Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #11

Server, Desktop and Wireless Computer System Security

Last Revised: 3/15/2005	*Approved: 12/12/2005*

Microsoft Windows NT Server Security:

At a minimum, all servers that could potentially store Medium or High risk EPHI must adhere to the following:

The Department of Radiation Oncology will follow the following procedure to secure all Windows servers:

- All servers will be installed by department system managers. They will be installed isolated from the network until all patches and anti virus software have been installed. If the server does not store medium or high risk EPHI it can then be moved to DMZ.

    1. The administrator account will be secured using a non-standard name and the password will meet the HIPAA security minimum requirements (See HIPAA Access Controls procedure # 13).
    2. All Windows services not required will be disabled on each server.
    3. McAfee (or equivalent) Anti-virus client is installed on each server and maintained centrally by the McAfee Service Center. Servers are configured to request updates on a daily basis from the service center.
    4. Microsoft Updates will be applied/pushed by the OCF group as appropriate safety and applicability is examined.
- All servers housing Medium or High Risk EPHI will be located in the private WUCON networks.
- All servers that store High or Medium risk EPHI will be kept in a location that has a secured/keyed access computer room (See: #9 RO Facilities Access Control Procedure).
- All servers must be password protected at startup into Windows. The administrators will ensure the servers are configured to prompt for logon, and that the passwords exceed the minimum requirements (See: #13 Access Controls Procedure).

Unix/Linux Server Security

Any Unix/Linux server used to access, transmit, receive or store Medium or High Risk EPHI will be located in the secure WUCON networks. All servers that store High or Medium risk EPHI will be physically located in a secure location in accordance with #9 RO Facilities Access Control Procedure. As part of the Unix Solaris OS installation process the root/superuser account will use a password that meets or exceeds the password policy as outlined in Policy #13, Access Controls Procedures. See additional Reference Materials for Unix in Addendum 1, New Solaris Build Checklist)

The following steps are taken on all Unix servers managed and maintained by the Department of Radiation Oncology system managers.

1. Disable all unnecessary services
   - Solaris – Edit the inetd.conf file, commenting out the services that are listed in the Attached Addendum.
   - Red Hat Linux – This OS comes with a built-in firewall which will be configured to block traffic on all unnecessary ports.
   - HP-UX – Edit the inetd.conf file to disable unnecessary services.

2. Install/Configure TCP wrappers
   - Solaris – Version 8 and older of Solaris need TCP wrappers to be installed, version 9 and newer of Solaris come with TCPwrappers already installed, (See Addendum 1 for how to configure TCPwrappers)
   - Red Hat Linux – Since this OS has a built-in firewall no additional changes are needed, thus TCP wrappers are not needed.
   - HP-UX – TCP wrappers will be installed and configured to permit only necessary services

3. Install/configure SSH
   - Solaris – Version 8 and older of Solaris needs SSH installed, version 9 and newer comes with SSH already installed. (See Addendum 2 for How to Configure SSH)
   - Red Hat Linux – Comes with SSH already installed (See Addendum 2 for How to Configure SSH)
   - HP-UX – Install OpenSSH client and server

4. Kernel Modifications
   - Solaris – See Addendum for specific modifications.
   - Red Hat Linux – No modification needed at this time
   - HP-UX – No modification needed at this time

5. Disable SNMPXDMIND & NFS Server/Client
   - Solaris – See Addendum for Specific Configurations
   - Red Hat Linux – Not required at this time.
   - HP-UX – Not required at this time

6. Disable/Configure Sendmail
   - Solaris – See addendum 1 for Specific Configuration
   - Red Hat Linux – Unless needed, disable
   - HP-UX – Unless needed, disable.

The following steps will be taken as needed to keep Unix systems as secure as possible.

1. Install OS's and Application Patches
   - Solaris – Cluster Patches should be updated on a monthly basis to ensure that non-critical problems are fixed. If a critical patch is issued it will be installed in a timely manner after the necessary testing has been done. The urgency of testing and installations will depend upon the severity of the update, as specified by CERT and other prominent security agencies.
   - Red Hat Linux – As part of the installation process, the RED HAT NETWORK ACTIVATION TOOL is setup. This tool is always running and checks for updates/ patches. There is an icon in the icon tray that will flash red when a new update/patch is available. These updates/patches will be evaluated and installed accordingly.
   - HP-UX – For version 11.0 and newer, pre-installed system and application software will be updated periodically as patches are released by the manufacturer.
   - SunOS, IRIX, HP-UX 10.0 and earlier – On systems for which vendor-supplied updates are no longer available, system and applications software will be updated manually, where feasible, in response to critical security advisories. Such systems may *not* be connected to unsecured (WUSTL) networks.

2. User Accounts and Passwords
   - Solaris and Red Hat Linux – Each OS employs a username and password login system, and a unique username and password is assigned to each individual user of the system. Passwords will be assigned in accordance with HIPAA Policy 13, *Access Controls*. Currently our Solaris server requires a password of minimum length of 6 characters, this will be changed by editing the /etc./default/passed file and making sure that the PASSLENGTH variable is set to 8, thus requiring the password length to be 8 characters. Also Solaris requires that the password contain at least 2 alphabetic characters, in this case both Upper and lower case are considered alphabetic. It also requires at least 1 numeric or special character. If this is determined not to be adequate, a password cracking application, such as CRACK, John the Ripper or an equivalent application, will be installed and implemented, to ensure passwords meet the requirements setup in Policy #13. Redhat Linux by default has password minimum length of 5, and does not require any of the necessary requirements to meet policy #13. Redhat Linux has a rather complicated password checking algorithm. This algorithm can be setup to meet the password length requirements but much like Solaris it does not require the necessary complexity that is required in Policy #13. Again if it is determined not to be adequate, a password cracking application, such as CRACK or John the Ripper or an equivalent application, will be installed and implemented, to insure that password meet the requirements setup in Policy #13

Workstation Security, All Computers:

At a minimum, all desktop and laptop computers maintained by the WU Department of Radiation Oncology must adhere to the following:

- All desktop and laptop computers will be installed by the Oncology Computing Facility (OCF) personnel or designates using the following security guidelines:

    1. The administrator account will be secured using a non-standard name and password in accordance with HIPAA security procedure #13 Access Controls. The administrator account, generally used to administer the computer will remain intact on the PC as a decoy, but will have no rights on the PC.
    2. All unnecessary Windows services will be disabled on each workstation.
    3. McAfee (or authorized substitute) Anti-virus client will be installed on the each desktop and laptop. PCs are configured to request updates on a daily basis from the McAfee (or authorized substitute) Service Center (currently, at 2:00 AM). In addition, McAfee (or authorized substitute) virus scan is scheduled to run on each client computer regularly (at least weekly). If a PC is turned off at the scheduled scan time, the virus scan will run at the next system boot.
    4. Desktops and laptops in WU Radiation Oncology will be updated remotely by OCF. Security and critical updates will be pushed to the client computer from an OCF server that downloads the updates from Microsoft.

- All new computers must be installed on the network by Oncology Computing Facility (OCF) personnel or designates, and may not be installed by individual users in the department. This practice will help safeguard against unprotected computers being placed on the network. In addition, a user's individually owned desktop or laptop computers may not be brought in and placed on the network without assistance from the OCF.
- All desktop and laptop computers must be password protected at startup into Windows.
- OCF will take adequate precautions to ensure that all desktop and laptop computers are inventoried and patched with the latest Microsoft critical updates, and with the latest anti-virus updates.
- If more than one user needs access to a system on a desktop or laptop, access should be granted according to procedures in #4 Information Access Security Procedure.

Additional Workstation Security for PC's with Medium or High Risk EPHI:

In addition to the above, all WU Radiation Oncology desktop and laptop computers that could potentially store or access medium or high risk EPHI must adhere to the following:

- Computers accessing Medium or High Risk EPHI will be located within the secure / private WUCON networks.
- All WU Radiation Oncology desktop and laptop computers that store or access medium or high risk EPHI should be kept in a location that can be physically secured when no one is using the computer (i.e. within a locked office). If a computer is located in a common or otherwise physically unsecured area, the computer must have a password-protected screen saver, and users must log off, or utilize the Lock Computer feature (Ctrl, Alt, Del key sequence then Lock Computer) when leaving the computer unattended.

Mobile System Security Procedures:

- Maintain Physical Security

  By virtue of their mobility, PDAs and laptops can be easy targets for theft and loss. Care should be taken to not leave laptops, handheld devices, or storage media (e.g. flash drive, CD, DVD, or zip drive) unattended. Office doors or physical locations should be locked when you leave. If located in an unsecured area, your mobile device should be locked with a security locking cable.

- Securing the Device

  Employ the following basic security measures:
  - Enable the power-on password. Users should treat their password in the same manner that they would treat a PIN number on their ATM card.
  - Install Anti-Virus software if the device is used on the network.
  - Whenever possible, disable Active X controls if supported by the device.
  - Block unauthorized network activity through appropriate security settings on the native device if the device supports it.
  - Check settings for Bluetooth, Infrared, wireless and cellular networks to ensure that they are turned off when appropriate and otherwise secure.
  - All devices should be labeled with your name and contact information.

- Securing the Data

  Mobile devices can too easily fall into the wrong hands. In these circumstances, highly sensitive information can be compromised not only on the device but on the server as well if the user was logged on.
    - Do NOT use your PDA for long term storage of EPHI. EPHI data must not be stored beyond the length of time that data is required, with a maximum storage time of 30 days on any mobile device
    - Do not store files containing password to other systems on the mobile device

For more information, see Addendum 2: Pocket PC Security

Addendum 1: New Solaris Build Checklist

___Install Solaris Companion CD

___Remove services from inetd.conf (See Description on Next Page)

___TCP Wrappers installation (See Description on Next Page)

___Install Log Checker

___Install SSH (Part of the Solaris OS as of versoin 9 and newer, See Description on Next Page for more details)

___Install Latest Patch Cluster

___Setup any RAID devices needed

___Fill out "New Solaris Build Checklist"

___Update System Information in Lotus Notes

___Create user accounts

___Setup ntpdate (See Description on Next Page)

___ Modify Kernal (See Description on Next Page)

___Create cron jobs

___Create file with system information (checklist, information sheet, notes, crontab printout,)

___Disable SNMPXDMIND and Disable NFSServer and NFSClient if not used (See Description on Next Page)

___Disable/Configure sendmail (See Dscriptions on Next Page)

___Edit newsyslog on system older than Solaris 9

New Solaris Build Checklist Description

Disable Inetd.conf Services

All unnecessary services should be disabled in /etc/inetd.conf. This is done by placing a "#" in front of the service. Below are a list of services that should be disabled as of 10/04, this is not necessarily an inclusive list, these services should only be enabled if needed.

2. in.ftpd
3. tftpd
4. in.telnetd
5. in.tnamed
6. in.uucpd
7. in.fingerd
8. systat
9. netstat
10. time
11. echo
12. discard
13. chargen
14. in.rshd
15. in.rlogind
16. in.rexecd
17. testsvc
18. sadmind
19. rquotad
20. rpc.rusersd
21. tpc.sprayd
22. rpc.rwalld
23. rpc.rstatd
24. rpc.rexecd
25. kcms.server
26. ufsd
27. cachesfsd
28. kerbd
29. xaudio
30. rpc.cmsd
31. rpc.ttdbserver
32. printer

TCP Wrappers

TCP Wrappers are not included with the OS in Solaris version 8 or older, when installing these version TCP Wrappers are part of the companion CD, install the source code and recompile enabling TCP version 6 on these version.

TCP Wrappers are included with the OS installed on Solaris 9 and newer. No changes need to made when installing on these OS's

TCP wrappers should be enabled (according the instructions sent with TCP Wrappers) for all the above inetd.conf services, whether these services are enabled or not .

Create an /etc/host.allow and /etc/host.deny file, put ALL:ALL in the /etc/host.deny file and then allow only necessary protocols and network in the /etc/hosts.allow file.

SSH Installation & Configuration

SSH and SFTP should be used in place of telnet, rlogin, rsh and ftp whenever possible.

SSH is not included in the OS installs for Solaris 8 and older. OPENSSH or equivialent should be installed on these version of the OS.

SSH is included in the OS installs for Solaris 9 and newer. If using the inetd.conf options disable startup from /etc/init.d by moving the following file

/etc/rc0.d/K03sshd to /etc/rc0.d/_k03sshd
/etc/rc1.d/K03sshd to /etc/rc1.d/_k03sshd
/etc/rc2.d/K03sshd to /etc/rc2.d/_k03sshd
/etc/rc3.d/S89sshd to /etc/rc3.d/_s89sshd

Added the following line to the /etc/inetd.conf file to enable SSH with TCP Wrappers from the inetd process (our preferred way)

```
ssh     stream tcp      nowait root     /usr/sbin/tcpd  sshd -i
```

Added the following to the /etc/services file if not already there.

```
ssh     22/tcp
```

Edit the sshd.conf file (Solaris 9 and newer located at /etc/ssh/sshd_config, Solaris 8 and older located at /usr/local/etc/sshd_config), to include at least the following.

AllowTCPForwarding no
PermitRootLogin no
StrictModes yes
PrintMotd no
CheckMail no
PasswordAuthentication yes
PermitEmptyPassword no
RhostsAuthentication no

Setup NTPdate

Solaris comes with xntpd. To enable xntpd edit or create the following file (/etc/inet/ntp.conf) to include at least following

server 128.252.120.1

Kernal Modifications

The following lines should be added to the /etc/system file. Items in ()'s are just for reference and should not be added to the file.

set nfssrv:nfs_portmon= 1 (allows only NFS requests from privileged ports)
set noexec_user_stack =1 (disable stack overwrite, not needed on 64-bit OS systems)
set noexec_user_stack_log=1 (log stack overwriting attempts not needed on 64-bit OS's)
set sys:coredumpsize=0 (disable core files)

Disable SNMPXDMIND & NFS Server and Cleint

To disable NFS Server and Client move the following files

/etc/rc2.d/S73nfs.client to /etc/rc2.d/_s73nfs.client
/etc/rc3.d/S15nfs.server to /etc/rc3.d/_s15nfs.server

To disable SNMPXDMIND move the following files

/etc/rc3.d/S77dmi to /etc/rc3.d/_s77dmi
/etc/dmi/conf/snmpXdmid.conf /etc/dmi/conf/snmpXdmind.conf.orig

Disable/Configure Sendmail

Sendmail version 8.10.0 and newer now use multi port options thus to be able to sendmail out you need to have sendmail running. So the following changes need to be made to the /etc/mail/sendmail.cf file

O DaemonPortOptions=Name=NoMTA4, Family=inet, Addr=127.0.0.1

Sendmail 8.9.x and older do not use the DaemonPortOptions so move the following file to disable sendmail. /etc/rc2.d/S88sendmail to /etc/rc2.d/_s88sendmail

Addendum 2: Pocket PC Security

PDA's, and Laptop's

A risk assessment should be performed on each device based on the data that is stored on it and the way it will be used. For PDA's that contain or will access EPHI the following checklist should be applied to these devices and users should be made aware of the following security shortcomings of these devices.

1. Power on Password - Microsoft has implemented a power on password. It is recommend that you change the settings to ensure it allows an alphanumeric password and enter a password that is at least 8 characters long. Follow common password procedures like not using a word that is found in a dictionary and including numbers will ensure your password cannot be easily guessed. Hard Password Creation can be found in the HIPAA Policy #16 procedure. At this point the Windows Mobile operating system does not provide a power-on banner prior to sign-on so you cannot warn users not to attempt to access the system without authorization. This may affect your ability to prosecute persons that attempt to hack the system. You may find that entering a warning banner in the Today screen, User Information as an acceptable work around for this.

   For Palm OS devices, a power-on password is native to the client, and should be implemented for those devices storing EPHI. The password must comply with the password standards as documented in policy #13, *Access Controls Procedures*. Unfortunately, the PALM OS shows the power on password in unencrypted, clear text format. If storing Medium or High Risk EPHI, the user must purchase a third party password encryption software package.

2. Memory Protection between Applications - Microsoft has not implemented memory protection in the Windows Mobile operating system. This means that any application can look at the memory of another application. So if you are storing passwords in encrypted format using a 3rd party program such as eWallet (http://www.iliumsoft.com/site/ew/ewallet.htm) or CodeWallet Pro (http://www.developerone.com/codewalletpro/pocketpc.htm) which must decrypt the passwords to display them, any application in the system could read this sensitive data. Microsoft made the decision to not implement memory protection between applications in the Windows Mobile implementation even though the Windows CE operating system has supported it since version 1.0. It is highly recommended that a review what of applications are allowed to be installed to minimize this risk.

3. File System Encryption – The Windows Mobile operating system, as well as the PALM OS, does not support file system encryption. You will need to check out 3rd party applications that support encryption of the file system to prevent unauthorized access to the files stored in the Pocket PC. Also, this includes the ability to encrypt data on storage cards such as the Secure Digital card or using NTFS with encryption.

4. Viruses – Microsoft and PALM OS do not include a virus scanner. Currently the virus scanners look for desktop viruses on the Pocket PC to prevent them from being spread. Applications such

as AirScanner, McAfee and Norton Antivirus are available to address this need. The virus profiles should be updated on a weekly bases.

5. Keyboard Sniffers – With the addition of different methods of input (using the SIP), a vendor could create a program to capture all your keystrokes and the applications they were fed into. So allowing a user to install an add-on SIP increases the risk of this occurring. Calligrapher (http://www.phatware.com/calligrapher/index.html) is an example of this SIP replacement that is safe. However installing applications like this that are not from a reputable vendor may allow them to capture your keystrokes. Microsoft does not have a method in the operating system to prevent keystroke capture from occurring so it is recommended that users be informed of the risk. Not applicable on PALM OS.

6. Internet Access – With the direct connections to the internet using Ethernet, Wi-Fi, GPRS/GSM or 1xRTT and in addition of desktop passthrough, an application running on the PC can silently send or receive data without your knowledge. There is no option to turn off passthrough access or disable the ability to connect to the internet if the user has the appropriate hardware. Therefore when using these devices on an unsecured network some of encryption service must be provided.

7. Internet Explorer – If the unit is to be used on the network Active X controls should be disabled. The Pocket PC can silently install ActiveX controls that are specifically designed to run on it when a user clicks on a link. There is a registry hack available to prevent the installation of ActiveX controls in RegKing (www.cewindows.net/applications/regking.htm) Also, if a user clicks on a .CAB file they can download and install an application so if you allow your users access to the internet, they can add applications without ActiveSync or even a PC.

8. Storing Passwords - By default the Windows Mobile 2003 and Pocket PC operating systems allow users to choose to store their username and password to access websites and network shares. Users should not store any passwords on the Pocket PC just in case it is lost or stolen. This applies to the PALM OS as well.

9. TCP/IP Services – The Pocket PC does not ship with any TCP/IP based servers installed. It does act as a client to servers using TCP/IP such as Netbios, HTTP, HTTPS, SMTP, POP3, IMAP4 and LDAP. Also, ActiveSync uses PPP and special ports 990, 999, 5678, and 5679. So if the device is to be used on an unsecured network you will need to secure the Pocket PC and install a firewall on it to prevent these services from be used by programs. Not applicable to Palm OS.

10. System logs – Neither the Pocket PC, nor the PALM OS device implements system logs to track what applications are used, when errors or problems occur or what is synchronized or installed on the device. So Third party product to do so should be installed if possible so that the device can be audited when necessary.

11. Program Installation – Programs can be installed using ActiveSync, a .CAB file on a website or a memory card inserted in the Pocket PC, or an executable program (.exe) copied to the Pocket PC. Also users can beam applications using the file transfer function in Windows XP using Infrared to the Pocket PC without even having ActiveSync installed on the PC. At this time, there is no built

in method to prevent users from installing applications. Further once an application is installed it may not be displayed in the Remove Programs. So before deploying any Pocket PC, It is recommended performing a hard reset before synchronizing and installing any additional applications. It should also be discussed with the user as to what applications present risk. PALM OS program installations must be performed by synching with the PC on which the cradle is connected.

12. Inability to control when applications execute – The Pocket PC operating system includes the ability to run applications on reset or power on. This ability could allow an application to run silently in the background without being visible to the user including in the list of running applications to the operating system. Right now Microsoft does not offer a method for users to know all the applications or processes running on their Pocket PC or how to stop them. Users should insure that all applications are properly shutdown when no longer in use.

13. HTML Page can prompt the user to dial a number - On the Pocket PC 2002, Windows Mobile 2003 and the SmartPhone 2002 and 2003 if a website or locally stored html page contains a url formatted like call and the user clicks on the link they are prompted with a do you want to dial box containing the number. This could allow a 3rd party to incur expensive charges for phone numbers that are dialed using their cellular phone. At this time there is no method of preventing the mobile device from prompting the user to dial the number in the link. As a workaround it is recommended that you advise users of the risk this presents.

For more information, See Addendum 3A: How to: Increase Information Security on the Pocket PC (Windows CE)

Addendum 3A: HOW TO: Increase Information Security on the Pocket PC (Windows CE)

This article was previously published under Microsoft Q314647

As the popularity of mobile devices increases, the security of the information and data on these devices becomes more important. The Pocket PC contains many features that reduce the risks that are associated with mobile devices. This article describes some of the security risks that are related to these devices and how to minimize those risks.

Securing Your Hardware
The Pocket PC provides many features for securing your device hardware. To reduce the possibility of data being stolen:

1. Use the Power On password on your device:
    1. Tap Start, and then tap Settings.
    2. Tap the Personal tab.
    3. Tap Password.
    4. Tap the type of password you want to use, and then tap a setting in the Prompt if device unused for box.
    5. Tap OK.

NOTE: For additional information about passwords, tap Start, tap Help, and then tap Password.

2. Password protect your PALM OS device:
    1. Tap Security
    2. Tap or script write your password
    3. Click Lock and Turn Off

3. Password protect your CompactFlash cards. The device must support this feature. For information about how to password protect your CompactFlash cards, please view the documentation that is included with your CompactFlash cards.

4. To protect against device failure, use Microsoft ActiveSync to frequently back up your device:
    1. In ActiveSync, click Backup/Restore on the Tools menu, and then click the Backup tab.
    2. To back up all of your information, click Full backup. To back up only new and changed information, click Incremental backup.
    3. Click Back Up Now.

NOTE: For additional information about backup, view ActiveSync Help.

Encrypting Your Data

You can encrypt your files on your Pocket PC through the use of third-party encryption products. Encryption provides data security if your Pocket PC password is compromised.

What to Encrypt?

* Your CompactFlash cards.
* Any confidential folders or files.

Products Available

* The Application Development Studio "PocketLock" program.
* The Applian Technologies "PassKey" program.
* The SoftWinter "seNTry" program.
* The Sofwareburo Muller "TheSafe" program.
* The V-ONE "SmartPass for CE" program.
* The Paragon Software "CryptoGrapher for Windows CE" program.

Protecting Your Communication Links

Because Pocket PCs can communicate with other devices, it is useful to secure your communication link by using one or more of the following methods or products:

* Obtain and install the Microsoft High Encryption Pack for Pocket PC. To do so, visit the following Microsoft Web site:

* Obtain and install a third-party antivirus program:
    - The McAfee "VirusScan for Pocket PC" program.
    - The Computer Associates "InnoculateIT for CE" program.
    - For more information about antivirus programs and Pocket PCs, please visit the following Microsoft Web site:

http://www.microsoft.com/mobile/pocketpc/columns/viruses.asp