Attachment 3 - Validation and Operation of Research Biorepository Informatics Systems

Dependability

Research biorepositories informatics management systems should have an operational infrastructure to support operation access 24 hours a day, seven days a week.

Disaster recovery

Research biorepositories informatics management systems should have processes defined and in place to cope with system downtimes and disaster recovery. System backups and restores should be tested on a regular basis to ensure the quality of the backup media and the restore process. All data stored outside the system should be encrypted to secure Protected Health Information (PHI) and Personally Identifiable information (PII).

Quality control

Research biorepositories informatics management systems should be periodically evaluated to ensure that the system is fulfilling the criteria advised in best practices and the latest needs of the research biorepository. Random quality control checks should be performed on the physical inventory confirming that the physical location of stored biospecimens matches that provided in the informatics system. All system tools and methods should be validated to ensure their accuracy in performing that task.

Physical security

All Research biorepository databases at an individual institution should be in a secure site monitored by the institution. Resources without the capabilities to provide such infrastructure should seek external hosting arrangements for their informatics system.

Software system validation

Initial validation of the informatics system should be well-documented ensuring data integrity, accurate process workflow and adequate audit trail.

A detailed written validation plan must identify high risk areas in the software and how they will be thoroughly tested. Particularly susceptible areas are data migration points, data flow junctures, system configurable areas, and any customised features.

A new software implementation requires more comprehensive testing than an upgrade to an existing system. A system upgrade should include re-testing of updated program elements and any high-risk areas of the program, whether presumed to be updated or not. To adequately test an upgraded system, a copy of the existing data should be used in a separate test environment.

Subsequent validation of each upgrade to the system should replicate a portion of the initial validation to prevent unidentified regression errors as well as a full validation of the upgraded portion of the system.