



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Device and Media Controls	Revision Date:	5/23/07
Policy #:	ISP-003	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Scope:

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

Purpose:

The purpose of this policy is to set forth guidelines governing the receipt and/or removal of hardware and/or electronic media that contain electronic protected health information (ePHI) or other sensitive company information into and out of the facility, the movement of such items within the facility, and the individual(s) responsible for their safekeeping. Unless secure measures are undertaken to ensure complete removal of sensitive information from media and storage devices prior to the disposal of such devices, unintended disclosure may occur.

Policy:

It is the policy of Essent to:

1. Protect the confidentiality and integrity of sensitive information by monitoring the receipt and/or removal of electronic media and storage devices into and out of the organization. Electronic media and storage devices includes: computers (desktop and laptop), hard drives, removable disks, floppy drives, CD ROM's, optical disks, PCMCIA cards, memory sticks, personal hand-held computer devices, and all other forms of movable media and/or storage devices.
2. Maintain records of the movement of hardware and electronic media within the organization.
3. Maintain records of the individual(s) responsible for safeguarding sensitive information and/or the equipment that houses sensitive information.
4. Recover all company information, electronic devices, documents, media, and/or storage devices from departing employees regardless of the reason for termination.
5. Destroy sensitive information contained on any storage device or electronic media prior to disposing of or reusing such media or devices.
6. Maintain records of the destruction, disposal, or reuse of any electronic media or storage devices.

All procedures developed by each facility pursuant to this policy must be submitted to the Facility Security Officer (FSO) and the Chief Security Officer (CSO) for approval.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Device and Media Controls	Revision Date:	5/23/07
Policy #:	ISP-003	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

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.
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. **Legal matters** – any information concerning any regulatory issues, complaints, lawsuits, or filings in local, state, or federal agencies or courts, or any legal contracts or agreements with any employee, vendor or other third party.
7. **Other information that is confidential** – Any other company 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 for Recovering Hardware and Other Storage Devices from Departing Employees

1. Department managers are responsible for coordinating with Human Resources and Information Technology in recovering all hardware and/or any other electronic storage devices from departing employees on or before their last day of employment. Department managers shall notify Human Resources if employees fail or refuse to return company property. Upon notification of failure to return company property by a departing employee, Human Resources shall withhold final paychecks and/or severance payments until all company property is returned.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Device and Media Controls	Revision Date:	5/23/07
Policy #:	ISP-003	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

2. Department managers are responsible for coordinating with Information Technology in recovering all documents and any other company information from departing employees on or before their last day of employment.
3. Department managers are responsible for obtaining the passwords associated with all password-protected files for which the departing employee was responsible for or had sole access to.
4. Department managers must coordinate with Information Technology and Human Resources to ensure that the CISD Help Desk is notified of all departing employees so that system access can be terminated. This notification shall occur within 24 hours of employee termination.

Procedures for Destruction of Storage Devices or Media:

1. Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device does not contain sensitive information and that the proper authorizations have been completed.
2. If the device or media contains the only copy of any sensitive information that is required to be retained until some future date, a retrievable copy of the information must be made prior to disposal of the device/media.
3. If the device or media contains sensitive information that is no longer needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to disposal. A typical "reformat" is not sufficient as it does not overwrite the old data.
4. Data disposal may occur through the use of complete overwriting of data, degaussing, or physical destruction. Physical destruction is required for non-functioning and/or non-writable media, except where prohibited by hardware vendor warranty replacement policies. Overwriting or degaussing methods should be used on any functioning media that may be disposed in a manner that does not prevent media reuse by third parties as may be required with leased equipment, exchanges, trade-ins, or resale of used equipment/media.
5. Documentation of the authorization and final disposition of data and equipment is mandatory. Disposal documentation must clearly identify the asset/media to be disposed of and include the date and means of authorization, removal of media, removal of data, and disposal of the device/media. This documentation must be maintained for a period of six years from the date of disposal/destruction.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Device and Media Controls	Revision Date:	5/23/07
Policy #:	ISP-003	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

6. Disposal activities will be periodically audited by the CSO. Violations of this policy will lead to sanctions up to and including termination of employment.

Procedures for Reuse of Storage Devices or Media:

1. Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain sensitive information.
2. If the device or media contains the only copy of any sensitive information that has not met its minimum retention period, a retrievable copy of the information must be created prior to reuse.
3. If the device or media contains sensitive information that is no longer needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical “reformat” is not sufficient if the equipment is being disposed of – reformat may only be used when the media is to be reused within the facility.
4. If using removable media for purposes of a system backup and disaster recovery, and the removable media is stored and transported in a secure environment, the use of a data destruction tool between uses is not necessary.
5. Reuse of equipment practices will be periodically audited by the CSO. Violations of this policy will lead to sanctions up to and including termination of employment.

Procedures for Movement of Equipment Housing Sensitive Information:

1. Prior to the movement of equipment housing sensitive information, each department is responsible for determining whether an exact, retrievable copy of the sensitive information is required.
2. When using storage devices and removable media to transport sensitive information, each FSO must implement a procedure to track and maintain records of the movement of such devices, the authorization, and the media/parties responsible for the information during its movement.
3. The movement of equipment will be periodically audited by the CSO. Violations of this policy will lead to sanctions up to and including termination of employment.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/20/05
Subject:	Device and Media Controls	Revision Date:	5/23/07
Policy #:	ISP-003	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	2

Accountability Procedures:

1. The CSO is responsible for the movement of hardware and electronic media into, out of, and within each facility.
2. The CSO shall maintain an inventory of all systems, applications, and/or hardware that contains sensitive information, the physical location of the system/application, and the person responsible for maintaining the security of the system.
3. The inventory must be continuously updated to reflect changes, additions, and/or deletions of systems/equipment.
4. The CSO must implement a tracking system for monitoring:
 - a. The movement of hardware/sensitive information within the organization,
 - b. The party responsible for safeguarding the information while it is being moved,
 - c. The steps taken to “sanitize” equipment before disposal or reuse, and
 - d. Authorizations for purchase, sale, or disposal of equipment/storage media.

References:

HIPAA Section 164.310(d)
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)