
Department: UW Medicine Information Technology Services

Policy Number: SEC-07 Business Continuity Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose:

This UW Medicine¹ Policy describes the required elements for a Business Continuity and Disaster Recovery plan. The plan describes how to maintain operations in response to an emergency and how to regain normal operations.

Definitions:

- See SEC-REF UW Medicine Information Security Program Glossary of Terms.

Policy:

All Systems with high availability requirements must have a Business Contingency and Disaster Recovery plan.

It is the responsibility of the System Owner to create and maintain the following:

- I. Business Impact Analysis
See UW Medicine Information Security Standard: *SEC-07.01 Information Security: Business Impact Analysis Standard.*
- II. Risk Assessment
See UW Medicine Information Security Standard: *SEC-09.01 –Risk Assessment Guideline.*
- III. System Criticality

¹ For the purposes of HIPAA UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; UW Physician's Eastside Specialty Center; Hall Health Primary Care Center; University of Washington Physicians; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine and University of Washington Health Care Components are subject to the UW Medicine Information Security Program.

The UW Medicine Confidentiality and Access Steering Committee and the UW Medicine Clinical Systems Advisory Committee periodically assess the relative criticality of enterprise systems. Departments that maintain their own systems, Department Administrators/Managers and System Owners must periodically assess the relative criticality of their systems in support of their contingency plans.

IV. Data Backup Plan

The plan should include who is responsible for the recovery process, allowable recovery period, recovery time objective, recovery point objective, frequency, retention period, off-site requirements, and logging of media,. This determination may be based upon how often data changes and how important those changes are. See UW Medicine Information Security Policy, *SEC-05 – Communications and Operations Management Policy*.

V. Disaster Recovery Plan

The Disaster Recovery plan establishes and implements procedures to restore data that is destroyed or unavailable after a disaster or disruption. The disaster recovery plan should cover all essential and critical business services. It is recommended that the System Owner review contracts with vendors for any specific requirements that may be needed for the recovery strategy.

Disaster Recovery plans must be documented and kept with other system documentation. Please see UW Medicine Information Security Standard *SEC-07.02 – Server Disaster Recovery Form*. Please contact IT Services Help Desk if you want to use UW Medicine's enterprise software to document your Disaster Recovery plan.

VI. Emergency Mode Operation Plan (Contingency Plan)

Each UW Medicine Entity has Emergency Processes that are activated (e.g., the Hospital Emergency Incident Command System (HEICS) processes) when systems are unavailable after a disaster or a significant disruption. Each entity must establish and implement procedures to enable continuation of critical business processes for the protection of the security of electronic protected health information while operating in emergency mode. These procedures should include processes for obtaining access to necessary ePHI during an emergency.

VII. Testing and Revision

Disaster recovery plans are periodically tested and kept up to date to take into account changing circumstances to ensure that they can be implemented in emergency situations and that the management and staff understand how they are to be executed.

VIII. Applications and Data Criticality Analysis

It is the responsibility of the UW Medicine Confidentiality and Access Steering Committee and the IT Services IT Steering Committee to periodically assess the relative criticality of enterprise systems. When departments maintain their own systems, Department Administrators/Managers and System Owners must periodically assess the relative criticality of their systems in support of their contingency plans.

References:

- I. 45 CFR Part 164; Section 308(a)(7) (i) Contingency Plan
 - II. 45 CFR Part 164; Section 308 (a) (7) (ii) (B) Disaster Recovery Plan, (C) Emergency Mode Operation Plan, (D) Testing and Revision Procedures, (E) Applications and Data Criticality Analysis
 - III. 45 CFR Part 164; Section 310 (a) (2) (i) Contingency Operations
 - IV. 45 CFR Part 164; Section 312 (a) (2) (ii) Emergency Access Procedure
 - V. ISO/IEC 17799 Section 11, Business Continuity Management
-
-

UW Medicine IT Services: _____ Date: _____
James S. Fine, M.D., CIO, ISO
