

# Information Security Awareness Training

How to protect electronic information at  
work and at home

Mount Auburn Hospital

## This program covers the following:

- Purpose for security training
- Potential threats
- Protecting data at work
- Protecting data at home
- Mobile device security
- Reporting security breaches
- Mount Auburn Policies

Mount Auburn Hospital

# Purpose for security training

## Protected Health Information

Protected Health Information (PHI) is information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse relating to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Protected Health Information includes, but is not limited to:

- Patient demographic data (e.g., address, date of birth, date of death, sex, e-mail/Web address)
- Medical record number, account number, or SSN
- Dates of service (e.g., date of admission, discharge)
- Medical records, reports, test results, appointment dates



Mount Auburn Hospital

# Purpose for security training

## Electronic Protected Health Information

Electronic Protected Health Information (ePHI) is protected health information that is computer based (e.g., created, received, stored or maintained, processed and/or transmitted in electronic media). Electronic media includes:



- Computers
- Laptops
- Disks
- Memory sticks
- PDAs
- Servers
- Networks
- Dial-mode
- e-Mail
- Websites

Mount Auburn Hospital

# Purpose for security training

## HIPAA Security Rule

HIPAA Security regulations were effective April 20, 2005

They compliment Privacy regulations published in 2003

Security regulations apply to electronic protected health information (ePHI)



Regulations require workforce security awareness training

They require Mount Auburn to protect the confidentiality, integrity, and availability of ePHI against reasonably anticipated threats such as hackers, viruses, and disasters

Mount Auburn Hospital

# Purpose for security training

## Who is responsible for computer security?



Every member of Mount Auburn's workforce is responsible for protecting ePHI.

Members of the workforce are expected to act responsibly and ethically when accessing Mount Auburn's electronic data and technology resources

Compliance with hospital policies and local, state, and federal law is required

The security of a system is only as good as its weakest link. If even one person does not pay attention to security, the security of the whole system is compromised.



Mount Auburn Hospital

# Purpose for security training

## Why do I need to learn about security?

Good Security Standards follow the "90/10" Rule:

- 10% of security safeguards are technical
- 90% of security safeguards rely on the computer user (YOU!) to adhere to good computing practices



Example: The lock on the door is the 10%.  
**Remembering** to lock, checking to see if it is closed, ensuring others do not prop the door open, keeping control of keys is the 90%.

10% security is worthless without YOU!

Mount Auburn Hospital

# Purpose for security training

## What could happen?

Poor security can place ePHI at risk. Some examples are:

- Your laptop containing ePHI is stolen
- A hacker breaks into an application and alters ePHI data
- A departmental server is destroyed by flood. No backup copy of the data was made



To be HIPAA-compliant, all covered entities must protect the Integrity, confidentiality and availability of ePHI and provide on-going security awareness training for their workforce.

Any insecure system can put the hospital at risk.

Mount Auburn Hospital

# Purpose for security training

## What else could happen?

- You could be held liable in court for violations you commit. Civil penalties from \$100 up to \$25,000 per year for each violation. Criminal penalties range from \$50,000 up to \$250,000 in fines and from 1 to 10 years in jail.



- Increased chance of lawsuits for Mount Auburn due to hacker-inflicted damages
- Your identity could be stolen
- Mount Auburn could receive negative press coverage for a HIPAA security incident.

Mount Auburn Hospital

# Potential threats

- Malicious Software (viruses, trojans, worms, spyware, or other)
- Threats from within Mount Auburn
- Instant Messaging
- Peer-to-Peer File Sharing
- Identity Theft
- Social Engineering

Mount Auburn Hospital

# Potential threats

- Some applications such as Instant Messaging (IM), Peer-to-Peer (P2P) file sharing, pose serious security risks. You should consider anything typed into IM or transferred through P2P to be visible to the entire internet.
- When used in conjunction with Internet sites outside of Mount Auburn, they can cause undesirable and damaging consequences
- For example, you are most likely to encounter malware browsing an external website
- When accessing external websites, members of Mount Auburn's workforce must be especially cautious

Mount Auburn Hospital

# Potential threats

## Malicious software

Malicious software (also known as malware) is a serious threat. These are programs that can "infect" other programs, damage hard drives, erase critical information, take critical systems off-line, and forward your data to external sites without your knowledge.

Malware includes:

- Viruses
- Worms
- Trojan Horse programs
- Spyware
- Programs which accidentally harm any system or data



Mount Auburn Hospital

# Potential threats

## Signs of malware

- Unusual items appearing on the screen (graphics, odd messages, or system error messages).
- Corrupted or inaccessible program files, hard disks, or diskettes.
- Programs taking longer to start up, running more slowly than usual, or not running at all.
- Increased number of pop-up advertisements
- Changed settings that can't be changed back to the way they were
- Web browser contains additional components that you don't remember downloading



Mount Auburn Hospital

# Potential threats

## How to protect against malware

Anti-virus software running on Mount Auburn's managed workstations protects against most malware.

Should you suspect that your computer is infected, take immediate action:

- Close all of your files and programs
- Document what symptoms were observed
- Shut down your system
- Contact the IS Help Desk at X5600



Mount Auburn Hospital



# Potential threats

## Instant Messaging



Instant messaging is the popular method of typing online conversations in real time.

Risks of Externally Hosted Instant Messaging:

- No virus protection
- A separate "exit" action is needed to stop it
- Hijacking and impersonation
- Malicious code
- Unauthorized access
- Poor password security
- Broadcasts the computer's presence online even if the interface is closed
- The data is sent to an external host before going to the intended recipient



Due to these characteristics of Instant Messaging, it poses serious security risks.

Mount Auburn Hospital

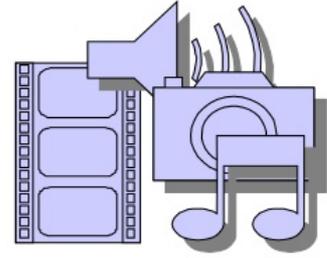
# Potential threats

## P2P file sharing

P2P (Peer-to-Peer) means file sharing between users on the Internet. Examples are Gnutella, KaZaA, Napster, Morpheus, eDonkey, BitTorrent and BearShare.

P2P file sharing is inherently insecure and lives on the fringes of legality. Badly-coded clients, viruses and Trojan Horses and potential lawsuits are just some of the many threats that users must face when they venture into the untamed wilderness of the P2P world. Some threats are:

- Some P2P programs share everything on your computer with anyone by default.
- Some P2P programs themselves contain "spyware".
- Much of the P2P activity is automatic, and its use is unmonitored.
- Creating multiple copies of a copyrighted work, music or videos and sharing them is illegal.
- Computers running P2P programs can be used to spread malware, share private documents, or use your file server for store-and-forward.
- Various types of illegal files can be downloaded and re-shared over these P2P networks by mistake.



Mount Auburn Hospital

# Potential threats

## Damage from within

Survey after survey has shown that most damage is done by insiders -- people with authorized access to a computer network. Many insiders have the access and knowledge to compromise or shut down entire systems and networks.

You are expected to report information that comes to your attention and that raises potential concerns about computer security. Call the IS Help Desk at X 5600.



Mount Auburn Hospital

# Potential threats

## Identity theft



Identity theft is the unauthorized collection and use of your personal information for criminal purposes. This information can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, and even secure employment. If this happens, you could be left with the bills, charges, bad checks, and taxes.

### Signs of Identity Theft:

- Unexplained bank statements, charges on phone, credit cards or other consumer accounts
- Being denied a loan you qualify for
- Unexplained changes in your bank access codes
- Missing credit card bills or other mail
- Unusual calls regarding your personal or financial information



Further reading on how to avoid identity theft and what to do as a victim

- <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>
- <http://www.consumer.gov/idtheft/>

Mount Auburn Hospital

# Potential threats

## Social engineering

Social engineering is the practice of obtaining confidential information by manipulation of legitimate users. A social engineer will commonly use the telephone or Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.

**Social engineers exploit the natural tendency of a person to trust another's word, rather than exploiting computer security holes.**



Mount Auburn Hospital

# Potential threats

## Social engineering

Signs of social engineering attacks to recognize:

- Refusal to give contact information
- Rushing
- Name-dropping
- Intimidation
- Small mistakes (misspellings, misnomers, odd questions)
- Requesting forbidden information



Mount Auburn Hospital

# Potential threats

## Avoid being a victim

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information.
- If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization unless you are certain of a person's authority to have the information.



- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a web site connected to the request.

Mount Auburn Hospital

# Protecting data at work

The best way to secure your system is to use a managed workstation. IS Support automatically updates anti-virus and patches on managed systems. Here are some additional tips to protect your data.

1. Use strong passwords
2. Pay attention to your computer's security
3. Use email safely
4. Use the Internet responsibly and securely
5. Dispose of media properly
6. Physically secure devices containing ePHI



Mount Auburn Hospital

# Protecting data at work

## 1. Use strong passwords

Why make it easy for hackers by using weak or simple passwords? Never devise passwords based on your real name, username or company name, or use easily guessed numbers such as 1234. Change your password frequently, and use passwords that are eight letters or more in length with lower and upper case letters, numbers and symbols.

## 2. Pay attention to your computer's security

Lock your computer with a password-protected screen saver before leaving your desk unattended. If you use a laptop, be sure it is secured with a cable or locked office. Before you go home, log off the network. Manage your data in a manner that reflects its sensitivity.



Mount Auburn Hospital

# Protecting data at work

## 3. Use email safely

The first rule of thumb is never open suspicious or unsolicited attachments. Avoid responding to spam, especially links that claim you will be removed from the spammer's mailing list. The second rule of thumb is never provide credit card numbers, passwords or personal information in response to email messages. Finally, check regularly for email updates and be sure to install anti-virus software if you manage your own workstation.



## 4. Use the Internet responsibly and securely

- Don't post sensitive company information or company-related comments on message boards, in chat rooms or anywhere else on the Internet.
- Don't visit inappropriate Internet sites.
- Don't download non-business-related files to Mount Auburn's network or to your Mount Auburn-issued computer. Downloads from the Internet are often virus hazards.

## 5. Dispose of media properly

Before electronic media is disposed of, appropriate care must be taken to ensure that no unauthorized person can access data by ordinary means. Electronic media such as floppy disks, rewritable CD-ROMS, zip disks, videotapes, and audiotapes should be erased if the media type allows it or destroyed if erasure is not possible.

Mount Auburn Hospital

# Protecting data at work

## 7. Physically secure devices containing ePHI

One of the easiest ways to pilfer ePHI is to gain physical access to a computer.

- Unless you are using a public workstation, use a password protected screensaver to lock your workstation when not in use.
- Secure work areas containing ePHI when unoccupied
- Password protect all mobile devices such as laptops, Blackberries and PDA's



Mount Auburn Hospital

# Protecting data at home

If you use your home computer to access applications at Mount Auburn and your home computer is not properly protected, you can put Mount Auburn's systems at risk.

1. Always use anti-virus software
2. Apply patches regularly
3. Perform regular backups
4. Shutdown your computer when not in use
5. Work securely from home
6. Protect against Malware
7. Protect yourself from Spyware
8. Make wireless networks secure



Mount Auburn Hospital

# Protecting data at home

## 1. **Always use anti-virus software**

Install anti-virus software and update it regularly. This software scans incoming emails for virus signatures and, if a virus is found, deletes or quarantines it. It's critical to update this software regularly with new definitions because there are hundreds of new viruses each month.

## 2. **Apply patches regularly**

Download computer updates regularly. If you use a Microsoft operating system, older computer systems, such as Windows 98 or 95, should be discarded in favour of Windows XP Professional, which is more robust and secure. Security updates are downloadable at [update.microsoft.com](http://update.microsoft.com). Sign up for Microsoft Security Update, a free email alert service that tells you when to take action and what software to download.

## 3. **Perform regular backups**

Ensure all your data is backed up on a regular basis. Critical data should be backed up at least at the end of every day. The backup copy should be stored at another site for especially important data. Should your home office be subject to fire damage even backup data could be lost.

## 4. **Shutdown your computer when not in use**

Any computer connected to the Internet is a target for unauthorized attempts to try to access your system. The risk is increased for users with permanent connections, (such as ADSL, cable modems and ethernet) because attached computers are permanently on the Internet while switched on.

Mount Auburn Hospital

# Protecting data at home



## 5. **Work Securely from home**

Guard company information at home as you would at the office. When working from home, guard your laptop, CDs, diskettes and papers that contain company information. Shred or destroy items that contain company information before discarding them.

## 6. **Protect against Malware**

- Use anti-virus software to scan for viruses on ALL new software prior to loading on your system (even "off-the-shelf" software)
- Don't use pirated, hacked, or otherwise illegal copies of programs
- Do NOT run programs obtained from the Internet without first scanning for viruses
- Secure physical access to your computer
- Back-up your files frequently, so you can restore damaged information



Mount Auburn Hospital

# Protecting data at home

## 7. Protect yourself from Spyware

- Don't click on links within pop-up windows. Click on the "X" icon in the titlebar instead of a "close" link within the window.
- Choose "no" or "cancel" when asked unexpected questions.
- Be wary of free downloadable software. Don't download programs from sites you don't trust, and realize that you may be exposing your computer to spyware by downloading some of these programs.
- Don't follow email links claiming to offer anti-spyware software. Like email viruses, the links may serve the opposite purpose and actually install the spyware it claims to be eliminating.



## 8. Make wireless networks secure

Because wireless networks, known as 802.11 or Wi-Fi, use radio links instead of cables to connect computers, they are more vulnerable to hackers. Easy-to-buy tools allow hackers to listen in or transmit data on your network. Several encryption technologies, such as Wi-Fi Protected Access, are available to prevent such eavesdropping.

Mount Auburn Hospital

# Protecting data at home

Mount Auburn IS does not provide support for home computers. If you need additional assistance with your home computer, possible resources include those listed below.

- <http://www.geeksquad.com/main.asp>
- <http://www.mcafee.com/us/>
- [http://www.cert.org/tech\\_tips/home\\_networks.html](http://www.cert.org/tech_tips/home_networks.html)
- <http://support.microsoft.com/>

These resources are provided as suggestions only. BIDMC does not endorse them or accept responsibility for their work.

Mount Auburn Hospital

# Mobile device security

Are you carrying hundreds of millions of dollars? You just might be. It could be in your laptop or PDA. Any items that contain confidential information could be of tremendous value to thieves and other saboteurs.

Keep the following security essentials in mind at the office and on the road:

- Lock your laptop to a fixed piece of furniture using a metal laptop cable if you leave it unattended. Locking devices are available through office-supply companies.
- Guard laptops, PDAs, CDs, cell phones and papers at all times.
- Implement a password-protected screen lock.
- Don't store sensitive information, such as usernames, passwords, social security numbers, bank account numbers, or credit card numbers on the device.
- Keep data backed up on a PC or server in case your mobile device is gone forever.
- Store important data separately. There are many forms of storage media, including floppy disks, zip disks, CDs, DVDs, and removable flash drives (also known as USB drives or thumb drives). By saving your data on removable media and keeping it in a different location, you can protect your data even if your laptop is stolen.



Mount Auburn Hospital

# Reporting security breaches

What is a security incident?

Anytime you suspect a Mount Auburn computer or ePHI has been compromised, whether that involves theft, hacking, a vicious virus, unauthorized use of IT technology or you witness an inappropriate or offensive use of email or the Web, you should report the incident, or seek help and advice from IS Support.

Why should I report a security incident?

If your system has been infected or any data has been lost, IS Support resources can help you clean up your system. Furthermore, as a user of the network, you should be aware of your rights and responsibilities.

How do I report a security incident?

Report security violations and computing problems to the IS Help Desk at 617-499-5600 (X 5600).



Where can you obtain more information?

You should be familiar with the contents of these Mount Auburn policies.

Mount Auburn Hospital

# DEVICE USE (B-14)

**Guidelines for usage include:**

- **Storage and access of sexually explicit, racist, and hate oriented materials is prohibited.**
- **Illegal and/or fraudulent practices are prohibited.**
- **Installation of devices and software for non-business related activities is prohibited. This includes, but is not limited to, gaming devices/software, instant messaging software, wallpaper and screen savers not installed by Information Systems.**
- **Attachment of devices and/or software to allow external access to the Hospital network not explicitly approved by Information Systems in accordance with policy "Computer Network Perimeter Security" is prohibited.**
- **Installation of software not properly licensed, if required, is prohibited.**
- **Deactivation of support tools, including antivirus software, systems security, and monitoring tools.**

Mount Auburn Hospital

# Security Management Process (B-103)

**Policy Summary: Mount Auburn Hospital must ensure the confidentiality, integrity and availability of its information systems containing EPHI by implementing appropriate and reasonable policies, procedures and controls to prevent, detect, contain, and correct security violations. Mount Auburn Hospital's security management program must be based on formal and regular processes for risk analysis and management, sanction policies for non-compliance, and information system activity review.**

**All Mount Auburn Hospital workforce members are responsible for appropriately protecting EPHI maintained on Mount Auburn Hospital information systems. Mount Auburn Hospital management is responsible for ensuring the confidentiality, integrity and availability of all EPHI maintained on Mount Auburn Hospital information systems.**

Mount Auburn Hospital

# The End

Thank you for taking the time to complete this training. After you complete the quiz, if you have any comments or recommendations regarding this material or IT security in general, please forward them to [rtodd@carergroup.harvard.edu](mailto:rtodd@carergroup.harvard.edu).

Annually, you will be required to complete HIPAA refresher training that will include material on privacy, confidentiality and security.

Mount Auburn IT Staff

Mount Auburn Hospital

# Security Awareness Training

- This concludes our IS Security Awareness Training module. Please complete the certification process by taking the short quiz at the link on intranet or the hardcopy version supplied by your supervisor.

Mount Auburn Hospital