

Procedure 1610 PR.01 Systems and Network Security

Revision Date: 04/20/05

Overview.....	1
Special provisions for systems with ePHI	1
Specific procedures for Computing Device Security	1
1. Understand and comply with Yale University's IT and HIPAA policies.....	2
2. Know your IT support providers and their role in information security.....	2
3. Report IT security incidents.....	2
4. Recognize when your computer may be compromised.....	2
5. Implement Yale password security recommendations.....	2
6. Ensure computing devices are physically secured.....	2
7. Avoid activities that may compromise security.....	3
8. Configure and use email securely.....	4
9. Use up-to-date protections against malicious software.....	4
10. Use secure <i>file transfer</i> and configure <i>file sharing</i> securely.....	4
11. Keep your operating system and application software up-to-date.....	4
12. Backup your data files and directories.....	4
13. Destroy data and dispose of computers properly.....	5
14. Privacy and security requirements apply to ALL locations, including your home.....	5
15. Implement additional security requirements for portable or handheld, and wireless devices.....	5

Overview

This document provides general procedures for securing a computing device used for Yale business whether located on Yale owned premises or elsewhere. The procedures are strongly recommended for all computing devices whether connected to a network or not. For some uses, the procedures are mandatory (see below). The methods actually used to implement the procedures as well as additional, more stringent, procedures will vary with specific location and will be detailed by local support providers. In particular, please see policy and practice information specific to the schools of Medicine and Nursing as documented at the [ITS-Med office of Information Security](http://its.med.yale.edu/security/) web site. (<http://its.med.yale.edu/security/>)

Special provisions for systems with ePHI

The IT security procedures described herein are mandatory for network connected computing devices that create, access, transmit or receive electronic Protected Health Information (ePHI). These requirements apply specifically to the University's Covered Components (the Group Health Plan Component; and the Covered Health Care Component: YSM, YSN, YUHS and Department of Psychology clinics), designated as such for purposes of complying with HIPAA regulations. Contact one of the following support units for details:

- ITS-Central (Group Health Plan Component & Department of Psychology)
- ITS-Med (School of Medicine)
- IT-YSN (School of Nursing)
- IT-YUHS (Yale University Health Services)

Specific procedures for Computing Device Security

Note that the following 15 procedures apply to every individual who uses a computing device for University business. However, procedures 8-15 are technical in nature and may be delegated to a responsible IT support professional.

Some of the technical provisions may be impracticable for computers not connected to a network. However, even in that situation, the procedures should be implemented to the extent possible, especially if there is any possibility that the device may be connected to a network in the future.

1. Understand and comply with Yale University's IT and HIPAA policies.

All individuals who use Yale University computing and networking facilities are required to read and abide by Yale's Information Technology (IT) Appropriate Use Policy 1607 and other relevant policies.

The Information Technology Acceptable Use Policy (ITAUP) is the overarching policy governing the use of computing technology at the university. Among critical provisions, the ITAUP prohibits sharing of accounts and passwords unless specifically authorized. The ITAUP also prohibits obtaining unauthorized access to IT systems or permitting others to do so.

HIPAA IT Security policies apply to all individuals who are a member of the University's Covered Components and who create, access, transmit or receive ePHI.

Links: [Policy 1607 ITAUP](#)|| [HIPAA](#)

2. Know your IT support providers and their role in information security.

All faculty, staff, and students on campus have access to IT support staff. Know who they are and the services they provide before you need them. IT support staff (Help Desks and Technicians) are trained in routine information security support and Yale's IT web sites have comprehensive information on security.

Yale has assigned IT Security Officials who are responsible for oversight of the IT security policies and procedures and who can be contacted regarding possible IT security incidents. If you have any questions about general IT security information or about the IT security component of the HIPAA regulations, you should contact one of the Information Security Office staff.

Links: [DSP](#) || [ITS](#) || [ITS-Med](#) || [YSN](#) || [YUHS](#)

3. Report IT security incidents.

If you believe sensitive data may have been compromised, you must notify Information Security at either the central ([ISO](#)) or Medical School office ([ISO-Med](#)). You must also promptly notify your immediate supervisor and administrative unit head if any Yale University physical or information asset is damaged.

4. Recognize when your computer may be compromised.

Information security compromise of a system often results in a dramatic change in your own computer's performance that can be observed by the user. If you notice your personal computer rebooting by itself, suddenly slowing dramatically or exhibiting any unusual behavior, seek assistance from your IT support provider to determine if your computer may have been compromised

5. Implement Yale password security recommendations.

Choose a password that is difficult to guess: use between 6-8 characters, vary the case of letters and intermix letters, numbers, and punctuation if the system allows. Advice on selecting good passwords is available at www.yale.edu/ppdev/Guides/its/passwords.pdf.

- Keep your passwords private. Do not share them with *anyone* including your supervisor, family, co-workers, or IT support provider.
- Change any weak default passwords for local applications (e.g., Meeting Maker, Tivoli backup, BMS etc.) , so that they employ strong passwords
- Change your passwords periodically. A list of [password change utilities](#) is available on-line (including changing NetID passwords).
- If your password is discovered or you determine that someone is using it to access your account, contact Information Security at either office: [ISO](#) || [ISO-Med](#).

6. Ensure computing devices are physically secured.

Information displayed on your computer screen can be viewed casually by anyone within view. If you leave the area and sensitive data is visible on the screen of your computer, such information can readily be viewed by anyone nearby who chooses to look. Use a screensaver that hides the screen after 10 minutes of inactivity and requires a password to restore the display. When you are away from your

computer for extended periods, secure the space, if possible, since physical access to your computer allows other methods of access to your data (e.g. inserting a disk or CD with tools for “hacking”).

Consider whether sensitive information displayed on your desktop can be seen by others; make sure to position your computer screen out of view by anyone who has no need to view it. In public areas use privacy screens to hide sensitive information or use a locking screen saver to protect your computer when you are away from your desk. Automatic time-outs for computer sessions will help protect confidential information.

Never leave portable computing devices unattended and unlocked. Make sure the access to data on the device and the access to the device itself is limited. Portable devices such as PDAs, USB memory sticks and laptops are all especially vulnerable in transit. They can be lost or stolen on your way to or from Yale. Good protective measures include putting them in a locked briefcase or cabinet or using password protection or encryption.

The physical safeguards of the HIPAA Security Rule include specifying the exact geographical locations of ePHI in local departments, data centers, or on non-Yale property and implementing steps to ensure that individuals who have no need to access ePHI systems cannot do so. These protective measures cover all types of computing mediums such as data servers, desktop PCs, personal digital assistants (PDAs), USB devices, CDs, DVDs, Diskettes, memory sticks, flash cards, smart phones and any future medium used to store ePHI -- whether these computing mediums are located on Yale property or not.

If you see someone in your area and you are uncertain if they have legitimate business to be there, either engage them to provide appropriate help or contact the Yale Security Department.

Yale business locations outside New Haven must abide by appropriate security policies which meet the same standards.

See Policy [5111](#) Physical Security policy for additional details.

7. Avoid activities that may compromise security.

When using a web browser, be aware that the less you know about a site, the greater the dangers. For secure sites (sites whose address begins with “https” instead of “http”) examine the web address carefully to assure it is as expected. Always examine embedded links to see that they point to an address consistent with what you expect. If any question, type in the expected address manually rather than follow a programmed link.

Be very careful when installing any program on your computer. Many programs that can be downloaded from the Web automatically install spyware or other malicious software (“malware”) on your computer. Only download software from Yale servers or well-known software vendors (Apple/Microsoft/Netscape/Symantec). Use Yale’s standard electronic procurement links to access University-approved vendors. If a link does not exist to a vendor from a Yale site, check with the [Procurement Office](#) before making an alternate Web-based purchase.

Electronic messages (e.g., email) or transactions containing sensitive or proprietary information about the University, faculty, staff, students, patients or others must be safeguarded to ensure the confidentiality and security of such information. For more information: [ITS](#) || [ITS-Med](#)

The following widely-used Internet programs represent significant potential security risks and are prohibited on any Yale computers with confidential or ePHI data:

- Peer-to-peer file sharing services such as Gnutella, Kazaa, Bittorrent, eDonkey and the like unless a particular application is specifically approved for Yale business (as identified in an official Yale software download site) or an exception is granted via the ISO; many of these programs open a direct route to your computer which may be used by others for direct access and many of these programs may directly share files on your computer to the Internet;
- Video games, particularly any that might be downloaded from the Internet;
- Shareware utilities such as so called “Internet Accelerators.”

In addition to the concerns listed above, many of these programs are packaged for download with spyware or dangerous malware which may seriously compromise your computers’ security.

Some programs, such as Instant Messenger, WeatherBug and other useful and apparently benign software can also pose risks. As with peer-to-peer, Yale prohibits the use of these programs on machines

containing confidential information or ePHI unless specifically approved (as identified on an official Yale software download site) or an exception is granted via the ISO.

In general, you should seek ISO advice if you wish to run any program on a machine containing confidential data or ePHI which has not already been approved for such use at Yale.

Link: [ITS-Med](#)

8. Configure and use email securely.

Use only official University email systems for Yale business related email.

When using email, don't open attachments unless you are expecting them and check any embedded links within emails to verify they point to the expected location.

The single greatest cause of email exposure of sensitive data is sending email to the wrong recipient so carefully check all addresses before sending.

Configure your email software to use secure protocols (e.g., "TLS/SSL" for both sending and reading email using email clients such as Eudora, Thunderbird and Outlook – your IT support provider can configure this option) at all the locations from which you use email. Use SPAM and virus filters provided by University email servers:

Links: [ITS](#) || [ITS-Med](#)

For email transmission of Protected Health Information, implement and use only the procedures permitted in [5123 PR1](#): Electronic Communication of ePHI.

9. Use up-to-date protections against malicious software.

Install the University provided anti-virus and anti-spyware tools and keep them up to date. Symantec AntiVirus and anti-spyware software is available at no fee to all Yale faculty, staff and students.

Links: [ITS](#) || [ITS-Med](#)

10. Use secure file transfer and configure file sharing securely.

File Sharing means you are allowing access to drives/directories/files on your local hard drive.. File sharing should be disabled or restricted and secured.

Options for secure file transfer include:

ITS-Med provides a [Yale File Transfer Facility](#)

[Pantheon](#) file transfer options

Secure file transfer clients for Windows, Macintosh and Linux are available

Any "electronic data interchange" between Yale and vendors must be only via links with equal or better security to that of a Virtual Private Network (VPN) connection.

Links: [ITS](#) || [ITS-Med](#)

11. Keep your operating system and application software up-to-date.

Keeping current with updates and patches provides an added layer of security. Your IT support organization can provide *automated* solutions to keep software up-to-date.

NOTE: *Consult your local IT support person if you are concerned that any update might affect the ability to access a University application (i.e., Oracle, IDX).*

Links: [ITS](#) || [ITS](#)- security guidelines

12. Backup your data files and directories.

So that if something happens to your computer, files and data will be recoverable. Centrally managed back-up services are available.

Links: [ITS](#) || [ITS-Med](#)

13. Destroy data and dispose of computers properly.

Many people assume deleting files totally removes the data. In fact, it does not and apparently deleted information can still be accessed by technically savvy people. If you have a device (including PC hard drives, CDs, Diskettes, USB keys, PDA's) containing sensitive data such as ePHI that requires disposal, reuse or donation, you must have all such sensitive data completely removed via such techniques as zeroing or degaussing or physically smashing the device. Contact your IT support staff, who can provide guidance on the necessary steps.

14. Privacy and security requirements apply to ALL locations, including your home.

Access to sensitive data must be limited to those users with a legitimate business need to access the information. Appropriate safeguards must be in place to prevent unauthorized exposure of sensitive information to anyone, including family members, friends, and others.

Use encryption technology (e.g. VPN and SSL) when accessing Yale systems remotely or over wireless networks.

VPN Links: [ITS](#) || [ITS-Med](#)

Install and use a hardware firewall at home. The current recommended hardware firewall is the [Linksys](#) BEF series. NOTE: *hardware* firewalls are recommended over *software* firewalls, but in some cases software firewalls such as [ZoneAlarm](#), are adequate, please consult your IT support provider or ISO with questions.

Never employ call forwarding on remote modem lines to gain access to ePHI systems which employ call-back user-authentication.

15. Implement additional security requirements for portable or handheld, and wireless devices.

Wireless devices (including laptops, smartphones and PDA's) must be configured to minimize the ability of unauthorized individuals to gain access to University resources or to monitor data communications. Wireless networks inherently provide a lower level of security than wired networks, making them problematic when handling ePHI. Clients should ensure their computing device is securely configured and if the computing device contains ePHI you should always enable a Yale VPN connection before making a wireless connection to the network.

Link: [ITS-Med](#)

Portable devices add another dimension to the problem of information security. Always protect a portable device with a password and configure the device to shut down (or lock in some other way) after a period of inactivity. That way, if the device is mislaid or stolen, access to the data will be made more difficult. If possible, encrypt any sensitive data that is stored on your portable device or media such as a "USB key" that you may use. Doing this may require technical expertise, please obtain assistance if needed.

Portable computing devices used for remote access that create, access, transmit or receive PHI must be enrolled in the [STOP—Security Tracking of Office Property](#) program. Please also check the ISO web sites to see if additional security measures might be available to assist in securing portable computing devices.

The official version of this information will only be maintained in an on-line web format. Any and all printed copies of this material are dated as of the print date. Please make certain to review the material on-line prior to placing reliance on a dated printed version.
