



Privacy and Security Policy and Procedures
TOPIC: Breach Notification Protocol
Policy #: 1
Effective Date: December 1, 2013

## I. BACKGROUND AND PURPOSE

The purpose of this Protocol is to establish a standardized breach notification and mitigation policy and procedure for all Illinois Health Information Exchange (ILHIE) participants (Participants) and the ILHIE Authority to follow. The obligations contained herein comply with and are in addition to those obligations contained in Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health (HITECH) Act and applicable Illinois law. This Privacy and Security Policy and Procedure shall be incorporated by reference into all existing and future Data Sharing Agreements (Agreement) with the Office of Health Information Technology (OHIT) and/or the ILHIE Authority pursuant to Section 4(a) of the Agreement.<sup>1</sup> All capitalized terms not otherwise defined shall have the same meaning as set forth in the HIPAA regulations.

## II. POLICY

Federal and state privacy and security laws protect a Patient’s protected health information (PHI) from an acquisition, access, use or disclosure of PHI in a manner which compromises the security or privacy of such information by unauthorized persons and entities (Breach). 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(s) (Other Participant(s)). The ILHIE is not involved in patient treatment, but functions as a Business Associate with respect to the electronic receipt and transmission of PHI and other permitted uses of PHI under the HIPAA regulations. This Business Associate status creates notification and mitigation obligations should the ILHIE Authority discover a Breach of PHI transmitted through the ILHIE.

Access, use or disclosure of PHI in a manner not permitted by the HIPAA regulations or with respect to certain categories of “specially protected” health information, in a manner not specifically authorized by the patient is presumed to be a Breach, unless the party which incurred the breach demonstrates there is a low probability that PHI has been compromised based on a risk assessment in accordance 45 CFR §164.402 of the HIPAA regulations. This risk analysis must be done for any known Security Incident by ILHIE Authority and all Participants. If the

---

<sup>1</sup> Currently the Data Sharing Agreement is signed by OHIT, but it will transition to the ILHIE Authority by December 31, 2013 or soon thereafter.

Security Incident is determined to be a Breach, it triggers notification and mitigation requirements for the ILHIE Authority and/or Participants.

### III. PROCEDURES

#### A. Participant Obligations

1. **Participant Contact:** Participant shall identify an individual to be the person to contact for notice and coordination in the event of a Breach or Security Incident.
2. **Breach Notification to the ILHIE Authority**
  - a) A Participant must regularly monitor and audit access to PHI by its Authorized Users. In the event a Participant discovers a Security Incident as defined in the HIPAA Security Rule, it must determine whether the Security Incident was a Breach of patient PHI that was transmitted through the ILHIE. In addition, Participant shall notify the ILHIE Authority of a Breach or Security Incident within ten (10) days, whether or not its investigation is complete by that date.
  - b) Notification shall be done via email or mail to the ILHIE Authority's Privacy and Compliance Officer or other individual designated by the ILHIE Authority (ILHIEA PCO) or via phone conference with the ILHIEA PCO provided that a written notice is subsequently provided to the ILHIE Authority.
  - c) Notification shall include sufficient information so that the ILHIEA PCO can conduct its own investigation and coordinate mitigation efforts. The information provided shall include, but not be limited to, the patients involved, the risk analysis determination and knowledge of the involvement of PHI aggregated from Other Participants' systems.
  - d) No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, meaning pings and other broadcast attacks on a party'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.

3. **Notification to Other Participants, Patients, the Secretary and the Media**

a) **Other Participants:** A Participant shall notify Affected Other Participants within 10 days of the Breach contemporaneously with its notification to the ILHIE Authority. Affected Other Participants (Affected Other Participants) are those Other Participants for which there is a reasonable possibility that the Other Participants' systems or data on those systems may have been negatively impacted by the Breach

b) **Patients:** The ILHIE Authority shall coordinate with Participant and Other Affected Participants the notification of the impacted patient (Patient) within the sixty (60) day period required by federal law. If the Participant and Other Affected Participants cannot agree on which of them should notify the patient, then the ILHIE Authority will notify the Patient.

c) **The Secretary:** Participant shall notify the Secretary within the sixty (60) day period required by federal law, unless the Participant agrees with the ILHIE Authority's determination that the ILHIE Authority or an Affected Other Participant should notify the Secretary.

d) **Media:** A Participant shall notify the media within the sixty (60) day period required by federal law, unless the Participant agrees with the ILHIE Authority's determination that the ILHIE Authority or an affected Other Participant should notify the media.

e) No notification is required regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, meaning pings and other broadcast attacks on a party'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.

4. **Costs of Notification:** Participant shall assume the costs of notification so long as the Breach was determined to be caused by acts or omissions of the Participant and its Authorized Users

5. **Coordination and Cooperation:** Participant agrees to cooperate in any investigation by another Participant, Affected Other Participant or ILHIE Authority. In addition, Participant agrees to coordinate notification and mitigation with Affected Other Participant(s), Other Participant(s) or ILHIE Authority.

6. **Mitigation**

a) Participant shall take reasonable steps to pursue, address and mitigate any Breach or other privacy and security issues detected at any time regardless of cause or fault.

b) Participant agrees to assume all mitigation costs associated with Breaches caused by acts or omissions of the Participant and/or its Authorized Users, subcontractors and Business Associates, but not including the ILHIE Authority.

c) Furthermore, the Participant agrees to indemnify the ILHIE Authority for mitigation costs if the Breach was caused by the acts or omissions of Participant, its Authorized Users, subcontractors and/or Business Associates. However, the ILHIE Authority will not indemnify Participant for any mitigation costs, including but not limited to, those associated with Breaches caused by acts or omissions of the ILHIE Authority, its subcontractors and Business Associates.

**B. ILHIE Obligations**

**1. Breach Notification/Coordination**

a) In the event the ILHIE Authority discovers a Security Incident as defined in the HIPAA Security Rule and determines it to be a Breach of a Patient's PHI transmitted through the ILHIE, the ILHIE Authority shall notify the Participant and all Affected Other Participants within ten (10) days.

b) The ILHIE Authority shall coordinate with Participant and Other Affected Participants notification of the Patient within the sixty (60) day period required by federal law. If the Participant and Other Affected Participants cannot agree on which of them should notify the Patient, then the ILHIE Authority will notify the Patient.

c) No notification is required hereunder regarding the ongoing existence and occurrence or attempts of unsuccessful security incidents, meaning pings and other broadcast attacks on a party'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.

d) ILHIE Authority may facilitate conference calls and other mechanisms to help Participant and any Other Participants coordinate their responses and communications regarding Breaches so that all such Participants are aware of mitigation efforts and costs, and the Breach is generally described in the same way in press releases and government filings.

e) The ILHIEA PCO shall direct and coordinate the mitigation efforts in a manner so as to minimize the burden on parties not deemed to have caused the Breach. Furthermore, the ILHIEA PCO shall determine, with the consent of Participant and Affected Other Participants, which party will notify the Patient, the Secretary and media if applicable.

**2. Mitigation**

a) The ILHIE Authority shall take reasonable steps to pursue, address and mitigate any Breach or other privacy and security issues detected at any time regardless of cause or fault.

b) The ILHIE Authority agrees to assume all mitigation costs associated with Breaches caused by acts or omissions by the ILHIE Authority and/or its subcontractors and Business Associates. However, the ILHIE Authority will not indemnify the Participant for any mitigation costs including but not limited to, those associated with breaches caused by acts or omissions of the ILHIE Authority, its subcontractors and Business Associates.

DRAFT