

**TITLE: EPHI9. INFORMATION SECURITY: DISASTER CONTINGENCY
AND RECOVERY PLAN**

POLICY:

CUMC conducts risk-based analysis to develop procedures and plans to address continuity of its operations in case of loss of Electronic Protected Health Information (EPHI) systems.

PURPOSE:

CUMC addresses possible availability problems caused by natural or man-made accidents and disasters.

APPLICABILITY:

Owners and custodians of information systems, Senior management of operational areas

PROCEDURES:

1. Each Department is required to perform a *Business Risk Assessment* for each EPHI system application that is used in the department's operations. The assessment should identify and define the criticality of applications and the repositories or data flows that contain the relevant and necessary data for the application. It should also address the frequency, and elements for data backups and the department's Disaster Contingency and Recovery plans.
2. Departmental **Disaster Contingency and Recovery Plan** includes:
 - A. An *Emergency Mode Operations Plan* for continuing short-term operations in event of temporary hardware, software, or network outage. This plan should contain information related to the end user process for continuing operations.
 - B. A *Recovery plan* for returning functions/services to normal on-site operations when a disaster is complete.
 - C. A procedure for periodic testing, review and revision of the Plan for all affected systems, as a group and individually as needed.
3. Each EPHI system should have a **Contingency Plan** documented for when hardware, software or networks become critically dysfunctional or cease to function (long term outage). (Consult Information Security Office for *Application security documents list: Emergency access, DR/ backup/ contingency.*) This plan may include an explanation of the magnitude of information or system unavailability in event of a long term outage and the process that would be implemented to continue operations during the long

term outage. In addition, the feasibility of utilizing alternative off-site computer operations should be addressed.

4. Information systems owners and custodians implement a **Data Backup Plan** or document the decision to forgo a plan with a risk-based analysis. See **Information security: Backup, device and media controls policy** (#EPHI7) for security of backup media and consult Information Security Office for documentation in *Application security documents list: Emergency access, DR/backup/ contingency* The plan should:
 - A. Define who is responsible for taking reasonable steps to ensure the backup of EPHI.
 - B. Define a backup schedule.
 - C. Specify the EPHI systems that are to be backed up.
 - D. Define where backup media is to be stored and workforce members who may access the stored backup media.
 - E. Define where backup media is to be kept secure before it is moved to storage, if applicable.
 - F. Define who may remove the backup media and transfer it to storage.
 - G. Define restoration procedures to restore EPHI from backup media to the appropriate information system
 - H. Define test restoration procedures and frequency of testing to confirm the effectiveness of the plan.
 - I. Document the retention period for backup media.

POLICY MAINTENANCE:

Information Security Office

REFERENCES:

All information security policies

CU Administrative policies in Computing & Technology

Health Insurance Portability and Accounting Act of 1996, 45 CFR

164.308(a)(7)(i), 164.308(a)(7)(ii)(A),
164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C),
164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E)

REVIEW/REVISION DATE:

November 2007