

Attachment H



Policies and Procedures
TOPIC: Breach Notification and Mitigation Policy
Policy #: TBD
Effective Date: TBD

I. BACKGROUND AND PURPOSE

The Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and/or other applicable Illinois law, including without limitation the Illinois Personal Information Protection Act (“PIPA”), preclude or require notice of the acquisition, access, use, or disclosure of a patient’s<sup>1</sup> Protected Health Information (“PHI”) in a manner which compromises the security or privacy of such information (“Breach” as further defined below and in Exhibit 1). In the performance of the bi-directional exchange of PHI as a health information exchange, the ILHIE Authority receives and transmits PHI from one Participant to another Participant. Accordingly, Breach notification and mitigation obligations may apply to both Participants and the ILHIE Authority, in its Business Associate capacity to the Participants, should there be a Breach of PHI utilizing ILHIE technology or infrastructure.

This Policy establishes a Breach notification and mitigation protocol for Participants of the ILHIE and the ILHIE Authority. It applies only to those privacy and security incidents which would qualify as a Breach under HIPAA, HITECH and/or other applicable law and which utilize ILHIE technology or infrastructure or which allow unauthorized access to ILHIE technology, ILHIE infrastructure or PHI through the ILHIE. The obligations contained herein comply with and are in addition to those obligations contained in HIPAA, HITECH and/or other applicable law. This Policy shall be incorporated by reference into all existing and future Data Sharing Agreements (“DSAs”) entered into by and between Participants and the ILHIE Authority.

All capitalized terms not otherwise defined within this Policy or the attached definitions (Exhibit 1) shall have the same meaning as set forth in the provisions of HIPAA and HITECH then in effect and/or the DSA. As used herein, HIPAA and HITECH are each deemed to include all of the regulations adopted thereunder for which compliance is required at the time in question.

---

<sup>1</sup> For purposes of this Policy, “patient” shall mean the individual who is the subject of the PHI and may include subscribers of payor programs or persons insured by health plans.

## Attachment H

II. POLICY
------------

### A. General

A Participant shall, promptly upon discovery of any Breach (whether of the ILHIE, or by the Participant, another Participant or the ILHIE Authority) report the Breach to the ILHIE Authority and the Affected Participants in accordance with this Policy.

### B. Participant Breach

A Breaching Participant shall, in accordance with its own policies, promptly investigate any and all Breaches. The Breaching Participant shall inform the ILHIE Authority and, in those cases where the Affected Participants can be identified, inform the Affected Participants of a Breach in accordance with the procedures set forth herein.

The Breaching Participant shall be responsible for notifying patients, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with those provided by any Affected Participant. An Affected Participant may also notify patients with whom the Affected Participant has or has had a relationship and whose PHI was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to advise and to coordinate any notice with the Breaching Participant and the ILHIE Authority.

The Breaching Participant shall be responsible for mitigating the Breach. The ILHIE Authority shall have the right to participate in the investigation and to know the results and remedial action taken, if any, except that the ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted to require any Participant to disclose any PHI to the ILHIE Authority if such a disclosure would not be permitted under HIPAA, HITECH or other applicable law.

### C. ILHIE Breach

The ILHIE Authority shall, in accordance with the procedures set forth herein, promptly upon discovery of any ILHIE Breach, report such ILHIE Breach to the Breaching Participant, as well as to Affected Participants. The ILHIE Authority shall promptly investigate any ILHIE Breach, mitigate the ILHIE Breach, and cooperate with the Breaching Participant and all Affected Participants with respect to any mitigation, reporting or other obligations that the Breaching Participant and/or Affected Participants may have. Each Breaching or Affected Participant, however, shall be responsible for notifying its patients to the extent required under HIPAA

## Attachment H

and/or HITECH and/or other applicable law, and the ILHIE Authority shall not give such notice unless and to the extent that a Participant has delegated to the ILHIE Authority the obligation to provide notice on behalf of that Participant. Notwithstanding the foregoing, the ILHIE Authority shall give any notice that it is required to provide under applicable law.

### D. Role of ILHIE Authority

Upon request by a Breaching Participant, the ILHIE Authority shall assist the Breaching Participant in identifying Affected Participants. Where multiple Participants are Breaching Participants or Affected Participants, upon the request of one or more Participants, the ILHIE Authority may coordinate communication and activities between those Participants, but nothing set forth in this Policy and Procedure shall require any Participant to delay its own investigation, reporting or other activities that it deems necessary or appropriate to comply with law or to assure the ongoing privacy and security of PHI. The ILHIE Authority shall not be responsible for making determinations as to which Participant is responsible for the Breach.

For all Breaches, an investigation of a Breach and all actions taken with respect to the Breach shall be documented and provided to the ILHIE Authority by the Breaching Participant. The ILHIE Authority may use this information for education, for policy and other safeguard development.

The ILHIE Authority shall prepare an annual report for Participants identifying Breaches which occurred within the previous year which utilized ILHIE technology or infrastructure or which allowed unauthorized access to ILHIE technology, ILHIE infrastructure or PHI through the ILHIE. Nothing, however, precludes the ILHIE Authority from notifying Participants more frequently if the ILHIE Authority determines that doing so will be beneficial to ILHIE operations. The ILHIE Authority shall not disseminate or publish PHI. The ILHIE Authority may disseminate or publish de-identified data to provide examples of Breaches for education and for policy and other safeguard development.

The ILHIE Authority may deactivate an Authorized User's access for cause in accordance with the Data Sharing Agreement.

III. PROCEDURES: GENERAL
--------------------------

- A. Participants shall appoint an individual to be contacted in the event of a Breach.
- B. A Participant shall, promptly upon discovery of any Breach (whether of the ILHIE or by the Participant, another Participant or the ILHIE Authority) report by email the Breach to the ILHIE Authority and the Affected Participants. Participants are not responsible for monitoring the ILHIE or other Participants for Breaches. Where a Participant reports an incident in good faith, the Participant will not be liable if the incident reported is subsequently determined not to be a Breach.

## Attachment H

- C. Participants and the ILHIE Authority shall cooperate in any investigation by the ILHIE Authority or any good faith investigation by another Participant. In addition, Participant shall cooperate with the legally required notification and mitigation activities of other Participants or the ILHIE Authority.

### IV. PROCEDURES PARTICIPANT BREACH

- A. Investigation: A Breaching Participant shall, in accordance with its own policies, promptly investigate suspected or actual reported Breaches.
- B. Notifying ILHIE Authority and Affected ILHIE Participants (“Informational Notification”): A Breaching Participant shall inform the ILHIE Authority’s Privacy and Compliance Officer or other individual designated by the ILHIE Authority (ILHIE PCO) and, in those cases where the Affected Participants can be identified, the Breaching Participant shall notify the Affected Participants of a Breach. The ILHIE Authority shall make Participant contact information available to all Participants to facilitate informational notification. No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, including pings and other broadcast attacks on a Participant’s firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.
1. Informational Notification shall be made promptly, but in no event more than five (5) business days from discovery of the Breach. Notification shall be made irrespective of whether or not the Breaching Participant’s investigation is completed.
  2. Informational Notification shall be done (i) via email or (ii) via phone conference with the ILHIE PCO and Affected Participants, provided that notice by email is subsequently provided to all Affected Participants and the ILHIE PCO.
  3. Informational Notification shall include sufficient information so that the ILHIE PCO, if requested by a Participant, can assist the Participant in its investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 2, to the extent that the Breaching Participant has knowledge of such items.
  4. Upon determination that a previously reported Breach is not a Breach, the Participant that reported the Breach shall send an updated status to the ILHIE Authority and Affected Participants.
- C. Notification Required by Law (“Legal Notification”): Except as provided in Section V, the Breaching Participant shall, at its expense, be responsible for notifying patients, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that the Breaching Participant shall use reasonable efforts to

## Attachment H

coordinate the required notices with the Affected Participant(s). An Affected Participant may also notify patients with whom the Affected Participant has or has had a relationship and whose PHI was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to advise and coordinate any notice with the Breaching Participant and the ILHIE Authority.

### D. Mitigation and Remediation:

1. The Breaching Participant shall take reasonable steps to pursue, address and mitigate any Breach which has resulted from its acts or omissions.
2. To the extent provided in the DSA or as required by applicable law, the Breaching Participant shall assume mitigation costs caused by the Breach of the Breaching Participant. Mitigation costs shall be limited to direct damages and will exclude all consequential, indirect or punitive damages.

E. Reporting Requirements: The investigation of a Breach and all actions taken with respect to the Breach shall be documented, and the documentation shall be provided by the Breaching Participant to the ILHIE Authority within thirty (30) days of the provision of Legal Notification to patients. The documentation should include, but need not be limited to, the items set forth on Exhibit 3, to the extent that the Breaching Participant has knowledge of such items. The ILHIE Authority need not be notified of specific workforce disciplinary actions and may not participate in any action or investigation by a Participant that would result in the loss of any applicable attorney-client privilege or work product protections. This Policy and Procedure shall not be interpreted to require any Participant to disclose any PHI to the ILHIE Authority if such a disclosure would not be permitted under HIPAA, HITECH and/or other applicable law.

### F. Role of ILHIE Authority:

1. If multiple Participants cannot agree on which is the Breaching Participant, on the request of one or more Participants, then the ILHIE Authority may facilitate the resolution of the matter.
2. The ILHIE Authority shall facilitate conference calls and other mechanisms to help Participants coordinate their responses and communications regarding Breaches to ensure that all such Participants are aware of mitigation efforts and costs and to ensure that the Breach is generally described in the same way in press releases and government filings.
3. The ILHIE Authority shall develop template documents to facilitate communication of Breaches to patients, the Department of Health and Human Services, the media, as well as other individuals or entities requiring notification in conformance with HIPAA, HITECH, and/or other applicable law. Use of such templates is not required.

## Attachment H

4. The ILHIE Authority may deactivate, suspend or revoke an Authorized User in accordance with the applicable Data Sharing Agreement.
5. All PHI that the ILHIE Authority receives or to which it has access in connection with any Breach hereunder shall be subject to the requirements of its Business Associate Agreements with Participants and to HIPAA, HITECH and/or other applicable law.
6. The ILHIE Authority shall take all action necessary to prevent all PHI that it receives in connection with any Breach hereunder from being subject to disclosure or release under the Illinois Freedom of Information Act (5 ILCS 140/1 *et seq.*) or similar federal or Illinois law or regulation requiring disclosure of government records or information.

V. PROCEDURE - ILHIE BREACHES
-------------------------------

- A. Investigation: The ILHIE Authority shall, in accordance with its own policies, promptly investigate actual or suspected ILHIE Breaches.
- B. Informational Notification: The ILHIE Authority shall inform the Breaching Participant, as well as Affected Participants, of the ILHIE Breach. No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, including pings and other broadcast attacks on ILHIE's firewalls, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI.
  1. Informational Notification shall be made as soon as possible, but in no event more than five (5) business days from discovery of the ILHIE Breach. Notification shall be made irrespective of whether or not the ILHIE Authority's investigation is completed.
  2. Informational Notification shall be done (i) via email or (ii) via phone conference with the ILHIE PCO, Breaching Participant and Affected Participants, provided that an email notice is subsequently provided to all parties.
  3. Informational Notification shall include sufficient information so that each Participant that receives notification can conduct its own investigation and mitigation efforts. Informational Notification should include, but need not be limited to, the items set forth on Exhibit 2, to the extent that the ILHIE Authority has knowledge of such items.
  4. Upon determination that a previously reported ILHIE Breach is not Breach, the ILHIE Authority shall send an updated status to any Breaching and Affected Participants.
- C. Notification Required by Law ("Legal Notification"): A Breaching Participant shall be responsible for notifying patients, the Department of Health and Human Services,

## Attachment H

and, if necessary, the media, as well as other entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that the Breaching Participant shall use reasonable efforts to coordinate the required notices with any Affected Participant. An Affected Participant may also notify patients with whom the Affected Participant has or has had a relationship and whose PHI was compromised by the Breach, the Department of Health and Human Services, and, if necessary, the media, as well as other individuals or entities if required under HIPAA, HITECH, and/or other applicable law; provided, however, that Affected Participants providing such notification shall use reasonable efforts to coordinate any notice with and advise any Breaching Participant and the ILHIE Authority. When the Breach is an ILHIE Breach the Breaching and Affected Participants may delegate to the ILHIE Authority notification of patients on the Breaching or Affected Participant's behalf. In any event, if the Breach is an ILHIE Breach, the ILHIE Authority shall pay for the costs of notification by either the Breaching Participant, the Affected Participant, or by the ILHIE Authority on behalf of the Breaching Participant or Affected Participant.

D. Mitigation and Remediation:

1. ILHIE Authority shall take reasonable steps to pursue, address and mitigate any ILHIE Breach.
2. To the extent provided in the DSA or as required by applicable law, the ILHIE Authority shall pay mitigation costs associated with ILHIE Breaches. Mitigation costs shall be limited to direct damages and will exclude all consequential, indirect or punitive damages.

E. Reporting: An investigation of an ILHIE Breach and all actions taken with respect to the ILHIE Breach shall be documented, and the ILHIE Authority shall provide such documentation to any Breaching Participant and Affected Participants within thirty (30) days of the provision of Legal Notification to patients. Documentation should include, but need not be limited to, the items set forth in Exhibit 3, to the extent that the ILHIE Authority has knowledge of such items.

F. Coordination between Participants: ILHIE Authority shall perform the role set forth in Section IV.F of this Policy with respect to ILHIE Breaches.

## Attachment H

### EXHIBIT 1: DEFINITIONS

**“Affected Participant”** means any Participant (other than a Breaching Participant) with respect to which a Breach has occurred or for which there is a reasonable possibility that a Breach has occurred with respect to its Systems or PHI, but which does not involve an act or omission of the Affected Participant or any of its Authorized Users, Workforce, Business Associates or Subcontractors that caused the Breach.

**“Authorized User”** means a Participant’s Workforce, agents, representatives, independent contractors, Subcontractors or other persons or entities authorized by such Participant, under the procedures set forth in sections 3 (b) and 5(a) of the Data Sharing Agreement, to access, use or disclose Protected Health Information from another Participant’s System. Consistent with the ILHIE intellectual property license (section 8a) of the Data Sharing Agreement, an Authorized User must be a person or entity that uses Services for accessing or transmitting Protected Health Information that was created (a) by a healthcare provider in Illinois, or (b) by a health care provider outside of Illinois and that is accessed by or provided to users located within Illinois.

**“Breach”** means any acquisition, access, use or disclosure of Protected Health Information utilizing ILHIE technology or infrastructure or which allows unauthorized access to ILHIE technology, ILHIE infrastructure or PHI through the ILHIE and compromising the security or privacy of such information except as set forth in 45 CFR 164.402. An access, use or disclosure of PHI in a manner not permitted by the Data Sharing Agreement, HIPAA, PIPA or other applicable law is presumed to be a Breach, unless the Breaching Participant or ILHIE demonstrates that there is low probability that PHI has been compromised based on a risk assessment using the factors set forth in 45 CFR 164.402 and the Breaching Participant or ILHIE demonstrates that the access, use, or disclosure does not constitute a Breach under HIPAA, PIPA or other applicable law.

**“Breaching Participant”** means a Participant whose act or omission, or the act or omission of that Participant’s Authorized Users, Workforce, Business Associates or Subcontractors caused a Breach.

**“Data Sharing Agreement”** or **“DSA”** means that agreement entered into by and between the ILHIE Authority and a Participant.

**“Deactivation Notice”** means the notification given by the ILHIE Authority to a Participant informing the Participant that an Authorized User of the Participant will no longer be able to access PHI through ILHIE.

**“Department of Health and Human Services”** or **“HHS”** means the United States Department of Health and Human Services.

**“HIE”** means a Health Information Exchange as defined in the Illinois Health Information Exchange and Technology Act and any and all regulations promulgated thereunder, as amended from time-to-time.

## Attachment H

**“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, and any and all regulations promulgated thereunder, as amended from time-to-time.

**“HITECH”** means the Health Information Technology for Economic and Clinical Health Act, and any and all regulations promulgated thereunder, as amended from time-to-time.

**“ILHIE”** means the Illinois Health Information Exchange as established by the Illinois Health Information Exchange and Technology Act, and any and all regulations promulgated thereunder, as amended from time-to-time.

**“ILHIE Authority”** means that governing body established by the Illinois Health Information Exchange and Technology Act, and any and all regulations promulgated thereunder, as amended from time-to-time. ILHIE Authority shall include its Workforce , Subcontractors and Business Associates. Where ILHIE Authority is used in the Policy and Procedure, it may mean the ILHIE Authority or OHIT or both as applicable.

**“ILHIE Breach”** shall mean a Breach of the ILHIE during the transmission of PHI through the ILHIE or a Breach due to the act or omission of the ILHIE Authority. An ILHIE Breach does not include a Breach of the ILHIE that did not occur during transmission through the ILHIE or due to the act or omission by the ILHIE Authority.

**“ILHIE PCO”** means the ILHIE Privacy and Compliance Officer or other individual designated by the ILHIE Authority.

**“Informational Notification”** means the notification that a Breaching Participant gives to ILHIE Authority and Affected Participants. Informational Notification should be contrasted to “Legal Notification” which is that notification required by HIPAA, HITECH and/or other applicable law.

**“Legal Notification”** means notification required by law to be made in the event of a Breach.

**“OHIT”** means the Office of Health Information Technology.

**“Participant”** means an individual who or entity, including without limitation an HIE, that has executed a Data Sharing Agreement with ILHIE Authority.

**“PIPA”** means the Illinois Personal Information Protection Act, and any and all regulations promulgated thereunder, as amended from time-to-time.

**“Protected Health Information”** or **“PHI”** has the same meaning as defined under HITECH, HIPAA, PIPA, and/or other applicable law.

**“System”** shall mean software, portal, platform, or other electronic medium controlled or utilized by a Participant through which or by which the Participant exchanges information under the DSA. For purposes of this definition, it shall not matter whether the Participant controls or utilizes the software, portal, platform or other medium through ownership, lease, license, or otherwise.

## Attachment H

EXHIBIT 2: INFORMATIONAL NOTIFICATION REQUIREMENTS
--

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected ILHIE Participants upon the discovery of a Breach or suspected Breach.

1. Date of Breach or suspected Breach.
2. Date of discovery.
3. Description of Breach or suspected Breach. Please be specific and include the number of individuals affected.
4. Description of Protected Health Information (“PHI”) used or disclosed. Please be specific as to the type of information.
5. Whether or not the following PHI was included in the unauthorized use or disclosure as well as explanatory details:
  - HIV/AIDS information including whether an HIV test was administered
  - genetic testing or counseling
  - alcohol or substance abuse
  - mental health
  - developmental disability
  - sexually transmitted infections
6. Whether or not the following PHI was included (in whole or in part) in the unauthorized use or disclosure as well as explanatory details:
  - Social security number
  - Driver’s license or State ID number
  - Account number, or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account
7. Recipient of unauthorized use or disclosure (include full identification, address, email, and phone number).
8. Description of any actions taken thus far with respect to investigation and mitigation efforts.

## Attachment H

EXHIBIT 3: BREACH REPORT REQUIREMENTS
---------------------------------------

To the extent known, the following information shall be submitted to the ILHIE Authority as well as other Affected ILHIE Participants within thirty (30) days of the provision of Legal Notification to patients.

1. Date of Breach.
2. Date of discovery.
3. Description of Breach. Please be specific and include the number of individuals affected
4. Description of Protected Health Information (“PHI”) used or disclosed. Please be specific as to the type of information.
5. Whether or not the following PHI was included in the unauthorized use or disclosure as well as explanatory details:
  - HIV
  - genetic testing or counseling
  - substance abuse
  - mental health
  - developmental disability
  - sexually transmitted infections
6. Whether or not the following PHI was included (in full or in part) in the unauthorized use or disclosure as well as explanatory details:
  - Social security number
  - Driver’s license or State ID number
  - Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account
7. Recipient of unauthorized use or disclosure (include full identification, address, email, and phone number).
8. Description of investigation.
9. Description of all applicable mitigation actions, including, but not limited to:
  - Retrieval of PHI
  - Whether or not disciplinary action was taken. NOTE: Specific details are not required
  - Technical modifications
  - Administrative modifications (e.g., adoption or modification of policies, workflow processes, etc.)
  - Physician modifications
  - Retraining

## Attachment H

- Credit monitoring provided to individuals
- Other

10. Date notification provided to individuals.

11. Date notification provided to the Department of Health and Human Services.

12. Date notification provided in media (if required).

## Attachment H