October 2006

Identity Theft

In the last year alone, nearly 10 million Americans became victims of identity theft. It is the fastest growing crime in the United States. Identity theft occurs when a thief uses someone else’s personal information, such as a social security number (SSN) or bank account number and uses the victim’s identity in order to commit fraud, or to masquerade as another person. Identity thieves use stolen personal information to:

- open and max out new accounts or credit cards in an unsuspecting victim’s name
- access insurance benefits to obtain medical services and prescription drugs
- hide past criminal activity in pre-employment background screenings

It is imperative that we proactively protect our personal information as well as the personal information data of UNC School of Medicine as required by the NC Identity Theft Protection Act.

Tips to Safeguard Personal Information

1. **Protect your Social Security Number** – Don’t carry your SSN in your wallet, if your wallet is lost or stolen, the thief now has everything he needs to steal your identity (name and address from your driver’s license and credit/debit card numbers).
2. **Guard your mail** – Consider depositing mail containing personal information directly in a post office deposit box instead of your home mailbox if it is not secured. Also, shred and destroy any documents that contain SSN, bank account, credit card or any other personal identifying information before you trash it.
3. **Be careful on the Internet** – Never use your debit card on the Internet. The use of debit cards is not protected by the same federal laws that credit cards are and debit card transactions come directly out of your checking account which can mean a depleted checking account and lots of overdraft fees until you get it straightened out… which could be awhile…well, you get the picture. When shopping online, deal only with reputable companies on secure sites. Install firewalls, virus protection and anti-spyware on your computer and keep them up to date. If using wireless, encrypt your wireless connection.
4. **Clean, Clean, Clean** - Be sure to properly sanitize your computer hard drive, cell phone or Personal Digital Assistant (PDA) before you sell it, give it away or otherwise dispose of it to ensure all personal information has been permanently erased.
5. **No Phishing, Don’t take the bait!** - Phishers attempt to fraudulently acquire personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Phishing is typically carried out using email or an instant message. Misspelled URLs or the use of subdomains are common tricks used by phishers. Another trick is to make the anchor text for a link appear to be a valid URL when the link actually goes to the phishers' site.
6. **Opt-out** – Call 1-888-5OPT-OUT or visit OptOutPrescreen.com to remove your name from pre-approved credit mailing lists. You will then receive a form in the mail to sign and return. You have the option of removing your name from the list for five years or permanently.
7. **Home ≠ Secure** – Just because personal information is in your home does not mean it is safe. For example, if you employ outside help such as repairmen or housekeepers avoid leaving your mail, checkbook, cell phone, PDA or anything with personal information lying around the house where it could be stolen.

8. **Never provide personal information to telephone solicitors.**

9. **Monitor credit reports** – Check credit reports for anything suspicious such as accounts opened in your name that you don’t recognize. You’re entitled to receive one free credit report from the big three credit bureaus (Experian, TransUnion and Equifax) every 12 months. Visit [www.annualcreditreport.com](http://www.annualcreditreport.com) for more information.

10. **Safe banking** – Check bank statements as soon as they arrive to check for any fraudulent charges. Report any lost or stolen credit/debit cards immediately to the issuing bank. If you use online banking, use a strong password for authentication.

**Your responsibility under the NC Identity Theft Protection Act**

In an effort to raise awareness of our compliance requirements, we would like to remind you of your **responsibility** to protect the personal identifying information (PII) data of UNC School of Medicine (SOM) as defined in the North Carolina Identity Theft Protection Act. During the 2005 legislative session, the North Carolina General Assembly enacted the North Carolina Identity Theft Protection Act which imposed new restrictions upon the collection and segregation of SSNs and upon the disclosure and security of SSNs and other personal identifying information. Please review the law in its entirety and ensure that you meet compliance requirements.

**NC Identity Theft Protection Act**

In addition, on October 1, 2006, an amendment to the North Carolina Identity Theft Protection Act became effective which requires the UNC SOM and other State agencies to notify individuals in the event of any incident of unauthorized access to, acquisition of, or breach of records or data containing personal information where

- the illegal use of the personal information has occurred or,
- the illegal use of the personal information is reasonably likely to occur or,
- it creates a material risk of harm to the individuals

Please contact the [School of Medicine Information Privacy and Security staff](#) to report an incident or for any questions regarding the Identity Theft topic.