



ESSENT HEALTHCARE, INC.

Section: Information Systems	Effective Date: 4/20/05
Subject: Assigned Security Responsibility	Revision Date: 6/26/08
Policy #: ISP-000	Review Date: 6/26/08
Responsible Party: Chief Information Officer	Revision #: 2

Scope:

This policy applies to all workforce members and all facilities of Essent Healthcare, Inc., (“Essent”).

Purpose:

The purpose of this policy is to assign overall responsibility for the protection of sensitive information to one individual at each Essent facility.

Policy:

It is the policy of Essent to:

1. Protect all sensitive information from unauthorized use or disclosure.
2. Formally recognize a “Chief Security Officer” (CSO) who has ultimate responsibility for the security of sensitive information contained in the information systems of Essent
3. Formally recognize a security officer at each Essent facility. The “Facility Security Officer” (FSO) is responsible for assisting the CSO with all aspects of securing sensitive information.
4. Distribute policies and procedures governing the security of sensitive information to all workforce members so that they can successfully comply with those policies and procedures.
5. Periodically review and update the HIPAA security policies and procedures on an as needed basis.

Definitions:

Sensitive information includes, but is not necessarily limited to, the following:

1. **Protected Health Information (PHI)** – Any individually identifiable health information that is created, maintained, stored, or transmitted by the facility.
2. **Electronic Protected Health Information (ePHI)** – PHI that is in electronic format.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Assigned Security Responsibility	Revision Date:	6/26/08
Policy #:	ISP-000	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

3. ***Personnel files*** – Any information related to the hiring and/or employment of any individual who is or was employed by Essent Healthcare, Inc.
4. ***Payroll data*** – Any information related to the compensation of an individual during that individual's employment with Essent Healthcare, Inc.
5. ***Financial/accounting records*** – Any records related to the accounting practices or financial statements of Essent Healthcare, Inc.
6. ***Other information that is confidential*** – Any other information that is sensitive in nature or considered to be confidential.

Workforce: (As defined by the HIPAA Regulations) includes employees, volunteers (board members, community representatives), trainees, students, contractors, and any other persons under the direct control of a covered entity.

Procedure:

1. The Corporate Compliance Officer (CCO) shall appoint a Chief Security Officer (CSO) who will have overall responsibility for preventing, detecting, containing, and/or correcting any system security violations within Essent.
2. The CSO shall report directly to the CCO in all matters related to HIPAA security and/or any related policy or procedural matters or security violations.
3. The CSO shall provide an update regarding the overall status of system security to the CCO on a periodic basis.
4. The CSO shall be responsible for the following:
 - a. Appointing a Facility Security Officer "FSO" at each Essent facility.
 - b. Directing operations as they relate to information systems and information technology including purchasing, investment, maintenance, and security.
 - c. Implementing accounting procedures ensure that all hardware and software purchases in excess of \$1,000.00 are reviewed in the appropriate manner as outlined in the Capital Expenditures Request (CER) policy.
 - d. Implementing the administrative safeguards, physical safeguards, and technical safeguards associated with the HIPAA security regulations.
 - e. Oversight of the security of all sensitive information contained, created, maintained, or stored within the information systems of Essent.
 - f. Ensuring adequate staffing of the information systems department.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Assigned Security Responsibility	Revision Date:	6/26/08
Policy #:	ISP-000	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

- g. Performing periodic risk assessments to identify threats to and vulnerabilities of information systems at Essent.
 - h. Providing appropriate training and education of all personnel and/or contractors that have access to information systems.
 - i. Monitoring activity to ensure information systems are being used appropriately.
 - j. Preventing, detecting, and responding to security violations.
 - k. Developing contingency plans to deal with threats and vulnerabilities of information systems in the event of a natural or man-made disaster.
 - l. Developing and implementing safeguards to reduce threats to, and limit weaknesses of, information systems and sensitive data.
 - m. Enforcing all policies and procedures related to use of information systems through disciplinary measures where necessary.
 - n. Periodically reporting on the overall security of the information systems to the CCO.
 - o. Periodically updating security policies and procedures to reflect changes in the organization and/or changes in the regulations.
5. Each FSO shall assist the CSO in fulfilling his duties by implementing policies and procedures to prevent, detect, contain, and correct security violations at his/her respective facility.
6. Each FSO shall be responsible for the following:
- a. Implementing policies and procedures that are developed and approved by the CSO.
 - b. Notifying the CSO of all security threats and system vulnerabilities.
 - c. Monitoring system activity to ensure appropriate use and prevent unauthorized access to systems and/or data.
 - d. Implementing training at the direction of the CSO.
 - e. Implementing security measures such as virus scanning software, firewalls, and other mechanisms to protect the integrity of all electronic data housed in the information systems.
 - f. Performing periodic audits and/or risk assessments of system activity to ensure compliance with system and security policy and procedures.
 - g. Implementing contingency plans in the event of a disaster or security breach.
 - h. Processing day-to-day operating requests.
 - i. Responding to security violations and reporting such violations to the CSO.
 - j. Enforcing all policies and procedures related to the security of sensitive information, ePHI, and/or the systems in which such information is housed.
7. The FSO shall be responsible for ensuring that all workforce members and system maintenance



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Assigned Security Responsibility	Revision Date:	6/26/08
Policy #:	ISP-000	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

personnel are adequately supervised and/or have appropriate authorization when working with sensitive information or in areas that house sensitive information. Access to sensitive information or areas that house sensitive information shall be granted only under direct supervision of the department head, or with adequate proof of proper authorization which may include but is not limited to the following:

- a. Pre-employment background checks
 - b. Approved access authorization request form
 - c. Approved/valid contracts with vendors
 - d. Persons authorized by contingency plan in the event of an emergency
 - e. See Essent Policy IS-001 Access Authorization
8. The FSO shall be responsible for distributing security policies and procedures to all employees who have access to or work in areas that house sensitive information. The FSO shall distribute all relevant security policies and procedures to the department heads. The department heads shall be responsible for reviewing the security policies and procedures with each of their respective employees.
9. On a periodic basis, the CSO shall review and update relevant policies and procedures to reflect changes in the organizational structure of Essent, and/or any regulatory changes.

References:

NIST Special Publication 800-66
NIST Special Publication 800-12
Final HIPAA Security Rule 164.308(a)(2)