Best Practices for File Shares or Shared Databases

What is a department file share or shared databases?

A department file share is access to data storage on a network-based system provided by an authorized University of Miami information resource such as Central Information Technology or a local, authorized Information Technology group. A database (db) may also be stored on a network file share and potentially accessible by multiple individuals. Within that file share/db, there may be various levels of privilege i.e. some individuals may be allowed to view, edit and even delete data. Other individuals may only be allowed to view data. Most importantly, unauthorized individuals should have NO access to the file share/db.

Important Issues

Will the file share/db contain individually identifiable information on patients, research subjects, students, donors and/or employees? Will the file share/db store other sensitive information (Human Resources information, confidential internal documents not for public disclosure or limited internal distribution such as plans, financial statements etc) that could potentially place the institution at risk if inappropriately disclosed or accessed?

If the answer is "Yes" then the following precautions and practices should be implemented.

- The file share/db is set up through central Information Technology or another authorized Information Technology group.
- The authorized IT group is responsible for securely configuring the file share/db as well as monitoring and timely application of all relevant security patches and anti-malware solutions. The dept and authorized IT group should agree on implementation and responsibility for adequate backup, restore, and disaster recovery procedures.
- Restrict the data elements stored to the minimum necessary to accomplish the business function. Particularly sensitive data elements include social security numbers, as well as HIV test results, mental health records, substance abuse, pregnancy results, etc. Do not store these elements unless there is a business need. Restrict access to only those who have a job-related need to see such sensitive information. Particularly if the file share/db should have this type of sensitive information, inter-act with your IT group to ensure adequate audit trails exist indicating "who and when" such information was accessed. In this regard, it is important to avoid use of generic user IDs. Every user should have a unique username.
- Again, access should be restricted to only members of that particular department/division/business unit who have a work-related need to access that file share/db.

No access should be allowed to unauthorized parties outside the department, division/business unit.

- Someone in your department should be responsible for maintaining an accurate list of who should have access, type of access (i.e. create, edit, delete or view only for example) and ensure that such access is reviewed regularly. That individual is also responsible for liaising with the authorized Information Technology group responsible for setup of the share/db.

- Such regular access review should include removing individuals who should no longer have rights to the share such as individuals who have transferred or who no longer have a job-related need for such access. The removal of such access should be done in a timely fashion. In some cases where risk analysis indicates an individual may be terminated or otherwise pose a risk to the information, then such access should be pro-actively removed.

For specific policies with regard to electronic protected health information (EPHI), please see http://privacyoffice.med.miami.edu/employees/policies-forms/security-policies-procedures (Medical domain username and password required).

For information security best practices, please see the CBL entitled "HIPAA Security Guide for IT Administrators and Business Unit Leaders" available in ULearn at http://ulearn.miami.edu.