

## HSC COMPUTING BEST PRACTICE GUIDELINES

Required for HIPAA as well as campus computing security

Security is an area that is receiving a lot of visibility in these days of having to get things done while under constant attack by malicious agents. Increasing security adds inconvenience and expense, but is necessary in order to protect our data.

There are a number of things you must do, and quite a few more that you can do to make your computer, work area, server and data more secure, whether you are using Protected Health Information (PHI) or not. These fall under the category of "Best Practice," recommended by security agencies. These practices are sorted by those required by HSC policy, and those that are recommended. If you have questions or would like additional information about any of these items, Faculty/Staff, contact your LAN administrator or the IT Services Help Desk at (303) 724-4375. Students, contact the Student Computing Coordinator at (303) 315-1397 or your schools IT representative.

**Remember, security is everybody's responsibility.**

You'll notice that some requirements appear in many sections. That's because each section is designed to be complete "in its own right." Therefore these essentials are repeated in each applicable section.

### **Desktop Computers:**

#### Required

- Log in to computer and domain with your individual account.
  - Do not share your login name or password with anyone else.
  - Change your password immediately after help desk or support personnel are finished using it to fix your system.
  - See HIPAA Safeguards policy  
<http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Keep your passwords current and change them in compliance with campus policy.
  - The password policy is located at <http://www.uchsc.edu/admin/policies/fp5-13.pdf>.
  - For help selecting an appropriate password, see <http://www.uchsc.edu/is/policies/ans2.htm>.
  - See HIPAA Safeguards policy  
<http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
  - CU System Password Policy:  
<http://www.cusys.edu/security/users/password.html>.
- Keep operating system and application patches and hot fixes up-to-date.
  - HSC IT Services offers a centralized patch management service.
  - See HIPAA Safeguards policy  
<http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Keep anti-virus software up-to-date and enabled.

## Revision Date

8/16/2005

- IT Services has purchased a volume anti-virus license, which allows us to provide anti-virus software free of charge to all HSC users. This includes faculty, staff, and students, on-campus, remote office, home, or laptop computers.
- IT Services updates the anti-virus definition files automatically on a weekly or more frequent basis.
- See <http://www.uchsc.edu/is/viruses/> for information on obtaining and configuring this free software.
- Occasionally run full scans, as undetected virus signatures can sit dormant on a drive for some time.
- The secure computing policy is located at <http://www.uchsc.edu/admin/policies/fp5-09.pdf>. See pages 2 and 3.
- See HIPAA Safeguards policy <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Don't install and use music-sharing applications like Napster, KaZaA, Morpheus, etc.
  - They are expressly forbidden by campus policy because they jeopardize campus security.
  - They use up network bandwidth and cause poor performance for others.
  - The users of these applications and the campus incur a legal liability.
  - The appropriate use policy is located at <http://www.uchsc.edu/is/policies/aup.htm>.
- Don't download or install non-business-related software.
  - See Use of Information Technology policy: <http://www.uchsc.edu/admin/policies/fp5-03.pdf>
- Practice data backup, storage, and retention procedures supportive of university and campus policy, as well as state data retention rules.
  - **Need storage & backup policy.**
  - The HIPAA Retention of Records policy is located at <http://www.uchsc.edu/hipaa/internal/docs/1.7.pdf>
- Create an emergency repair disk (ERD)
  - Update periodically or when new users or system configuration changes.
  - Store with backups, off-site if possible.
- Properly dispose of your old computer systems.
  - For disposal procedures, see [http://www.uchsc.edu/is/policies/pc\\_disposal.htm](http://www.uchsc.edu/is/policies/pc_disposal.htm).
  - **Need policy.**

### Recommended

- Ensure workstation is protected from inappropriate access.
  - Lock the cover on the system to prevent unauthorized physical access to internal hardware components.
  - Attach cable locks to prevent the computer console from being physically removed from the room.
- Use password protected screen savers.
  - Set screen saver up to activate automatically after "a few minutes" of inactivity or lock your workstation by hitting Ctrl-Alt-Del and selecting the "Lock Computer" option before leaving your desk.
- Turn the monitor so it faces away from a public area.

Revision Date

8/16/2005

- If you have trouble remembering your various passwords, consider installing a password vault application. These are available free or at low-cost on the web.
- Use computers with newer operating systems (OS).
  - Legacy OSs do not take advantage of many current security features and are inherently insecure. Legacy OSs include Windows 95/98/ME/NT, and Mac OS older than 9.1.
- Format your Windows computers using the most secure file system, currently NTFS.
- Do not set up file sharing on your computer.
  - Non-password protected shares are forbidden by campus policy (Page 3, Secure Computing Policy, <http://www.uchsc.edu/admin/policies/fp5-09.pdf>). But even password-protected shares contain vulnerabilities. That's how many viruses are spread.
  - If you need to share data, store that data on either a departmental or IT Services-owned community server.
- Do not store PHI, sensitive, or critical information on your desktop computer, i.e. your "C" drive.
  - Always store sensitive information on a secure server. Sensitive information can include things as simple as lists of names and email addresses, social security numbers, and other identifiers.
- Minimize the number of applications and custom programs installed on any work computer.
  - The greater the number of applications installed, the greater the potential for patches and unplanned events to damage or crash your machine.
- Suggested configurations for Web Browser Privacy and Security settings. Carnegie Mellon, [http://www.cmu.edu/computing/documentation/web\\_configure/web\\_configure.html](http://www.cmu.edu/computing/documentation/web_configure/web_configure.html), has a lot of good information.
- For systems creating, modifying, or transmitting highly sensitive information (some types of Protected Health Information (PHI), SSN or credit card numbers, install firewall and intrusion detection software.
  - Contact Information Systems for help in configuring appropriately. These utilities, if improperly configured, can prevent you from being able to do your job and prevent your computer from receiving anti-virus software or patch updates.

#### **Paper PHI:**

##### Required

- Verify fax number before sending document.
- Use cover sheet that includes statement of HSC privacy practices.
  - **Is there a standard (short, i.e. 1 paragraph) HSC notice that can be included? We should include a link to it.**
- Don't leave documents containing PHI or sensitive information unattended.
- See HIPAA policy at <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 7 for fax machine policy
- Protect networked printers with access controls and passwords. Like computers, they are vulnerable to attack and can serve as network attack agents.

## Revision Date

8/16/2005

- Keep paper PHI locked up in secure file storage drawers or rooms.
- When no longer needed, promptly shred printed material.

### Recommended

- Adopt a "clean-desk" policy.
  - Put away any sensitive or critical information after use.
  - Do not leave material out when you leave your desk.
- Locate printers and fax machines in areas where the public cannot see any PHI or other sensitive information being printed, copied, sent or received.

### **Document Storage:**

#### Required

- Maintain physical control over portable media like external USB/FireWire drives, zip disks, flash memory cards and devices, DVDs/CDs, floppies.
- Media containing PHI and sensitive data should be encrypted using strong encryption and passwords/keys meeting campus password standards.
  - [http://www.uchsc.edu/is/helpdesk/bulletins/pgp\\_notification\\_042204.htm](http://www.uchsc.edu/is/helpdesk/bulletins/pgp_notification_042204.htm)
  - **Need a policy for this.**
- Do not store or edit HSC or CU documents on personal computers or home PCs; leave it on protected servers or use protected university equipment.
  - Security policies and disposal procedures cannot be performed against personal equipment, making such equipment a risk to data security and integrity.
  - See HIPAA policy at <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Remove PHI from media before the media are made available for re-use.
  - Use a disk wiping program to ensure removal of data.
  - These can be found on the Internet by searching using the term "disk wiping."
  - Many of these applications are free.
- Make sure portable storage devices (i.e. DVD/CD, zip disk, flash drive, Magneto-optical (MO) disc, floppy disk, etc.) containing PHI are properly erased or destroyed when the data is no longer needed.
- Be aware of the State of Colorado data retention policies and rules before destroying data records.
  - The HIPAA rules on data retention are located at <http://www.uchsc.edu/hipaa/internal/docs/1.7.pdf>.

#### Recommended

- Lock rooms containing PHI, sensitive or critical information.
- Restrict access to areas where documents are stored.
- Limit the critical/sensitive data or PHI that is stored on portable storage media.

### **Servers:**

#### Required

- Keep operating system and application patches and hot fixes up-to-date.
  - See HIPAA Safeguards policy <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Keep anti-virus software up-to-date and enabled.

## Revision Date

8/16/2005

- IT Services has purchased a volume anti-virus license, which allows us to provide anti-virus software free of charge to all HSC users. This includes faculty, staff, and students, on-campus, remote office, home, or laptop computers.
- IT Services updates the anti-virus definition files automatically on a weekly or more frequent basis.
- See <http://www.uchsc.edu/is/viruses/> for information on obtaining and configuring this free software.
- Occasionally run full scans, as undetected virus signatures can sit dormant on a drive for some time.
- The secure computing policy is located at <http://www.uchsc.edu/admin/policies/fp5-09.pdf>. See pages 2 and 3.
- See HIPAA Safeguards policy <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Allow only authorized users to have access to data on the server; limit that access to what is needed for that person to do his/her job.
  - **Need policy and procedures.**
- Keep server in locked room with access limited to only approved people.
  - Limit physical access to the server.
  - Remember that the value of a machine includes not only the value of the hardware itself, but the value of the data on it, and the value of the access to your network.
- Perform a periodic risk analysis - know what applications on your server contain PHI or other sensitive information.
  - **Need procedures.**
- Perform periodic information system activity reviews of your server, including procedures to review records of information system activity including:
  - audit logs
  - access reports (access of resources)
  - security incident tracking reports
  - **Need policy and procedures.**
- Identify and respond to suspected or known security incidents.
  - Report any such incidents to the IT Services Help Desk (724-4357) or to the HIPAA Security Officer (724-0495).
- Lessen harmful effects of security incidents. Perform each of the activities below as appropriate.
  - Review anti-virus web sites for virus removal/system repair.
  - Analyze system logs to determine when problem occurred.
  - Review intrusion detection logs and patch or repair vulnerabilities.
  - Perform vulnerability scans and patch or repair vulnerabilities.
  - Implement data protection and physical security practices.
  - Hold a "lessons learned" meeting to evaluate management of security incident.
- Perform regular backup of sensitive information, PHI, and critical information.
  - Have a backup plan that describes backup routine and includes an off-site storage location of backup media.
  - Backups should be tested regularly. Having a backup does you no good if you can't restore your data.

## Revision Date

8/16/2005

- Information Systems provides a backup service for servers outside of IT Services. Contact the Help Desk (724-4357) for additional information.
- **Need policy.**
- Document the procedure for the disposal of PHI and/or the hardware on which it is stored, when it is no longer needed.
  - **Need policy and procedures.**
- Notify IT Services of your server name and IP number, as well as the system administrator names and emergency contact information so you can be alerted to emergency or security-related information.
- Properly dispose of your old servers.
  - For disposal procedures, see [http://www.uchsc.edu/is/policies/pc\\_disposal.htm](http://www.uchsc.edu/is/policies/pc_disposal.htm)

### Recommended

- Store the server(s) in a location with appropriate environmental controls.
  - Adequate air conditioning
  - Humidity and dust control
  - Provide backup power in the form of an uninterruptible power supply (UPS) or other power management.
- Don't display the last logged-on user name.
- Disable the feature that allows CD-ROMs and audio compact discs (CDs) to run automatically when you insert them in your CD-ROM drive.
- Rename local administrator account.
  - Create a bogus administrator account that has no rights.
  - Give both complex passwords.
- Disable and rename guest account; give guest account complex password.
- Avoid multiple services running on the same server wherever possible.
  - Running web servers, application servers, and data servers all operating from the same piece of equipment increases data risk.
- Document security incidents and their outcomes.
- Have a disaster recovery plan.
  - Plan should include dealing with emergency conditions such as power loss, force of nature, act of war or terror, personnel contingencies (e.g. loss of personnel due to death or injury, disease, etc.) etc.
  - Test the plan.
  - Include plans for operating in an emergency mode.
  - **Needs policy and procedures; possibly plan template.**
- Use servers with newer operating systems (OS). Legacy OSs do not take advantage of many current security features and are inherently insecure.
- Provide temporary employees and student workers with individual Stargate accounts that have only limited access.
  - Only minimum necessary access should be granted (see <http://www.uchsc.edu/hipaa/internal/docs/1.3.pdf>).
  - Have temporary employees and student workers sign a sponsored user form and complete HIPAA training (if appropriate). The sponsored user form is located at <http://www.uchsc.edu/is/forms/sponsor>.

## Revision Date

8/16/2005

- Instructions for setting up temporary accounts can be found at <http://www.uchsc.edu/is/lan-admins/Steps4tempusers.pdf>.
- Put in place testing and revision procedures for software and hardware changes.
  - Policy is needed.
- Document repairs and modifications to physical components.
  - Policy is needed.
- Perform regular security scans of your server(s). Free software, such as Microsoft Baseline Security Analyzer, is available on the web.
- For systems creating, modifying, or transmitting highly sensitive information (some types of Protected Health Information (PHI), SSN or credit card numbers, install firewall and intrusion detection software.
  - Contact Information Systems for help in configuring appropriately. These utilities, if improperly configured, can prevent you from being able to do your job and prevent your computer from receiving anti-virus software or patch updates.

### Data:

#### Required

- Limit access to data to those who need the data to do their jobs.
  - Develop formal procedure for how authorization is granted and who is allowed to grant it.
  - Develop procedure for maintaining documentation of each person granted access, and ensure authorization is removed when individual no longer needs access to perform his/her job.
- Allow access to data only through individually identifiable accounts.
  - See HIPAA Safeguards policy <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- Have a contingency plan in place, describing how the data will be accessed in case an attack penetrates the system and damages the data.
- Ensure removal of PHI from media before the media are made available for re-use. New hard drives are cheap, privacy violations are very expensive.
  - Erase drives and media with an approved disk wiping program that ensures all data is physically overwritten. Many free disk wiping tools are available on the web.
  - Include non-standard media such as flash memory cards in these considerations.
  - If media was used to store PHI or highly sensitive data, consider destroying it rather than recycling it.
- Document departmental policies and procedures relating to PHI, sensitive, confidential, proprietary, or critical data.
  - Make documentation available to those responsible for implementing the procedures to which the documentation pertains.
- To retain the integrity of the data, do not allow multiple copies of a database to co-exist.
  - If multiple copies of a database exists, it creates questions as to which copy is the "system of record."

Revision Date

8/16/2005

#### Recommended

- Password protect access to the data in an application, if possible.
  - Use recommended password configuration.
- Grant only minimum necessary access.
  - See HIPAA minimum necessary policies at <http://www.uchsc.edu/hipaa/internal/docs/1.3.pdf>
- Maintain written policies governing access to data, usage of that data, and disposal of the data.
  - These policies should be readily available to all users of the data and should be updated regularly.
  - Users should receive training on these policies.
- Put in place controlled conditions for testing and revision of software programs.
- Write and retain maintenance records documenting modifications to the application.
- Maintain and regularly review audits of access of the data for irregularities.
- Develop procedures for obtaining necessary PHI during an emergency.
- Develop procedures to terminate a session after a predetermined time of inactivity.
- Review documentation periodically and update as needed.

#### **Handheld Devices:**

##### Required

- When it is necessary to store PHI on a handheld device, ensure the data has been encrypted and the system is password protected.
  - The password should be the same as the domain password, and should be changed each time the domain password is changed.
  - Don't forget to also encrypt data on external memory cards.
  - HSC IT Services has licenses for PGP. There is a small charge for the license and installation. See [http://www.uchsc.edu/is/helpdesk/bulletins/pgp\\_notification\\_042204.htm](http://www.uchsc.edu/is/helpdesk/bulletins/pgp_notification_042204.htm)
  - The keys are stored on a server, and data can be decrypted if the original key is lost.
  - If you make a change to your keyring, copy the new keys to the keyserver.
- Never leave the device in a public place.
- Always lock the device when not in use.
- Do not store your encryption keys with the device, e.g. if your keys are on a diskette, do not store that in the case along with a laptop computer.
- Synchronize and back up the data on your handheld device.
  - Be aware of problems synchronization of your handheld device may cause to your data, address lists, or email.
- If the device is damaged or broken, do not return it to your retail service center for repair; contact the Help Desk so the device can be re-imaged or erased.
  - These devices are frequently not repaired, just replaced. Any data on the device would then potentially be available to buyers of surplus equipment.
- If device is lost or stolen, and contains PHI, sensitive, or critical information, notify your department and the HSC HIPAA Privacy Officer immediately.

##### Recommended

## Revision Date

8/16/2005

- Prior to purchasing your handheld device, contact the Help Desk to make sure it is a brand and model that is supported by IT Services.
  - IT Services may not be able to provide setup, configuration, synchronization, or problem resolution of systems that we do not regularly support or that are outdated.
- Prior to installing software on your handheld device, ensure that it is supported by IT Services.
- If possible, don't store PHI, sensitive, or critical information on device.
- Use the device for HSC purposes only.

### Remote Access:

#### Required

- Keep operating system and application patches and hot fixes on home and remote office computers up-to-date.
  - Enable Automatic Updates on Windows 2000 and higher computer.
  - Enable the Software Update feature, found in the System Preferences on Macintosh OS X.1 and higher.
  - Or visit the update site for your computer platform (i.e. Windows, Apple, UNIX).
    - Windows' current update site is <http://v5.windowsupdate.microsoft.com/v5consumer/default.aspx?ln=en-us>
    - Apple's current update site is <http://www.apple.com/support/>.
- Keep anti-virus software up-to-date and enabled.
  - IT Services has purchased a volume anti-virus license, which allows us to provide anti-virus software free of charge to all HSC users. This includes faculty, staff, and students, on-campus, remote office, home, or laptop computers.
  - IT Services updates the anti-virus definition files automatically on a weekly or more frequent basis.
  - See <http://www.uchsc.edu/is/viruses/> for information on obtaining and configuring this free software.
  - Occasionally run full scans, as undetected virus signatures can sit dormant on a drive for some time.
  - Uninstall other anti-virus software products.
    - Use of multiple anti-virus products can cause your computer to behave in a bizarre fashion.
  - The secure computing policy is located at <http://www.uchsc.edu/admin/policies/fp5-09.pdf>. See pages 2 and 3.
  - See HIPAA Safeguards policy <http://www.uchsc.edu/hipaa/internal/docs/7.1.pdf>, page 4.
- All users of HSC remote access services must use approved access control technologies when accessing the campus network from a remote location.
- Special requirements for high speed Internet connection users (i.e. DSL/Cable modem, microwave, etc.).
  - Use only supported operating systems:
    - Windows 98, 2000, XP Professional, or higher
    - MacOS 8.1 or higher (with Open Transport 1.3 or higher).

## Revision Date

8/16/2005

- Your home computer's name must be <userid>PC, where <userid> is your Stargate ID (see [computer names](#) for details).
- A VPN client must be installed.
  - VPN is used for:
    - File service, printer access, telnetting to an on-campus computer, or reading your email with Outlook.
  - You don't need to use VPN to access webmail or get to Internet sites.
- Do not connect to the Internet while using VPN to access data from HSC because:
  - Your Internet access will be slower.
  - This introduces the possibility of malware downloaded to your computer also being sent to your HSC resource.
- Use personal firewall software.
  - For Windows systems, Zone Alarm is available free from [http://www.zonelabs.com/store/content/company/products/zna/m/freeDownload.jsp?lid=zaskulist\\_download](http://www.zonelabs.com/store/content/company/products/zna/m/freeDownload.jsp?lid=zaskulist_download).
  - [TunnelBuilder VPN client](#) and [Norton/Symantec Personal Firewall for the Macintosh](#) are available for Macintosh systems. These are not free.
- Home networks are not supported because:
  - There is no way to secure them and no way to track continued compliance.
  - Home networks contain a vulnerability called split tunneling.
    - Split tunneling divides the network connection into multiple parts that may allow hackers to access the HSC network if one of your home systems has been penetrated.
  - See wireless section below.

### Recommended

- Install anti-spyware software on your computer; download updates and run regularly.
  - Many anti-spyware products are available for download free from the web.
  - Search on the keyword "spyware" for a list of offerings.
- In order to ensure that your login script runs and maps your drives, log into the HSC domain from the login prompt, checking the "log in using dial-up connection" box from the Ctrl-Alt-Del screen, rather than connecting to the domain after login to the desktop has completed.
- For same "look and feel" each time you log in, always log in using your Stargate account and Stargate as the domain. As long as you don't select the dial-in connection box, you won't be running Remote Access software or VPN.

### **Wireless:**

#### Required

- Keep operating system and application patches and hot fixes up-to-date.
- Keep anti-virus software up-to-date and enabled.
- Install and run firewall software.
- Disable file-sharing.
- Contact your LAN Administrator or the IT Services Help Desk for secure set-up information.

Revision Date

8/16/2005

- See <http://www.uchsc.edu/is/wireless/> for additional information.
- If you have a home wireless network and want to access UCHDSC:
  - Change the default password needed to access your WL devices.
    - WL access points and routers require passwords for initial configuration and maintenance.
    - These devices have factory default passwords which should be changed when you set up the system.
    - Choose a complex password consisting of a minimum of eight characters, selected from numbers, upper- and lower-case letters, and special characters.
  - Register your home WL computers. That is, your WL router should only offer service to those computers that you register at home.
    - Change the default home WL network name.
    - The name of your home WL network is called its service set identification (SSID). Change the SSID from the industry default name (which is how your WL network will initially boot up) to make it more difficult for casual users to use.
  - Do not use a name that can identify you or your family.
  - Be aware that SSIDs are "case sensitive" and must match on both the wireless gateway and on the software client utilities of your computers using wireless cards.
  - Disable the broadcasting of the home WL network name.
    - Set your SSID so that it does not broadcast its services.
    - If that's not possible, select the "closed network" option.
  - Limit the number of simultaneous users.
    - Set your home router to support only the number of computers you possess. Only issue enough IP addresses to support your home network.
    - Apply a MAC filter (12 digit hexadecimal number, generally found on the back of the network card, known as the hardware or MAC address) with the "allowed" MAC addresses of your wireless cards.

### Recommended

- Encrypt your home WL network.
  - Use WiFi Protected Access (WPA) - uses a longer key (up to 256 bits) that changes periodically (with a default of 50 minutes)
  - Provides a longer, changing key and adequate security against eavesdroppers.
  - If possible, use the pre-shared key (WPA-PSK) mode for your home WL system.
- Use lower power settings
  - If possible, set "adjust antenna transmit power" high enough to provide signal coverage for your home, but low enough so that your neighbor several doors away can't also use your wireless network.
  - If your wireless router doesn't have the ability to adjust these settings, physically locate the unit in the center of the house and away from windows.

Revision Date

8/16/2005

- Disable DHCP settings and manually set static IP numbers on all wireless cards.

#### Web:

##### Required

- Ensure all web server patches are up-to-date.
- If you publish information on the web, and it will be available on the Internet, do not include information like IP number, server or computer name, modem line phone numbers, user account name or password.
- If confidential data will be published on the web site, require users to make secure connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocols.
- If transferring data to/from FTP sites, use only secure file transfer protocols (SFTP) or Secure Copy (SCP) over a Secure Shell (SSH) connection.
- Avoid setting up Web based applications unless you are familiar with and able to create robust applications that are not susceptible to common web attacks such as cross-site scripting, SQL injection attacks, man-in-the-middle vulnerabilities, redirection, etc. If you don't know how to configure your web server to prevent these types of attacks:
  - seek guidance from IT Services and web publications personnel
  - request that IT Services host your web site

#### Email:

##### Required

- Email spam can spread malicious code by spoofing "TO" and "FROM" e-mail addresses to make it appear that the email is from the HSC email team, server administrators or even friends and co-workers. This makes it difficult to tell which attachments are legitimate and which carry malicious code. Because of that:
  - don't open an attachment unless it is something you are expecting.
  - never click on an executable attachment, even if it appears to come from someone you know.
  - never apply a patch from an attachment, especially if the email tells you the attached patch, update, or fix will repair a computer vulnerability. Software manufacturers do not send patches via email attachment; they will provide the link to the patch location.
  - If you must install something, go to the vendor's web site or use an automatic update service to download the patch.
- Email or documents attached to an email message and sent within the campus or hospital systems listed below do not need to be encrypted.
  - HSC, The Children's Hospital (TCH), University Physician's Inc. (UPI), University of Colorado Hospital (UCH), and National Jewish Hospital (NJH) have a private network, and mail does not go out to the Internet to move from one email account to another.
  - HSC, in conjunction with the above institutions, has a separate e-mail system that provides encryption for sensitive messages when they need to be sent to institutions or patients over the Internet.

## Revision Date

8/16/2005

- see <http://www.uchsc.edu/is/securemail/> for additional information about this offering.
- Public e-mail systems like aol.com, hotmail.com, etc. don't support e-mail encryption. Don't use one of these systems to transmit PHI over the Internet.

### Recommended

- If at all possible, don't send PHI in an e-mail message or as an attachment to an email message.
- Make reasonable efforts to either encrypt or de-identify information if PHI must be sent over the Internet. Reasonable precautions may include:
  - Send only the minimum necessary information when it is necessary to send PHI over the Internet.
  - Try to avoid sending sensitive information over the Internet. Discussing infectious diseases over the Internet is more sensitive than discussing a cold.
  - Ensure that you are sending to the correct e-mail address before sending PHI over the Internet.
- Use a disclaimer at the end of your message. The disclaimer could be something like "CONFIDENTIALITY NOTICE: The information contained in this message is legally privileged and confidential information intended only for the use of the individual or organization to whom it is addressed. If the reader of this message is not the intended recipient, or the employee or the agent responsible to deliver it to the intended recipient, be advised that you have received this e-mail in error and that any use, dissemination, forwarding, printing or copying of this e-mail is strictly prohibited. If you have received this e-mail in error, please notify the author immediately by replying to this message and delete the original message. Thank you."

## Databases:

### Required

- Ensure all database patches are up-to-date
- Apply the principle of least privilege.
- Ensure that all accounts, including administrator, have only the specific permissions they need to execute authorized functions.
  - Change the passwords periodically.

### Recommended

- Use Windows Authentication.
- If possible, rename default administrative accounts and change the default passwords.
- Change the Startup Account that starts SQL Server from LocalSystem to a non-descriptive login and password.
  - Assign this account a new login with very few rights to your machine. It must be set up to "Log on as a service," and possibly "Log on as batch."
  - DON'T change this service account password, or the application may break!
- Use database views instead of queries.
- Audit failed logins and denied access messages.

Revision Date

8/16/2005

- Make use of stored procedures.

MORE INFORMATION ON DATABASE SECURITY:

[http://searchsecurity.techtarget.com/tip/1,289483,sid14\\_gci884696,00.html](http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci884696,00.html), Preventing SQL Injections

[http://searchsecurity.techtarget.com/tip/1,289483,sid14\\_gci526170,00.html](http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci526170,00.html), Implementing database security and integrity

[http://searchsecurity.techtarget.com/tip/1,289483,sid14\\_gci870023,00.html](http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci870023,00.html), SQL Server security

HSC HIPAA link

<http://www.uchsc.edu/hipaa/>

HIPAA online training instructions

<http://www.uchsc.edu/hipaa/uldi.htm>

Email best practices

<http://www.uchsc.edu/is/email/bestpractice.htm>

HSC Appropriate Use Policies (AUP)

<http://www.uchsc.edu/is/policies/>