



## ESSENT HEALTHCARE, INC.

---

|                           |   |                        |                |
|---------------------------|---|------------------------|----------------|
| <b>Section:</b>           | <b>Information Technology</b>             | <b>Effective Date:</b> | <b>4/20/05</b> |
| <b>Subject:</b>           | <b>Disaster Recovery/Contingency Plan</b> | <b>Revision Date:</b>  | <b>4/20/05</b> |
| <b>Policy #:</b>          | <b>ISP-017</b>                            | <b>Review Date:</b>    | <b>6/26/08</b> |
| <b>Responsible Party:</b> | <b>Chief Information Officer</b>          | <b>Revision #:</b>     | <b>1</b>       |

---

### Scope:

This policy applies to all Information Systems team members at all Essent Healthcare, Inc., (“Essent”) facilities.

### Purpose:

The purpose of this policy is to establish procedural guidelines in the event of an emergency that requires a facility to enter a contingency period where normal computing operations are either limited or entirely unavailable while ensuring the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI).

### Policy:

It is the policy of Essent to ensure that efficient patient care and hospital operations continue in the wake of a loss of computing services while taking the appropriate steps to restore those services in the least amount of time.

---

### *Procedures:*

Effective immediately it is required that all mission-critical network, server, and storage devices and all approved software application or operating system packages in the Essent computing enterprise are covered under either a warranty or maintenance contract from the original equipment manufacturer (OEM) or under a warranty or maintenance contract with an approved third-party vendor. The specifications and terms of any warranty or maintenance agreement must be commensurate with the mission criticality of the device or software. All agreements must be reviewed and approved by the CSO or their designee.

In the event of a catastrophic system failure as defined by the loss of one or more systems within one or more of the hospitals the following procedure should be adhered to.

1. The helpdesk personnel and/or the On-call person are notified of the problem by the facility users.
2. The extent of the problem will be assessed by the on-call person. Notification will go to the facility Information Systems Director, if the issue is deemed as a disaster. The Director or a designee will then notify the Corporate IS team, local administration, and the local department heads.
3. Department heads will be required to have the users go on downtime procedure, while the systems are not available.



## ESSENT HEALTHCARE, INC.

---

|                           |   |                        |                |
|---------------------------|---|------------------------|----------------|
| <b>Section:</b>           | <b>Information Technology</b>             | <b>Effective Date:</b> | <b>4/20/05</b> |
| <b>Subject:</b>           | <b>Disaster Recovery/Contingency Plan</b> | <b>Revision Date:</b>  | <b>4/20/05</b> |
| <b>Policy #:</b>          | <b>ISP-017</b>                            | <b>Review Date:</b>    | <b>6/26/08</b> |
| <b>Responsible Party:</b> | <b>Chief Information Officer</b>          | <b>Revision #:</b>     | <b>1</b>       |

---

4. Establish a MIS Hot Line in the command center for procedural instructions.
5. Damage Assessment

### MEDITECH Software and Hardware Failure

The servers for Sharon Hospital, Merrimack Valley Hospital, and Paris Regional Medical Center are currently housed in their respective facilities. For those facilities not yet on the Corporate Data Center, they will be required to follow the procedures found in this policy as closely as the situation allows and engage the appropriate vendors that their facility is contracted with for service and support.

The servers for Crossroads Regional Medical Center and Nashoba Valley Medical Center are located in the Essent Healthcare Data Center. The servers support the two facilities with MEDITECH Clinical and Financial systems. The hardware used is provided from Dell Corporation with EMC storage system. They are under Dell GOLD maintenance with 7X24X4 coverage. All hardware failures will be handled with Dell authorized personnel. The procedure for handling the call is as follow:

1. If the system is assessed to be repairable by internal means, the technician reporting to assess the damage will make the repair and notify all appropriate personnel including the Facility Director of Information Systems (FDIS) and the Essent Healthcare CIO.
2. If internal personnel assess the system to be non-repairable, then external vendors will be called.
3. If internal or external personnel assess the system to be non-repairable in a timely manner, the following method should be used to restore service to critical areas.
  - a. Backup tapes should be retrieved from offsite storage. Backups are performed in accordance with policy # **ISP-005**.
  - b. In the event of a failure of one or two of the non clinical servers, the only course of action is replacement of broken components or the purchase of a new server or new components.
  - c. Corporate IS personnel / vendor resources would then work with MEDITECH to move backup data from the other clinical systems to the new servers. MEDITECH is the software vendor for each facility's HCIS. MEDITECH has 7X24 support coverage.
  - d. Corporate IS personnel / vendor resources would then work to continue to replace broken components and restore service back to the existing hardware.

### WAN Infrastructure Disaster



## ESSENT HEALTHCARE, INC.

---

|                           |   |                        |                |
|---------------------------|---|------------------------|----------------|
| <b>Section:</b>           | <b>Information Technology</b>             | <b>Effective Date:</b> | <b>4/20/05</b> |
| <b>Subject:</b>           | <b>Disaster Recovery/Contingency Plan</b> | <b>Revision Date:</b>  | <b>4/20/05</b> |
| <b>Policy #:</b>          | <b>ISP-017</b>                            | <b>Review Date:</b>    | <b>6/26/08</b> |
| <b>Responsible Party:</b> | <b>Chief Information Officer</b>          | <b>Revision #:</b>     | <b>1</b>       |

---

The WAN of Essent Healthcare is based on multi-protocol label switching (MPLS) technology supplied by AT&T and it connects all facilities to the Data Center and to each other via a fully meshed design.

1. If the system is assessed to be repairable by internal means, the technician reporting to assess the damage will make the repair and notify all appropriate personnel including the Director of Information Systems and the Corporate Network Manager or their designee.
2. If internal personnel assess the system to be non-repairable, then external vendor will be called. Currently a service contract exists with Nextira One to support all Cisco WAN components. Nextira One has 7X24X4 support coverage.
3. In an event that the failure is due to the telecommunications lines, AT&T is notified of the issue. AT&T has 7X24X2 support coverage.

### **LAN File Server Disaster**

The LAN infrastructure is the responsibility of the facility IS department. If the system is assessed to be repairable by internal means, the technician reporting to assess the damage will make the repair and notify all appropriate personnel including the Director of Information Systems. If internal personnel assess the system to be non-repairable, then external vendors should be called. Currently a service contract exists with Dell on the file servers. The current LAN switches are under service contract with Nextira One. It is the responsibility of the information systems director or their designee at each Essent facility to provide the corporate network manager with any network device inventory changes as the Nextira One contracts are maintained centrally.

### **Testing and Policy Revision**

It is required that testing and logging of the following items be completed quarterly and any suggested changes to the disaster recovery and contingency plan be submitted to the CSO:

- Back-up electrical generator testing
- Uninterruptible power supply (UPS) testing
- Fire suppression validation
- Temperature controls (HVAC)
- Hardware / software inventory verified against the inventory of maintenance / support providers' contracts
- Verify escalation procedures with hardware / software maintenance / support vendors
- Review down time procedures



## ESSENT HEALTHCARE, INC.

---

|                           |   |                        |                |
|---------------------------|---|------------------------|----------------|
| <b>Section:</b>           | <b>Information Technology</b>             | <b>Effective Date:</b> | <b>4/20/05</b> |
| <b>Subject:</b>           | <b>Disaster Recovery/Contingency Plan</b> | <b>Revision Date:</b>  | <b>4/20/05</b> |
| <b>Policy #:</b>          | <b>ISP-017</b>                            | <b>Review Date:</b>    | <b>6/26/08</b> |
| <b>Responsible Party:</b> | <b>Chief Information Officer</b>          | <b>Revision #:</b>     | <b>1</b>       |

---

- Test random tape from off-site storage for restoration viability

### **Mirror-site / Complete Hardware Replacement**

In the event of a total facility disaster at the Waltham data center, efforts are ongoing to establish a process that may include an outsourced mirror site, the establishment of a mirror site within another Essent facility, and / or a contract agreement with a hardware vendor that is capable of supplying a full interim system replacement at one of Essent's New England facilities within 24 hours.

### **References:**

HIPAA Section 164.308a7iiB  
HIPAA Section 164.308a7iiC  
HIPAA Section 164.310a2i  
NIST Special Publication 800-12 & 800-53