Best Practices for Websites with Sensitive Data

Will the site store individually identifiable information on patients, research subjects, students, and/or employees? Will the site store other sensitive information 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.

- If the site is **only** to be accessed by University of Miami Medical personnel, the site should **not** be directly accessible from the Internet. When not on the medical campus, the site should only be accessible after using an approved remote access solution such as Citrix or an approved VPN.
- The site should employ SSL technology (similar to when you log on to a bank, the site begins with http**s**://, not http://) so that all transmissions between users and the site are encrypted.
- Access to the site and database should be granted only to persons with a legitimate business need.
- Such access should be granted through a documented process which should also include provisions for regular review, modification, and removal of access as appropriate (e.g., if a previously authorized user has transferred to another area, access must be removed in a timely fashion).
- Avoid storing Social Security numbers (SSN) if possible. If they must be stored in the back-end database, mask all but the last four digits if displayed on the site.
- Only grant access to the full SSN to those who have some business need.
- Do not store credit card numbers.
- Each individual user must have a unique username and require some authentication method such as a password or token.
- If password authentication is used, password requirements should meet minimum complexity requirements (a minimum of eight characters, a mix of alphabetic and numeric characters, etc.).
- The back-end database and website should only be stored 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 back-end database and the website as well as monitoring and the timely application of all relevant security patches and anti-malware solutions as well as implementation of adequate backup, restore, and disaster recovery procedures.
- All access to the site/database should be logged in an audit trail.

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.

In addition, here are some links to Security Tips that may be relevant:

- Protecting Sensitive Data is Everyone's Responsibility
- Encryption: The Key to Privacy and Security