Best Practices for SharePoint Sites with Sensitive Data

Does the site store individually identifiable information on patients, research subjects, students and/or employees? Does the site 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 SharePoint site should not be directly accessible from the internet, i.e. when outside of the University of Miami data network; the site should only be accessible after using an approved information technology encrypted remote access solution such as Information Technology's Citrix portal or an approved VPN solution.
- The SharePoint site should employ SSL technology so that all transmissions between the user and the site are encrypted.
- 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 SharePoint site.
- 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.
- The SharePoint database should only be housed on a secure information resource managed by an authorized IT group, with appropriate restrictions to prevent access by unauthorized users.
- The authorized IT group is responsible for securely configuring the SharePoint solution, monitoring and timely application of all relevant security patches and anti-malware solutions as well as implementation of 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. In this regard, it is important to avoid use of generic user IDs. Every user should have a unique username.

- Inter-act with your IT group to ensure adequate audit trails exist.

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

For General Information Technology Policies please see http://www.miami.edu/index.php/it/information_technology_policies_and_procedures/