Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #7

Data Backup and Contingency Planning Procedure

Last Revised: 3/15/2006	*Approved: 12/12/2005*

Scope of Procedure

The scope of this Procedure covers the steps that RO follows to protect or recover from an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains EPHI is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Planning
- Emergency mode operation plan

1) Applications and Data Criticality Analysis

The HIPAA Security Committee will review application criticality (to patient care) relative to risk and security measures each year when it convenes for its periodic assessment of HIPAA procedures in the department.

The initial assessment revealed that all critical (to patient care) applications reside on BJ Hospital computers managed by the BJC Information Systems Group. (See BJC's Information Systems Disaster Recovery Procedures)

2) Data Backup Plan

The following general plan is provided to describe the department's backup procedures for computers storing EPHI and managed by WU staff.

- Type of data: Computers store no critical (to patient care) data
- Department, Off-Site storage: Secure computer room, FP 208-10 serves as offsite storage site for secure computer room, CSRB 4441, and vice versa. Backup media in each facility are stored in locked cabinets within the secure computer rooms.
- Media: LTO and DLT tape, removable hard drives
- Courier: The department engages Access Courier to transport tapes between sites. A Business Associate agreement has been signed.

- Testing for recovery: Requests for recovery of files provide a real-time test of backup recovery. The backup procedures will be reviewed at the HIPAA Committee annual, periodic assessment of HIPAA procedures in the department.

3) Disaster Recovery Plan

Overview: The RO Department Disaster Recovery process, for purposes of EPHI protection and restoration, is included in the Computer Disaster Recovery section of the Department Emergency Plan.

- Department Emergency Plan and Procedures (General response and recovery)
- Computer Disaster Recovery (Specific Computing response and recovery)

Department Emergency Procedures

The Department Emergency Plan is part of the general WUSM Emergency Plan. The Department Emergency Plan is organized by physical facility and contains the following response items:

- Notification calling trees
- Emergency response teams
- Emergency assembly areas and communication guidelines
- Emergency safety procedures
- Illness and injury management procedures
- Location of emergency supplies

Regular evaluation drills and emergency power tests are conducted. In the handbook the following section, Computer Disaster Recovery Procedures, details computer recovery procedures.

Computer Disaster Recovery Procedures

1. Response (anyone, after attending to safety and any injury to patients and workforce):

- Notify the appropriate Information Systems section:
  - OCF Help Desk Support — Call : 314.362.9740
  - OCF Web Support Request — http://rocweb/oissupport
  - BJC IS Help Desk — Call : 314.362.4700
- If patients are being treated, document treatment and billing information on paper for later data entry

2. Recovery (OCF will take the following steps; BJC IS follows BJ recovery plan):

- Assessment of availability and capability of:
  - Personnel

- Assess operational status and damage to:
  - Computer rooms (power, HVAC, etc.)
  - Network infrastructure(firewalls, switches, links)
  - Network services(WUSTL, WUCON, RO, CARENET)
  - Servers (evaluate operational status, event logs)
  - Applications (evaluate operational status)
  - Data (perform database integrity checks, evaluate logs)

- Formulate and execute recovery plan based upon damage assessment
  - Plan staged recovery at recovery computing site
  - Restore vital network links and infrastructure as needed
  - Reconfigure servers as needed
  - Restore Applications and data from backup
  - Restore secondary services

- Reevaluate

4) Emergency Mode Operation Plan

Emergency mode operation of patient treatment in Radiation Oncology requires calibrated treatment machines to be operating in a safe and effective manner as well as access to the electronic copy (or hardcopy) of patient medical records. Treatment machine operation is the responsibility of BJH Clinical Engineering; IMPAC MultiAccess (EMR) and Clinical Desktop application access is the responsibility of BJC Information Systems; access to hardcopy of patient medical records is the responsibility of BJH Health Information Management (HIM). Emergency mode operation of the clinic would be coordinated with these BJ groups by the Radiation Oncology Executive Director.

In the event that the Siteman clinic is destroyed or inoperable, the RO Department Chairman and Executive Director would be required to make arrangements to utilize another Radiation Oncology facility to treat patients during the repair of the Siteman facility.

Emergency mode operation will be reviewed (as necessary) at the annual meeting of the RO HIPAA Committee.