

# TOP TEN DATA SECURITY SAFEGUARDS

## HIPAA and Data Security

Individuals who create, access, transmit, or receive electronic protected health information (ePHI) need to understand and implement the following ten safeguards, which ensure that computers meet basic security requirements. While you are responsible for the security of University data, your University IT support provider can assist you with any technical requirements.

1. ***Read and understand the University policies on privacy and data security.***

HIPAA policies apply to all individuals who are a part of the University's health care components and who create, access, transmit, or receive ePHI. These policies can be found online at [www.privacysecurity.umn.edu](http://www.privacysecurity.umn.edu).

2. ***Understand what you need to do and what you need help with.***

Recommendations for safe computing practices can be found at [www.safecomputing.umn.edu](http://www.safecomputing.umn.edu). If your department is interested in receiving University assistance to develop appropriate technical support models, call 1-HELP (612.301.4357).

3. ***Know what incidents to report and where to report them.***

If you believe private data has been compromised in a network or computer incident, you must notify the Office of Information Technology by sending an e-mail to [abuse@umn.edu](mailto:abuse@umn.edu). Inform your immediate supervisor if any physical facility or device is damaged.

4. ***Recognize when your computer may be compromised.***

If you notice your computer exhibiting unusual behavior, run the AntiVirus software to check if it is updating properly and when it was last updated (should be within last seven days). If a virus is found or you need assistance, contact your designated technical support office or the central help desk at 1-HELP (612.301.4357).

5. ***Implement password security recommendations.***

The Office of Information Technology has developed a password guide for selecting strong passwords. Basic guidelines include:

- Choose an obscure password, using a minimum of 8 characters and a combination of numbers, special characters, and mixed case letters.
- Change your passwords every 90-360 days.
- Keep your passwords private.

6. ***Ensure computing devices are physically secured, including laptops.***

The Securing Private Data Standard outlines the requirements for physically securing computing devices at the University. Basic guidelines include:

- Lock your office when you leave for extended periods of time to restrict physical access to your computer.
- Require a password to start-up and return from a screen saver to protect information stored on your hard drive and displayed on your screen.
- Personal computing devices, such as laptops and PDAs, may contain confidential, protected health information and may connect to the University network. Do not leave them unattended, or lock them in secure locations.
- A laptop security lock is another way to further deter theft. Locks may be purchased through Techmart or University of Minnesota Bookstores.

# TOP TEN DATA SECURITY SAFEGUARDS

## HIPAA and Data Security *continued*

### 7. *Follow safe computing practices when surfing the Web and/or using e-mail.*

When cruising and using the Internet, phishing, spyware, peer-to-peer software (e.g. BitTorrent, Kazaa), and identity theft are all potential hazards. Learn more about these topics and what you can do to protect your computer and yourself at [www.safecomputing.umn.edu](http://www.safecomputing.umn.edu) and click on “safe computing topics.”

In your daily e-mail transactions, the following precautions will help your e-mail remain secure:

- Never open an e-mail attachment from an unknown source. Even if you know the sender, if the subject line appears fishy or you are not expecting an attachment, you may want to call the sender to verify the attachment before opening.
- Enabling a Secure Sockets Layer (SSL) protocol is **mandatory** to send e-mail through a University-provided account (An SSL encrypts both the password and the e-mail message). Visit [www.umn.edu/securelt/](http://www.umn.edu/securelt/) for more information and setup assistance.
- Do not use non-University provided e-mail accounts to send University-related information, as they are not appropriate or secure. **Only xxx@umn.edu addresses are supported by OIT and centrally administered e-mail servers.**
- Check all addresses carefully before hitting “Send” to prevent transmission of sensitive data to the wrong recipient(s). When appropriate, distinguish between using “Reply” and “Reply All.” When sending e-mails to large groups of people, use “Bcc:” to prevent the possible spread of viruses.

### 8. *Incorporate data security principles into your overall data management plan.*

- Secure file sharing – file sharing should be disabled to block access to files on your local hard drive. If you need to share files, use a secure file server maintained by your IT provider, or copy the information to portable media or a CD. If you need to share a printer, connect directly to a network.
- Backup data files – verify that data stored on a network server is automatically backed up on a nightly basis. Data that is not stored on a network server must be backed up on removable media and stored in a secure location.
- Destroy and dispose of data/data storage devices properly – solely deleting files does not completely remove the data from your computer. If you have a device containing ePHI that requires disposal, reuse or donation (including PC hard drives, CDs, floppy disks, USB keys, or PDAs), follow deletion instructions at [www.umn.edu/oit/security/assureddelete.html](http://www.umn.edu/oit/security/assureddelete.html) or contact University Computer Services to arrange for free computer recycling pick-up.

### 9. *Keep your operating systems and AntiVirus software up-to-date.*

It is University policy that all computers connected to the University network have working AntiVirus software and critical security patches installed and up-to-date. Contact your IT provider to set up your computer to receive automatic updates and patches to deliver an extra layer of security.

### 10. *Apply the Securing Private Data Standard to ALL locations and mobile devices.*

Computing devices used on and off campus must comply with all University-related HIPAA policies. Implement the same procedures at home and on your PDAs as you do at work to keep private information safe from unauthorized access. Private University data should **only** be stored on University-owned equipment and hardware.