Criticality & Recovery Preparedness: ePHI Systems
5100 EX.A

Criticality Designation

1. Primary source of PHI *for treatment (patient care)*
2. Primary source *for billing or scheduling or other healthcare operations not related to treatment*; or primary source *for approved research study*
3. Primary source of PHI *for pre-research*; or secondary source of PHI *for research/pre-research*; secondary source of PHI *for treatment, payment or healthcare operations; or teaching*

Criticality mapped to Recovery Preparedness Levels

Level-1 includes critical applications or data that require and can afford the cost of the highest level of availability.

- Recovery Goal: These systems will sustain a single failure without loss of service or with an outage of less than one (1) hour.
- Typical system configuration:
  - includes multiple machines running in a clustered, automatic or rapid failover environment;
  - may include shared data across more than one location; and
  - includes a fully functional alternate service on another server, or at another site, if one server fails.
- Current examples in this category include:
  - Transplant database; DI Dicom Server

Level 2 includes critical services for which the cost of keeping data in sync across primary and back-up servers may not permit Level 1 preparedness.

- Recovery Goal: These systems can be restarted in a fully functional condition at an alternate site including all data and systems capability within a four (4) hour window, once the decision to failover is taken.
- Typical system configuration includes:
  - mirrored copy of database on dual-ported or SAN disks in remote Data Center; and
  - backup or failover server that can take over for the primary server.
- Current examples in this category include:
  - YMG - IDX
  - ED L&H dictation system (for billing)

Level 3 includes critical applications or data for which the cost of keeping data in sync across primary and back-up servers may not permit Level 1 or Level 2 preparedness.

- Recovery Goal: These systems can be rapidly restored with most essential functions without full redundancy of production services. Service will be at least partially restored within four (4) hours, once the decision to failover is taken.
- Typical configuration:
  - includes multiple application servers distributed across two Data Centers;
  - does not require shared data; and
  - does not require servers large enough (CPU or Disk) to run full production loads, thereby reducing costs.
- Current ITS-Med examples in this category include:
  - Primary source PHI for approved research study
  - Primary source PHI for pre-research

Level 4 includes non-critical services for which hardware maintenance contracts and tape backups suffice for preparedness.

- Recovery Goal: These systems may be down for most or all of a day, or possibly more, until a failed system is repaired or alternate host system is identified. Additional application recovery may be required once the system is functional. Application recovery may involve the assistance of DBAs, developers and departmental interaction.
- No advance provision is made for relocation of the service in case of loss of a Data Center, though systems can be restored manually with preemption or sharing of computer systems at an alternate location.
- Current Yale examples in this category include:
    - Primary source PHI for approved research study
    - Primary source PHI for pre-research
    - Secondary source of PHI for operations or teaching
    - Secondary source of PHI for research/pre-research
    - Yale's internal ITS billing systems, faxing systems, software development and licensing systems.

Off-Site Tape Backup:

Off-site tape back ups are prepared and shipped to another state for storage for production applications which need to be recovered in the case of complete destruction of all on-campus equipment and tape back-ups. Off-site tape back-up is typically provided as an addition to a Level 1 or Level 2 service, though optional for all levels of preparedness, but additional costs may be required for configuration, especially if the system is not housed in a Data Center or if the amount of data is large.

NOTE: full backups of data and systems are maintained off-site without any supporting equipment. Restoration of service will require creating or leasing a machine room space, purchasing and delivering new computer equipment, installing and restoring operating systems, and then restoring data. Such restoration will typically require at least two weeks or more and the data restored will be several weeks to a month out of date. This level of back-up is provided as a deep fall-back behind a higher level of recovery and is expected to be used only in the direst of emergencies.