Installation and Maintenance of Health IT Systems

Unit 9b

Creating Fault Tolerant Systems, Backups, and Decommissioning

Backup Strategies

•The HIPAA Security Rule establishes the requirement to keep exact backup copies of all healthcare data in a manner that can be retrieved in a timely manner to restore documentation should data be corrupted or lost. Retention time for such data is generally accepted at lifetime plus one year.

Backup Strategies

- Requirements:
  - •Healthcare Data must be retained, on average, for the person's lifetime plus one year. Multiple versions of the data should exist to correct for errors or corruption
  - •A copy of the data must be protected at a location off-site geographically to protect it from natural disaster, fires, flooding and such.
  - •The data must be easily retrievable so data can be restored in a timely fashion
  - •The data must be protected through the use of encryption and stored in a secure location.

Backup Strategies

- **A Backup Window -** The time it takes to complete a given backup. This backup window is determined by both the amount of data that must be backed up and by the speed of the network infrastructure that handles the data.
- Issues arise when the backup window reaches peak operation cycles, potentially straining resources and slowing down the system.

Backup Strategies

- **Types of Backups:**
  - Full Backups: offer the ultimate in data protection, take longer to complete and lots of storage pass to keep multiple file versions
  - Incremental Backups provide a much faster method of backing up data than a full backup. Only the files that have changed since the last full or incremental backup are included.

Backup Strategies

- **Types of Backups:**
  - Differential backups offer a middle ground by backing up all the files that have changed since the last full backup.
  - Synthetic Full Backup. are used to compensate for a small or nonexistent backup window. In a synthetic full backup, information is taken from a full backup and the differential or incremental to create a new full backup tape.

Backup Strategies

- **Types of Backups:**
  - File system snapshots: Available through VM environments and later UNIX versions - Backups of the file system at several times during the day without needing large amounts of additional storage media and can create reliable backups of their systems without needing to shut down running applications for fear of data on disk changing while the backup is happening.

Backup Strategies

- **So, what are the primary options for backup?**
- **Direct backup**: This option has a tape drive, autoloader or library directly connected to each and every server so that each and every server can directly backup and restore data.
- **Network backup:** This has much larger tape drives, autoloaders or libraries connected to just one server. It backs up the data of all servers through that one backup server.
- **SAN backup:** This has some form of storage network to which all the servers and the backup device is connected so that, with appropriate arbitration, all the servers can backup to these shared devices.
- In reality, most people use a combination of the above.

Backup Strategies

- Backing up databases require extra considerations. Before embarking on a backup strategy for your EHR databases, consult with your EHR vendor to ensure your backup strategy is compatible with your database infrastructure

Creating a Plan for Decommissioning Systems and Data

- Active data is properly retained and inactive data is archived or disposed of in a secure manner consistent with the organizational needs.
  - Complete a full data audit and identify the data you are collecting and note redundancies
  - Determine the data owners and stakeholders.
  - Identify which data is inactive and which data is still active
  - Consider reporting/ retrieval requirements before decommissioning

Creating a Plan for Decommissioning Systems and Data

- Be sure your retention policies are well documented and are consistent with federal and state guidelines.
- Be sure to standardize on a single well navigatible archival system.
- Develop a plan and a schedule for Decommissioning.
- Ensure integrity of archived data and destruction of decommissioned data