Policy & Procedure	ID No.	4788
Subject: HIE Security Incidents & Breaches of Unsecured Data	*Category:*	Management of Information
Facility Scope: AtlantiCare Health System	*Department:*	Health Information Exchange (HIE)

POLICY:

To set forth minimum standards that Authorized Users shall follow in the event of a Security Incident or Breach of Unsecured Data.

PROCEDURE:

1.1 *Compliance with Law*

Authorized Users shall comply with the following:

- § 13402 of the Health Information Technology for Economic and Clinical Health Act ("HITECH) Act, and specifically (the "Breach Statute");
- HHS Final Rule for Breach Notification for Unsecured PHI (45 CFR Parts 160 and 164) (the "Breach Notification Rule");
- The New Jersey Identity Theft Prevention Act ("NJITPA"), N.J.S.A. 56:8-161 et seq. (the "NJITPA Breach Statute"); and
- NJITPA rules governing Written Security Programs, N.J.A.C. 13:45F-1.1 et seq., Subchapter 3 (the "NJITPA Breach Rule").

Capitalized terms under this AtlantiCare HIE Policy shall have the same meanings given to such terms under the Breach Notification Laws, unless specified to the contrary.

1.2 *Detecting Potential Breaches*

1.2.1 Each Authorized User shall strive to detect any circumstances that could lead to or result in a potential or actual Breach.

1.2.2 Any Authorized User who has reason to believe that a Breach involving PHI or PI (under state law) has or may potentially occur with regard to another Authorized User's Data being accessed or disclosed through the AtlantiCare HIE must report such information to the AtlantiCare HIE Privacy Officer and/or AtlantiCare HIE Security Officer.

1.2.3 As part of striving to detect Security Incidents and Breaches, Authorized User's systems shall be audited for evidence of Breaches in accordance with the AtlantiCare HIE Policy governing Auditing.

1.3 *Investigating Incidents and Breaches*

1.3.1 Authorized Users shall investigate and evaluate any and all reports of internal Breaches (or potential security breaches).

1.3.2 The AtlantiCare HIE Privacy Officer and AtlantiCare HIE Security Officer, as appropriate, shall investigate reported and detected breaches that may affect another Authorized User of the AtlantiCare HIE.

1.3.3 Authorized Users and the AtlantiCare HIE will adhere to the Breach Notification laws when determining whether or not a Breach has occurred under HITECH or State law. Steps for investigating a reported incident and potential Breach should include at least an evaluation of the following:

- Was the information De-identified, or a Limited Data Set *minus* dates of birth and zip codes? (If yes, not covered by the Breach Notification Laws).
- Is the information PHI, including Limited Data Sets?
- Was the PHI or PI "unsecured"?
- Was there an "unauthorized" access, use or disclosure of PHI in violation of the Privacy Rule?
- Does the access, use or disclosures fall within an Exception[1]?
- Does the Privacy Rule violation ***compromise*** the security or privacy of the PHI – e.g., is there a "***low probability"*** *that the PHI has been compromised. Consider the following factors:*

1) Nature & Extent of PHI

For this factor, HHS suggests that CEs and BAs consider the *type* of PHI involved, such as if the PHI was of a more "sensitive" nature. An example given is if credit card numbers, social security numbers,

---

[1]
- **Unintentional Exception:** unintentional access, acquisition, or use of PHI is not a "breach" if it was:
  - By a *workforce member* under the *direct control* of the CE or BA;
  - In "*good faith*" unintentional;
  - Within *course/scope* of the employment/ professional relationship (with CE/BA); *and*
  - Was *not further acquired*, accessed, used or disclosed in a manner not permitted under the Privacy Rule.

  Example: a billing employee receives and opens an e-mail containing PHI about a patient which a nurse mistakenly sent to the billing employee. Billing employee notices the intended recipient, alerts the nurse, and deletes it. The billing employee unintentionally accessed the PHI to which he was not authorized to have access, but since the billing employee's use of the information was in good faith and within the scope of authority, it does not constitute a breach – as long as the employee did not further use/disclose the information accessed in a manner not permitted by the rules.

- **Inadvertent Exception:** inadvertent disclosure of PHI is not a "breach" if it was:
  - *From* a person who is otherwise authorized to access the PHI at the facility of the CE or BA
  - *To* another similarly situated person at same facility and
  - The information received is not further acquired, accessed, used, or disclosed without authorization by any person.

- **Not Retained Exception:** if an unauthorized person to whom such PHI is disclosed would not ***reasonably*** have been able to retain such information -- no breach.

or other information that increases the risk of identity theft or financial fraud are involved, then this would ***cut against*** finding that there is "low probability" that the PHI was compromised. With respect to clinical information, HHS points out that CEs and BAs might consider things like the *nature of the services*, as well as the *amount* of information and *details* involved. It is worth noting that in a footnote, HHS specifically calls out that "sensitive" information is not just things like STDS, mental health or substance abuse.

2) Unauthorized Person

To evaluate the second factor, HHS suggests that CEs and BAs consider who the unauthorized recipient is or might be. For example, if the recipient person is someone at another CE or BA, then this may support a finding that there is a lower probability that the PHI has been compromised since CEs and BAs are obligated to protect the privacy and security of PHI in a similar manner as the CE or BA from where the breached PHI originated. Another example given is if PHI containing dates of health care service and diagnoses of certain employees was impermissibly disclosed to their employer, the employer may be able to determine that the information pertains to specific employees based on other information available to the employer, such as dates of absence from work. In this case, there may *be more than a low probability* that the PHI has been compromised.

3) Acquired or Viewed

The third factor requires CE and BAs to investigate and determine if the PHI was *actually* acquired or viewed or, alternatively, if only the *opportunity existed* for the information to be acquired or viewed. One example given here, which is a common scenario that arises for many CEs and BAs, is where a CE mails information to the wrong individual who opens the envelope and calls the CE or BA to say that he/she received the information in error. HHS points out that in such a case, the unauthorized recipient viewed and acquired the information because he/she opened and read the information and so this cuts against a finding that there is low probability that the PHI was compromised. To contrast, HHS offers an example of how to analyze this factor in the context of lost laptops. Specifically, HHS explains that if a laptop computer is stolen and later recovered and a forensic analysis shows that the otherwise unencrypted PHI on the laptop was never accessed, viewed, acquired, transferred, or otherwise compromised, the CE or BA could determine that the information was *not* *actually* acquired by an unauthorized individual even though the opportunity existed.

However, here HHS is also quick to point out that if a laptop is lost or stolen, HHS would not consider it *reasonable* to delay breach notification based on the hope that the computer will be recovered and that forensics might show that the PHI was never accessed.

4) Mitigation

The final factor to analyze is mitigation. HHS reminds CEs and BAs that each must attempt to mitigate the risks to PHI following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) or will be destroyed. When determining the probability that the PHI has been compromised, CEs and BAs should consider the extent of what steps needed to be taken to mitigate, and how effective the mitigation was. HHS offered an example that CEs and BAs may be able to obtain and rely on the assurances of an employee, affiliated entity, BA, or another CE that the entity or person destroyed PHI it received in error, while such assurances from *certain* third parties may not be sufficient.

1.4 *Reporting Obligations*

1.4.1 Each Authorized User is expected to notify the AtlantiCare HIE Privacy Officer and/or the AtlantiCare HIE Security Officer in the event that he/she becomes aware of any actual or suspected Security Breach of unsecured PHI accessed through the AtlantiCare HIE.

1.4.2 Notification shall be made in the most expedient time possible and without unreasonable delay.

1.4.3 Initial notification of the Breach or potential Breach may be made to the AtlantiCare HIE Privacy Officer or AtlantiCare HIE Security Officer, as appropriate, by telephone hotline.

1.4.4 Additional information to be included in any reports or third party notices shall be provided in writing.

1.5 *Responsibilities in the Event of a Breach*.

1.5.1 Each Authorized User must develop and implement a Breach plan as part of their HIPAA policies and procedures. The plan shall provide that, in the event the Authorized Users becomes aware of any actual or suspected Breach of unsecured PHI, either through notification by another Authorized User or otherwise, such Authorized User must, at a minimum:

- Notify the AtlantiCare HIE Privacy Officer and/or AtlantiCare HIE Security Officer, as appropriate, regarding the Breach or potential Breach;
- In the most expedient time possible and without unreasonable delay, investigate (or, in the case of a Connected-HIE, then to require its applicable sub-network participant to investigate) the scope and magnitude of such actual or suspected Breach, and identify the root cause of the Breach or potential Breach;
- Mitigate to the extent practicable, any harmful effect of such Breach that is known to the Participant. Participant's mitigation efforts shall correspond with and be dependent upon their

internal risk analyses.

- Cooperate with AtlantiCare and any other Authorized Users affected by the Breach to notify (or require the applicable Authorized User to notify) the Patient and any applicable regulatory agencies as required by and in accordance with applicable federal, state and local laws and regulations, including but not limited to HITECH and New Jersey's breach notification law.

1.5.2 The AtlantiCare HIE may conduct its own investigation, which Authorized Users must cooperate with. This includes providing the results of the internal investigation, including the facts and circumstances surrounding the incident, and any action taken to mitigate harmful effects. Authorized Users must cooperate with each other, the AtlantiCare IT Enterprise Steering Committee and Administrator, and any applicable regulatory agencies, whether state or federal.

1.6 The KeyHIE Breach Communication Policy is attached to this policy as additional guidance for Authorized Users.