



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to IT Facilities	Revision Date:	4/20/05
Policy #:	ISP-006	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

Scope:

This policy applies to all employees and agents of Essent Healthcare, Inc. (“Essent”).

Purpose:

The purpose of this policy is to safeguard the confidentiality, integrity, and availability of protected health information (PHI) and other sensitive information within Essent’s information systems/applications by controlling access to the buildings/facilities that house these systems/applications.

Policy:

In an effort to safeguard PHI and other sensitive information from unauthorized access, tampering, or theft, it is the policy of Essent to restrict access to facilities that house information systems and/or contain sensitive information by:

1. Safeguarding all facilities and equipment from unauthorized access, tampering, and/or theft
2. Restricting access to systems that house sensitive information to only those individuals who are authorized to use such systems
3. Documenting system maintenance and repairs
4. Providing access to individuals as necessary to restore lost data in the event of an emergency via a written contingency plan.

Key Definitions

Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Protected Health Information (PHI): Individually identifiable health information that is created by or received by the organization, including demographic information that identifies an individual, or provides a reasonable basis to believe the information can be used to identify an individual, and relates to:

- Past, present or future physical or mental health or condition of an individual.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to IT Facilities	Revision Date:	4/20/05
Policy #:	ISP-006	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

- The provision of health care to an individual.
- The past, present, or future payment for the provision of health care to an individual.

Restricted Area: those areas of the building(s) where protected health information and/or sensitive organizational information is stored or utilized. These areas include, but are not limited to the following examples:

1. IS departments,
2. IS control desks,
3. Check-in desks/stations,
4. Nursing/Patient Care stations/desks,
5. Employee meeting rooms/kitchens located in patient care areas,
6. Mailrooms,
7. Offices,
8. Cubicles,
9. Storage closets and cabinets (including medication storage areas),
10. Information Services equipment rooms,
11. Business Office
12. Human Resources offices
13. Administrative offices.

Unrestricted Area: those areas of the building(s) where protected health information and/or sensitive organizational information is not stored or is not utilized there on a regular basis. These areas include the following:

1. Lunch rooms,
2. Conference rooms,
3. Building parking lots,
4. Building entry ways,
5. Main hallways, and
6. Restrooms.

Vendors: persons from other organizations marketing or selling products or services, or providing services to Essent. Examples include, but are not limited to the following:

1. Pharmaceutical Representatives,
2. Equipment Repair Service Personnel,



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to IT Facilities	Revision Date:	4/20/05
Policy #:	ISP-006	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

3. Food Services, and
4. Independent Contractors.

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

Workstation: An electronic computing device, such as a laptop or desktop computer, or any other device that performs similar functions, used to create, receive, maintain, or transmit ePHI. Workstation devices may include, but are not limited to: laptop or desktop computers, personal digital assistants (PDAs), tablet PCs, and other handheld devices. For the purposes of this policy, “workstation” also includes the combination of hardware, operating system, application software, and network connection.

Procedures:

1) Security of Restricted Areas

- A) Restricted areas and facilities must be locked and alarmed when unattended (where feasible). In situations where a restricted area cannot be locked, all workstations, filing cabinets, and other equipment that houses or accesses sensitive information must be secured when unattended or not in use.
- B) Preferred methods of security include: electronic key card where possible, locked door with punch code lock, locked door with a separate key.
- C) Only authorized workforce members may receive keys to access restricted areas (as determined by the Facility Security Officer through Departmental requests).
- D) Restricted areas that house information systems or sensitive information must have appropriate controls in place to ensure that temperature and humidity are maintained at ideal levels, and that electric power to critical systems cannot be interrupted (as outlined in the contingency plan/emergency mode operations plan).
- E) Workforce members are required to return the key(s) to the Human Resources department (or Supervisor) on their last day of employment/last day of contracted work or services being provided.
- F) Workforce members must report lost and/or stolen key(s) to the Facility Security Officer immediately.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to IT Facilities	Revision Date:	4/20/05
Policy #:	ISP-006	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

G) The Facility Security Officer is responsible for facilitating the changing of the lock(s) within 24 hours of a key being reported lost/stolen and maintain a log of all such activities.

2) Identification of Authorized Persons

- A) All workforce members must wear an identification badge at all times while at any Essent facility.
- B) Workforce members are required to return their identification badge to the Human Resources department (or Supervisor) on their last day of employment.
- C) Visiting vendors must register (sign in and out) on the Hospital Visitor Log and obtain visitor identification badges from the department they are visiting. Vendors are instructed to return the visitor identification badge and sign out prior to leaving the premises.
- D) In the event of an emergency that requires a facility to employ a written contingency plan, authorized persons may include vendors and other outside resources. These individuals must register (sign in and out) on the Hospital Visitor Log and obtain visitor identification badges from the department they are visiting. These individuals must be escorted at all times during the contingency period. Vendors are instructed to return the visitor identification badge and sign out prior to leaving the premises.

3) Persons Allowed in Restricted Areas

- A) Workforce members will be allowed into restricted areas only upon approval and only when needed to perform their job duties.
- B) Patients will be allowed into restricted areas only if they are accompanied by an authorized workforce member.
- C) Family members and friends briefly visiting workforce members may enter a restricted area only if an authorized workforce member is present as an escort.
- D) Vendors (wearing an Essent Visitor ID badge) will be allowed into restricted areas only if an authorized workforce member is present as an escort.
- E) Essential vendor resources (wearing an Essent Visitor ID badge) during a contingency period will be allowed into restricted areas only if an authorized workforce member is present as an escort.
- F) Vendors at Essent on a long-term contract (wearing an Essent Visitor ID badge), are allowed into restricted areas, once acclimated to the areas, without an escort.

4) Persons Allowed in Unrestricted Areas



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Access to IT Facilities	Revision Date:	4/20/05
Policy #:	ISP-006	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

- A) Workforce members
- B) Patients
- C) Vendors
- D) Workforce family members and friends
- E) All visitors

5) **Enforcement**

- A) All employees are responsible for escorting unauthorized personnel out of restricted areas immediately.
- B) Report violations of this policy to the Facility Security Officer.
- C) Workforce members in violation of this policy are subject to disciplinary action, up to and including termination.
- D) Visitors in violation of this policy are subject to removal from premises, loss of vendor privileges and/or termination of services from Essent.

References:

HIPAA Section 164.310(a)
NIST Special Publication 800-12
NIST Special Publication 800-14
NIST Special Publication 800-18
NIST Special Publication 800-53
CMS Information Security Acceptable Risk Safeguards (Version 1.1; April 7, 2004)