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

POLICY:

Risk-based analyses are conducted to develop procedures and plans to address continuity of institutional operations in case of loss of information systems, including systems that store sensitive data including EPHI and PII.

PURPOSE:

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

APPLICABILITY:

Owners and custodians of information systems, Vice presidents of operational areas

PROCEDURES:

1. Each department is required to perform a *Business Continuity Assessment* for each information 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** should include:
   A. An *Emergency Mode Operations Plan* for continuing short-term operations in the event of temporary hardware, software, or network outage. This plan should contain information related to the end user process for continuing operations. This plan should be strategically aligned with the Hospital's ***Disaster and Emergency Operations Plan***.
   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.

3. Each information 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 to be implemented to continue operations. In addition, the feasibility of utilizing redundant hardware and/or alternative off-site computer operations should be addressed.

4. Information systems owners and custodians will 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*** (# I240) for security of backup media. Consult Information Security Office for documentation in *Application security documents list: Emergency access, DR/ backup/ contingency.* The plan should:

    A. Identify who is responsible for taking reasonable steps to ensure the backup of sensitive data.
    B. Define a backup schedule.
    C. Ensure that any backups to be stored offsite are encrypted.
    D. Specify the systems storing sensitive data that are to be backed up.
    E. Identify where backup media are to be stored and workforce members who may access the stored backup media.
    F. Identify where backup media are to be kept before it is moved to storage, if applicable.
    G. Identify who may remove the backup media and transfer it to storage.
    H. Define procedures to restore sensitive data from backup media to the appropriate information system.
    I. Ensure that recovery procedures are exercised annually and that deficiencies are addressed in a timely manner.
    J. Define test procedures and frequency of testing to confirm the plan effectiveness.
    K. Document the retention period for backup media.

RESPONSIBILITY:

Information Security Office

REFERENCES:

All information security policies
Health Insurance Portability and Accountability 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:

March 2005
June 2009
June 2011
Revised: June 2013; **March 2015**