Subject: How To Avoid A Data Breach

2007 was a year filled with data breaches, many involving well known national corporations. Make sure you're not making the headlines in 2008 by following security best practices.

Most breaches are the result of multiple failure points. Therefore, taking even some of the recommended measures can greatly reduce the risk of data breaches, or at least mitigate their impact if they do happen by enabling early detection and quick remediation.

Here are some basic tips that can help achieve this:

1. Be aware of information security policies and follow them: Employees are responsible for following School of Medicine information security policies. Please visit the following links to ensure you are up to date on current policies.

   School of Medicine and UNC Health Care System policies: [http://www.med.unc.edu/security/HIPAA/policies](http://www.med.unc.edu/security/HIPAA/policies)

2. Know your sensitive data and safeguard it: Determine where your sensitive data assets are. Control access to this data, preventing unauthorized viewing, copying, printing and backups. When reading about lost laptops with sensitive data (encrypted or not), one often wonders what such data was doing on a laptop in the first place – start there.

3. Apply the least privilege principle: Ensure users and applications have the minimum required access, especially with regards to sensitive data. Privileges should not be based on future needs but current ones. Regularly review existing privileges and revoke the ones that are no longer required.

4. Encrypt sensitive data: Use encryption coupled with authentication to protect sensitive data. Sensitive data transmitted over the network or stored on mobile devices such as laptops, PDA's and USB jump drives must be protected.

5. Monitor system activity: Monitoring and auditing gives you an additional and necessary layer of security. Systems and/or applications containing sensitive data should be monitored for unauthorized access.

6. Regularly check and harden configurations: Keep all system and application patches up to date and be sure to use strong passwords. A surprising number of breaches are due to weak passwords.

Be aware that you are responsible for protecting sensitive information. Unauthorized use or release of sensitive information may subject the violator to personal, civil, and/or criminal liability and legal penalties. Violations may constitute grounds for corrective action up to and including termination of employment or student status, loss of UNC Health Care and UNC School of Medicine privileges or contractual or affiliation rights in accordance with applicable UNC Health Care procedures.