



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Data Backup and Storage	Revision Date:	4/21/05
Policy #:	ISP-005	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

Scope:

This policy is applicable to all Essent information systems that contain confidential and/or sensitive information.

Purpose:

The purpose of this policy is to set forth guidelines for protecting against loss of important information stored within the information systems of Essent by requiring periodic information backups.

Policy:

It is the policy of Essent to create and maintain exact, retrievable copies of all sensitive electronic information based on the schedule described below. Each FSO must maintain a log for all backups performed. All backup media rotations must include off-site storage.

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.
4. **Payroll data** – Any information related to the compensation of an individual during that individual's employment with Essent.
5. **Financial/accounting records** – Any records related to the accounting practices or financial statements of Essent.
6. **Other information that is confidential** – Any other information that is sensitive in nature or considered to be confidential.

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



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Data Backup and Storage	Revision Date:	4/21/05
Policy #:	ISP-005	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

Procedure:

This procedure should be followed at every Essent facility for every system that contains confidential or sensitive data in electronic format.

MEDITECH (MAGIC and Client Server) and LAN based Servers

Frequency/Method

- A full back-up of each MEDITECH and LAN based server must be performed nightly during a time of lowest system activity. For MAGIC systems, on one of the weekly backups a spot check must be done to ensure reliability of the tape and tape drive.
- Tape drives must be cleaned according to the drive manufacturer's recommendations and the cleaning tape used only the number of times prescribed by the media manufacturer.
- A minimum 14-day tape rotation is required. Enough media should be procured in order to maintain at least one full rotation off-site.

Media Storage

- Only tapes that are certified by Meditech may be used for backup purposes.
- Media tapes should not be re used after they have exceeded the manufacturers' threshold.

Log

- Backup attempts must be logged daily. Unsuccessful backups must get resolved within 24 hours of failure. Any hardware or software upgrades that are direct result of solving the backup issue must be documented in the log.
- Hardware issues related to the Dell servers are covered under the 7X24 GOLD service package from Dell.



ESSENT HEALTHCARE, INC.

Section:	Information Systems	Effective Date:	4/21/05
Subject:	Data Backup and Storage	Revision Date:	4/21/05
Policy #:	ISP-005	Review Date:	6/26/08
Responsible Party:	Chief Information Officer	Revision #:	1

- All logs must be retained for at least six years.

Each facility is responsible for the integrity of the backups performed at that facility and is required to maintain an accurate daily log. These logs will be subject to audits performed by the CISD.

The CISD Network Manager is responsible for the integrity of the backups performed at the CDC and is required to maintain an accurate daily log. These logs will be subject to audits by peers. Logs should be kept for six (6) years.

Department managers that are responsible for department specific systems are required to maintain the integrity of their daily backups. These backups will be subject to audits by the FSO.

References:

HIPAA Section 164.308(a)(7)(ii)(A)
NIST Special Publication 800-12
NIST Special Publication 800-18
NIST Special Publication 800-53