



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy</b>	<b>Effective Date:</b>	<b>3/31/05</b>
<b>Subject:</b>	<b>Privacy Audits</b>	<b>Revision Date:</b>	<b>9/08/09</b>
<b>Policy #:</b>	<b>HIPAA-010</b>	<b>Review Date:</b>	<b>9/08/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>2</b>

---

**Scope:**

This policy applies to all Privacy Officers of Essent Healthcare, Inc., (“Essent”).

**Purpose:**

The purpose of this policy is to set forth the requirements for monthly HIPAA privacy audits.

**Policy:**

It is the policy of Essent to perform privacy audits on a monthly basis to ensure compliance with the HIPAA Privacy Rule. The purpose of these audits is to ensure that individuals who have access to protected health information (PHI) are properly authorized and that there is a legitimate business purpose for the access. Sanctions will be applied against any employee who accesses (or attempts to access) PHI without a legitimate business purpose in accordance with the sanctions policy.

---

**Procedure:**

1. All Privacy Officers are responsible for completing privacy audits on a monthly basis at their respective facilities.
2. Privacy audits shall consist of a sample of recent patient visits as follows:
  - a. Up to ten (10) employees and/or their dependants who were treated during the period under review are to be included in the sample (if less than 10 such patients exist they shall all be reviewed)
  - b. All VIP’s who were treated at the facility during the period under review are to be included in the sample
  - c. Five (5) randomly selected patients who were treated during the period under review are to be included in the sample
3. For each account sampled:
  - a. Run PCI and MIS audit logs to identify all individuals who have accessed the record
  - b. Review “disclosure accounting” logs
  - c. Review access to the medical record for appropriateness as defined by the Health Insurance Portability and Accountability Act (“HIPAA”)



## ESSENT HEALTHCARE, INC.

---

<b>Section:</b>	<b>HIPAA Privacy</b>	<b>Effective Date:</b>	<b>3/31/05</b>
<b>Subject:</b>	<b>Privacy Audits</b>	<b>Revision Date:</b>	<b>9/08/09</b>
<b>Policy #:</b>	<b>HIPAA-010</b>	<b>Review Date:</b>	<b>9/08/09</b>
<b>Responsible Party:</b>	<b>Corporate Compliance Officer</b>	<b>Revision #:</b>	<b>2</b>

---

- d. Research any instances of questionable access
  - e. Review questionable accounts with the Corporate Compliance Officer
  - f. Implement sanctions as needed
  - g. Document findings and resolutions
4. Enter the number of accounts reviewed and the findings on the monthly compliance report card which shall be reviewed during each quarterly compliance committee meeting.
  5. Every July, the monthly privacy audit shall be replaced with a “privacy review” to determine any physical threats to patient privacy. Privacy reviews shall include the following:
    - a. Perform a walk-through inspection of the facility making sure doors are locked as appropriate.
    - b. Identify areas within the hospital that may lead to privacy violations such as computer monitors that are positioned such that visitors might see the information or nursing stations that are unattended.
    - c. Document findings and proposed resolution.
    - d. Follow-up to ensure that the deficiencies have been addressed and that corrective action has been taken.
    - e. Summarize the results of the review (including methodology, findings, and resolution) and submit a report to the CCO.

### References:

HIPPA Subpart E