.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

See HEALTHeLINK Privacy & Security Policy Glossary

IV. Procedures

- A. Clinical/Medical records shall be retained for six years from the date of discharge or death, or for residents who are minors, for three years after the resident reaches the age of majority. (18)
- B. Clinical/Medical information, in excess of 10 years old, will be compressed and archived to digital storage media within the data center. The archived data will be subject to normal back-up policies and procedures.
- C. Elysium audit reporting records retention will be governed by the ‘Audit Reporting’ Policy S03 Audit Reporting.

V. References

Title 10 NYCRR §415.22(b)



Title of Policy: Audit Reporting		Policy # S03
Effective Date: 09-13-07	Revision Effective Date:	

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to set forth appropriate practices to effectively log and audit all user activity with the HEALTHeLINK application. This policy supports the appropriate use and ensure patient confidentiality, maintain secure operations, support investigations of privacy breaches and responding to requests from consumers about accesses to their information that were mediated by the HEALTHeLINK. This policy shall also establish a procedure for third party requests of the audit logs. This policy complies with Federal and State laws.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

See HEALTHeLINK Privacy & Security Policy Glossary

IV. Procedures

A. Logging

- a) The Elysium application will appropriate log all user activity including: end user login/logoff date and time, device address, actions taken by each user, content; type of data being accessed/activity begin performed and date/time of each event. All security and system administrative functions will be included in this log.
- b) All logged activity will be retained on-line and accessible within the Elysium application for 180 days. Audit log information exceeding 180 days old and not exceeding 7 years old will be archived to digital storage media within the data center. Logs older than 7 years will not be maintained.
- c) All audit records will be protected against unauthorized access, modifications and deletions.

B. Request of Audit Report

- a) Requests for Audit Reports will be documented on an ‘Audit Request Form’ and recorded in an ‘Audit Request Log’
- b) A HEALTHeLINK workforce member, under the direction of the Executive Director, will be responsible for the creation and maintenance of an ‘Audit Request Form’ and ‘Audit Request Log’
- c) The HEALTHeLINK Executive Director will periodically report on the types of Audit Reports being requested to the Operating Committee.

V. References

HIPAA, 42 CFR Part 2

The Connecting for Health Common Framework: Auditing Access to and Use of a Health Information Exchange, ©2006, Markle Foundation.



Title of Policy: Data Maintenance and Filtering						Policy # S04	
Effective Date: 09-13-07				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to set forth appropriate practices for maintaining participant’s data and to effectively filter patient data according to Federal and State laws.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

N/A

IV. Procedures

- A. It is the responsibility of each data source provider to send data unfiltered to HEALTHeLINK.
- B. It is the responsibility of HEALTHeLINK to properly receive and protect this data from unauthorized access.
- C. It is the responsibility of HEALTHeLINK and the Elysium application to effectively filter patient data according to Federal and State laws.
- D. Each data source provider continues to own its data. HEALTHeLINK holds the data on behalf of each data source provider as a custodian and has no ownership rights in the data.
- E. If a data source provider leaves HEALTHeLINK, The provider’s data must be returned or destroyed, if possible, by HEALTHeLINK. One to one electronic health information exchanges made while a participant of the exchange will not be returned or destroyed.

V. References

NYS HIV Law: PHL Article 27-F

NYS MHL §§1.03 and 33.13

42 CFR Part 2

The Connecting for Health Common Framework: Resources for Implementing Private and Secure Health Information Exchange, ©2006, Markle Foundation



Title of Policy: Secure Transport				Policy # S05			
Effective Date: 09-13-07				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

This policy will address the way in which information is transmitted to and from data sources with regard to the HEALTHeLINK exchange infrastructure.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

See HEALTHeLINK Privacy and Security Policy Glossary

IV. Procedures

- A. Electronic information sent between two sites, across unsecured communication lines, will be encrypted using currently accepted, 128-bit or higher, encryption techniques.
- B. It's recommended that a firewall will exist at both the sender and receiver sites.

V. References

http://www.connectingforhealth.org/resources/collaborative_response/hie_model/6.php



Title of Policy: Physical Security Policy				Policy # S06			
Effective Date: 09-13-07				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

This policy defines the responsibilities of individual computer users with regard to the physical security of the HEALTHeLINK application. This policy complies with Federal and State laws.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

See HEALTHeLINK Privacy and Security Policy Glossary

IV. Procedures

HEALTHeLINK application and its data may not be transported without appropriate authorization, in accordance with HEALTHeLINK policies controlling inventory custody and transfers as well as make provisions to eliminate theft, fraud, destruction, or other abuses of HEALTHeLINK.

Copying of computer software, data, and manuals. Computer software, computer data, and/or software manuals may not be copied or transmitted electronically without appropriate prior consent.

HEALTHeLINK participants and members of its workforce accessing the HEALTHeLINK application must ensure that each workstation used to access the computer system is not misused or abused, and the workstation is located in an area in which access is restricted to authorized users only.

All devices accessing the HEALTHeLINK system must have updated anti-virus software loaded and a supported desktop operating system on the individual device.

Violations or suspected violations of computer resource security must be reported at once to the Executive Director of HEALTHeLINK.

V. References

Health Insurance Portability and Accountability Act (HIPAA) Public Law 104-191



Title of Policy: Data Center Security Policy						Policy # S07	
Effective Date: 6/29/08				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

It is the policy of HEALTHeLINK to set forth appropriate practices to effectively secure all data within the HEALTHeLINK clinical system. The policy establishes the principle that all data on computer systems purchased, licensed or otherwise inventoried by HEALTHeLINK must be protected from loss due to equipment failure, malicious code, denial of service attacks, and unauthorized access or removal. This policy complies with Federal and State laws.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

Participant Authoritative Source (PAS) - A representative of the participant who is responsible for managing the interaction between the Participant’s employees, agents & subcontractors AND HEALTHeLINK. This includes, but is not limited to, access and usage of HEALTHeLINK sponsored programs and applications.

IV. Procedures

A. Access Control

Access to the HEALTHeLINK system will be granted by the Executive Director of HEALTHeLINK. This may in turn be carried out by the management of the HEALTHeLINK data center for purposes of support. All access rights to the HEALTHeLINK system must be granted in writing. The data center will maintain lists of persons authorized to access the various administrative computer systems and their level of access. The HEALTHeLINK Executive Director or designee will review access rights on a yearly basis. All individuals authorized to access the HEALTHeLINK system are responsible for all activities occurring during their access. Users may not access HEALTHeLINK data center without appropriate

authorization and only for the purposes for which their access is authorized. Any attempt to access or to assist in the access of HEALTHeLINK via an unauthorized means is a violation of this policy and will be subject to disciplinary action, which may include but is not limited to termination of access to the system and dismissal of services and/or the employee(s) involved. Violators are also subject to civil or criminal liability.

The data center will provide an environment that restricts physical access to the computer system to the appropriately authorized users. As appropriate, the data center will have defined procedures for maintaining data integrity during hardware repair, will set up a schedule of preventive maintenance for the computer system, and will maintain a log of hardware malfunctions.

The data center will provide and implement reasonable security measures to protect the computer system against natural disasters, accidents, and deliberate attempts to damage the system.

The data center will take action to provide reasonable protection against such environmental threats as flooding, lightning, extreme temperatures, and loss or fluctuation of electrical power and will provide adequate disaster recovery plans and procedures, including use of off-site storage for critical systems data.

B. User IDs

Data center operations will assign each user of the HEALTHeLINK system a unique identification (i.e., a logon ID). Guest accounts are specifically prohibited except in cases fully documented and justified in writing to the HEALTHeLINK Executive Director. Management of the user ID and passwords will comply with the HEALTHeLINK user ID and password policy. Data centers using logon IDs will take steps to assure that user IDs and passwords are not stored in logon documents or executable files.

Data Center Management must authorize all contract vendor accounts before they have been created. Contract vendors will only be given access to the system that pertains to their contract. Individual user IDs shall be created for access from the remote connections. These accounts will expire on the date predetermined date (i.e. 30, 60, 90days) by the contract or on termination of the contract.

C. Remote Access

HEALTHeLINK computer resource which is accessible from a remote workstation via a dial-up communications line, VPN, wireless and which enables access to data centers providing administrative applications shall use strong authentication that validates user ID and password and industry best practice encryption.

Remote access either by VPN, dial up communications line or wireless HEALTHeLINK data network shall take reasonable steps to restrict the access of the dial-up user to only the HEALTHeLINK data for which the user is authorized and to restrict the visibility of HEALTHeLINK data for which the user is not authorized.

The procedures for the electronic transmission of any computerized institutional data to an entity external to the HEALTHeLINK should be documented and approved by the HEALTHeLINK Executive Director to ensure that they meet standards set by the State of New York and the Federal government.

The HEALTHeLINK network will maintain an up to date hardware firewall and will incorporate the use of proxy services and other software that aids in protecting the server and data stored on the server from intruders.

V. References

New York State Information Security Breach and Notification Act
Health Insurance Portability and Accountability Act (HIPAA) Public Law 104-191



Title of Policy: Elysium Application Security				Policy # S08			
Effective Date: 06/29/08				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

User Level Application Security is provided within the design of the Elysium application to ensure access is granted on a need-to-know basis and at the minimum access level necessary for each user to perform their job duties. There are different level of access that can be granted based on the roles and responsibilities of the user. The Elysium application consists of a large number of databases stored on a Domino platform. Access to the databases and the database records are solely through the web, and are secured using features contained within the platform through Domino IBM’s architecture. The application exploits the standard Domino architecture to provide additional application level security.

Users of the Elysium application are required to treat their IDs and password as sensitive and confidential information. IDs and passwords are prohibited from being shared and users are responsible for their use. All user accounts that have not logged on within 180 days will be disabled. Users will be automatically logged off of the Elysium Application after 15 minutes of inactivity.

II. Who Should Know This Policy

This policy applies to all participants of HEALTHeLINK that have registered with and are participating in HEALTHeLINK and its workforce members including employees, medical staff, contractors and volunteers.

III. Definitions

N/A

IV. Procedures

A. Elysium’s Application Security

a) Elysium User Attributes

Every end user of Elysium is described in detail in the Elysium Address Book. Any attributes of the user described in the address book can be used to enable or restrict access to databases and to functions within the database application.

b) User Type

The user type, often referred to as license type, determines whether an Elysium licensee can “logon” to Elysium. Some users such as Fax or Contacts have no login to Elysium but can still be defined in the address book. For those users who can log on, the primary user type determines the database design that will be their primary application. For users who log on, the relevant primary license types may be one of the following:

- Elysium Workstation¹ includes all EMR application users
- Elysium Virtual Health Record includes users who log on directly to the Virtual Health Record with no EMR or Personal Database

c) User Level Application Patient Index

All users have access to a search of the Community Patient Index. To successfully search for a patient record, users must enter one of the following:

- Patient’s medical record number
- Social Security Number
- Insurance ID
- Last Name
- First Name
- DOB

If the user can find the patient with the above search criteria, demographic and eligibility information can be displayed for that patient.

d) Elysium Workstation and Every Workgroup Database (ECD)

All Elysium Workstation users are affiliated with an Every Workgroup Database (ECD). Every Workgroup Database has a name, which is also the name of a corresponding group in the address book. If patient consent is given to a member of the ECD group, users in this group have the ability to review all the records that are either sent to this workgroup database or created by users in the database including results, referrals, prescriptions, forwarded messages, forms, etc. An ECD can be equated to an EMR

¹ For a complete description of the user types see the Elysium Operations Manual

database in a physician office. All end-users configured to use the Elysium system are affiliated with exactly one ECD.

e) Virtual Health Records (VHR)

Virtual Health Records will have unrestricted access to all Every Workgroup Databases (ECDs). Only Emergency Room and Urgent Care Physicians will have direct access to the Elysium Virtual Health Record if affirmative consent from the patient has been obtained. These users would have no need for an ECD, and would log directly into the Elysium Virtual Health Record. They would have the ability to read all documents in the ECDs and the patient index demographic and eligibility information.

In an emergency situation in which the patient is unconscious or otherwise unable to give or withhold consent, and the treating clinician determines that information that may be held by HEALTHeLINK may be material to treatment, and the patient has not previously withheld consent for the ECD organization to access his/her information, HEALTHeLINK may allow the physician to access the patient's information through "break the glass" capability. The physician must attest that all of these conditions apply, and the Elysium software must maintain a record of this access.

Physicians with Elysium Workstation licenses will need information as described for the patient index above to search for patient information in the Virtual Health Record. If a physician selects a patient from the Virtual Health Record they must attest affirmative consent from the patient has been obtained. HEALTHeLINK may then allow the physician to access the patient's information through "break the glass" capability.

Inappropriate use of HEALTHeLINK's "break the glass" capability will subject to state and federal civil and criminal penalties. All "break the glass" actions are logged, as are all the accesses to the documents the user opens.

f) Domino/IBM Database Security

Domino IBM provides a complete architecture to govern the access to databases, database records and functions within the database design. An Access Control List or ACL controls access at the highest level to the database and the records stored within it. Every database created on the platform has a default ACL that Axolotl has configured to support Elysium application security and to prevent unauthorized access. Accesses to the databases and the database records for the end users are solely through the web.

B. Elysium's Password Management

- a) All IDs and passwords are to be treated as sensitive, confidential information. Users prohibited from sharing their passwords with anyone, including administrative assistants or secretaries.
 - b) Users are ultimately responsible for the use of their ID and password and are subject to state and federal civil and criminal penalties associated to its use of it.
 - c) **The Elysium password policies are:**
 - Passwords will not be visible on the screen as they are keyed during the logon process
 - Passwords will be sent in encrypted form from the browser to the Elysium application
 - Users will be forced to change their initial password upon logon
 - Users will have the persistent opportunity to change their password
 - Users will not be allowed to compose a password with one-character or keyboard scales
 - Passwords will be a minimum of 7 characters.
 - Passwords must be alphanumeric
 - Passwords are case sensitive
 - A user Id will be systematically revoked if the password is entered incorrectly 5 consecutive times during the same logon session attempt. A help desk resource will have to reset the password in order to reactivate the user.
 - A password will expire automatically every 90 days at which time the user will have to reset it
 - A user will be notified within 15 days of impending password expiration
 - There will be 5 generations for password history. IE: a user will be unable to input any of the 5 latest passwords that they have previously used
- C. Elysium's Dormant Accounts and Automatic Logoff**
- a) Users accounts that have not logged on within 180 days will automatically be disabled.
 - b) Users will be automatically logged off of the Elysium Application after 15 minutes of inactivity.
- D. Elysium's Application Authentication**
- a) Users accessing the application will use two-factor authentication when remotely accessing Elysium application.

V. References

N/A



DRAFT

Title of Policy: Disaster Recovery/Business Continuity Plan		Policy # S09
Effective Date:	Revision Effective Date:	

Review Date:							
Revision Date:							
Policy Replacing:							

PENDING

I. Statement of Policy

II. Who Should Know This Policy

III. Definitions

IV. Procedures

V. References



Title of Policy: Access Via External Networks						Policy # S10	
Effective Date: 09/16/11				Revision Effective Date:			

Review Date:							
Revision Date:							
Policy Replacing:							

I. Statement of Policy

Health information exchanges involving networks external to HEALTHeLINK necessarily involve HEALTHeLINK entering into comprehensive, multi-party trust agreements that will be signed by all eligible entities who wish to exchange data via a particular network. It is the policy of HEALTHeLINK to enter into such agreements only where all signatories are required to abide by a common set of terms and conditions that establish each signatory’s obligations, responsibilities, and expectations. Those obligations, responsibilities, and expectations will create a framework for safe and secure health information exchanged, and must be designed to promote trust among the signatories, while protecting the privacy, confidentiality, and security of the health data that is shared.

Procedures under this Policy S10 will be amended to reflect the terms of the applicable external network as and when HEALTHeLINK becomes a signatory to such agreement.

II. Who Should Know This Policy

This Policy applies to all information exchanges involving networks external to HEALTHeLINK.

III. Definitions

See HEALTHeLINK Privacy & Security Policy Glossary.
See DURSA – Section 1. Definitions.

IV. Procedures

A. NwHIN

1. “Outbound” Information - For any DURSA Participating User requesting information from HEALTHeLINK via the NwHIN, the terms of the DURSA supersede HEALTHeLINK’s Security Policies with the exception of Policy S06 (Audit Reporting). More specifically, for access to HEALTHeLINK via the NwHIN, the DURSA application process (“On-Boarding”) including the technical specifications for securely connecting to the NwHIN, the certifications made by DURSA Participants in the DURSA and the policies and procedures adopted by the Coordinating Committee (as defined in the DURSA) supersede the HEALTHeLINK Security Policies.

2. “Inbound” Information – For any HEALTHeLINK Authorized User requesting information from an entity on the NwHIN, both the HEALTHeLINK Security Policies and DURSA will apply.

V. References

Restatement I of the Data Use & Reciprocal Support Agreement (DURSA),
Version Date: May 3, 2011



HEALTHeLINK™

**PRIVACY AND SECURITY POLICY
GLOSSARY**



HEALTHeLINK Policy Glossary

Revised 09/16/11

Acronyms

CHITA: Community Health Information Technology Alliance

DofB: Date of Birth

DURSA: Data Use and Reciprocal Sharing Agreement

EMR: Electronic Medical Record

EPID: Elysium Patient Identifier

FName: Patient First Name

HHS: Department of Health and Human Services

HIPAA: Health Insurance Portability and Accountability Act of 1996

HITECH: Health Information Technology for Economic and Clinical Health

IPID: Institution Patient Identifier

IT: Information Technology

LName: Patient Last Name

NwHIN: Nationwide Health Information Network

NYS DOH: New York State Department of Health

PBM: Pharmacy Benefit Management Systems

PHI: Protected Health Information

RHIO: Regional Health Information Organization

SSN: Social Security Number

Affirmative Consent

Means the consent of a patient obtained through the patient's execution of a HEALTHeLINK *Patient Consent to Participate in HEALTHeLINK Health Information Exchange* form.

Audit Log

Means an electronic record of the access of information via HEALTHeLINK, such as, for example, queries made by authorized users, type of information accessed, information flows between HEALTHeLINK and Participants, and date and time markers for those activities.

Authorized User

Means an individual who has been authorized by a Participant or HEALTHeLINK to access patient information via HEALTHeLINK.

Breach

Means any acquisition, access, use, or disclosure of protected health information (PHI) that compromises the security or privacy of the PHI.

Break the Glass

Means the ability of an authorized user to access a patient's protected health information (PHI) without obtaining an affirmative consent in accordance with HEALTHeLINK Patient Consent policy.

Business Associate Agreement

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

Care Management

Means (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.

Clinical/Medical Record

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

Data Supplier

Means an individual or entity that supplies protected health information (PHI) to or through HEALTHeLINK. Data Suppliers include both Participants and entities that supply but do not access PHI via HEALTHeLINK (such as clinical laboratories and pharmacies).

Data Integrity

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

De-Identified Data

Means 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 if it satisfies the requirements of 45 C.F.R. § 164.514(b).

Demographic Information

Means 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.

DURSA Participant

Means any organization that (i) meets the requirements for participation as contained in the DURSA Operating Policies and Procedures; (ii) is provided with digital credentials; and (iii) is a signatory to the DURSA or a Joinder Agreement. HEALTHeLINK is a DURSA Participant.

DURSA Participant User

Means 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 (entities or individuals that have executed a HEALTHeLINK Participation Agreement ("PA")) and their Authorized Users, as defined in the PA, are DURSA Participant Users.

Employees

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

Failed Access Attempt

Means an instance in which an authorized user or other individual attempting to access HEALTHeLINK is denied access due to use of an inaccurate log-in, password, or other security token.

Health Care Operations

Means any of the following activities to the extent that the activities are related to covered functions of the Participant:

- 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; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination (including disease management), contacting of health care providers and members with information about treatment alternatives; and related functions that do not include treatment;
- Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider 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;
- Underwriting, premium rating and other activities relating 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);
- Conducting or arranging for medical review, legal services and auditing functions, including fraud and abuse detection and compliance programs;
 - Business planning and development, such as conducting cost management and planning-related analyses related to managing and operating, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
 - Business management and general administrative activities, including but not limited to:
 - Management activities relating to implementation of and compliance with the HIPAA Privacy Rule;
 - Customer service, including the provision of data analyses for subscribers, members, plan sponsors, or other customers, provided that protected health information is not disclosed to such subscriber member, plan sponsor, or other customer
 - Resolution of internal grievances;
 - The sale, transfer, merger or consolidation of all or parts with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and
 - Creating de-identified health information, or a limited data set, and fundraising for benefit.

Incidental Disclosure

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

Individually Identifiable Health Information (IIHI)

Means 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 condition or payment for healthcare and that identifies or can be used to identify the individual.

Insurance Coverage Review

Means 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

Level 1 Uses

Mean Treatment, Quality Improvement, Care Management, and Insurance Coverage Reviews.

Level 2 Uses

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

Marketing

Means (1) any communication about a product or service that encourages recipients to purchase or use the product or service, unless the communication is made (i) to describe a health-related product or service (or payment for such product or service) that is provided by, or included in a plan of benefits of, the entity making the communication, including communications about: the entities participating in a health care provider network or health plan network; replacement of, or enhancements to, a health plan; and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits; (ii) for the treatment of the individual; or (iii) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or settings of care to the individual; or (2) an arrangement whereby a Participant discloses Protected Health Information to another entity, in exchange for direct or indirect remuneration, for the other entity to communicate about its own products or services encouraging the use or purchase of those products or services.

Master Patient Index (MPI)

Means index in which patient demographic data is stored

Minor

Means a person under eighteen (18) years of age.

Minor Consent Information

Means protected health information (PHI) relating to medical treatment of a minor for which the minor provided his or her own consent without a parent's or guardian's permission, as permitted by New York law for certain types of health services (e.g., family planning, HIV testing, mental health or substance abuse treatment)

New York eHealth Collaborative (“NYeC”)

Means 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, RHIOs, CHITAs 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 NYS DOH to administer the SCP and through it develop Statewide Policy Guidance.

Non-repudiation

Means 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.

One-to-One Exchange

Means a disclosure of protected health information (PHI) by one of the patient's providers to one or more other providers treating the patient 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. A one-to-one exchange is an electronic transfer of information that is understood and predictable to a patient, because it mirrors a paper-based exchange, such as a referral to a specialist, a discharge summary sent to where the patient is transferred or lab results sent to the Practitioner who ordered them.

Participant

Means a Provider Organization, Payer Organization, or Practitioner that has directly or indirectly entered into a Participation Agreement with HEALTHeLINK and accesses protected health information via HEALTHeLINK.

Participation Agreement

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

Payment

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

Payer Organization

Means 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.

Personal Representative

Means 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.

Practitioner

Means a health care professional licensed under Title 8 of the New York Education Law or a resident or student acting under the supervision of such a professional.

Protected Health Information (PHI)

Means individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Protected health information excludes individually identifiable health information in employment records that a covered entity maintains in its capacity as an employer and education and certain other records subject to, or defined in, the Family Educational Rights and Privacy Act, 20 U.S.C. §1232g.

Provider Organization

Means an entity such as a hospital, nursing home, home health agency or professional corporation legally authorized to provide health care services in New York State

Quality Improvement

Means conducting quality measurement, assessment and improvement, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health and reducing health care costs, evaluating Practitioner and provider performance, clinical decision support tools, evidence-based clinical protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives and related functions. Care management by payers may include (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; provided, however, that no such activity may include utilization review or other tasks designed to determine whether a payer should cover or make payment for a health care service.

Record Locator Service or Other Comparable Directory

Means a system, queryable only by authorized users, that provides an electronic means for identifying and locating a patient's medical records across data suppliers.

Research

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

Sensitive Health Information

Means 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.

Social Security Number

Means 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.

Substance abuse treatment program

Means an individual or entity that provides alcohol or drug abuse diagnosis, treatment or referral. For the purposes of these policies, the term “program” includes both individual substance abuse providers and substance abuse provider organizations.

Treatment

Means 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

Means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technologies or methodologies approved by the Secretary of Health and Human Services. The two HHS-approved technologies and methodologies are encryption and destruction.

Workforce

Means HEALTHeLINK Participants' employees, volunteers, trainees and other persons whose work is under the Participants' direct control, regardless of whether they are paid.