**Information Security Checklist – For DAHS also located at med.unc.edu/ahs/research/security**

**This checklist, developed by the School of Medicine Information Security Office, is designed to be a high level list of items that will help improve information security in your environment. The list is intended to be a baseline and is certainly not all-inclusive. Questions about particular items can be sent to** **security@med.unc.edu****. This checklist is for DAHS researchers only – do not distribute to other departments. OIS will be developing an expanded version of this for the School of Medicine.**

**PC Desktops**

All DAHS machines are all supposed to be on the AD domain – this is a network setting that OIS should have come out and done in 2011 and 2012. If you are on the AD domain, #’s 1, 2 and #5 below are already taken care of. If you are not sure if you are on the AD domain, contact OIS.

1. Configured to automatically update Windows Security Patches
	1. Most machines are configured this way. Ask OIS Tech Support if unsure.
	2. If you are on the AD domain, this is done automatically
2. Symantec Endpoint Protection installed and configured for automatic updates
	1. Most machines are configured this way. Ask OIS Tech Support if unsure.
	2. If you are on the AD domain, this is done automatically
3. Always accept updates for third party applications such as Adobe Reader, Firefox, Thunderbird, Java, etc. If you are not sure if an update is legit or a ‘spoof’ please contact OIS
	1. Secunia PSI is a useful tool that can help with updates of most products we use. It can be found at: <http://secunia.com/products/consumer/psi/>
	2. \*\*Specific to DAHS – a new system called CSSM will be rolled out to DAHS (we are the first department to get it) – this will allow OIS to automatically manage ALL software updates.
4. Registered in AD Domain
	1. Ask OIS Tech if unsure
5. Password protected screen saver with automatic logout
	1. Logoff or screen lock when leaving the desktop: [instructions here](http://www.it.cornell.edu/security/howto/screenlockhowwin.cfm)
	2. If you are on the AD domain, this is done automatically
6. Do not configure any applications to store password locally.
7. Do not store sensitive information on local desktop.
	1. Definition of Sensitive Data: <http://help.unc.edu/6475>
8. Use network storage to store important data
	1. Network storage is normally mapped as a higher letter, such as the J drive. If unsure whether you have been assigned network storage, ask OIS Tech Support.
	2. If you need to sign up for network storage, contact OIS for details.
9. Iron Mountain backup installed for important local machines. This can be helpful if you store information on your local machine – note item #7 above about sensitive information. See Iron Mountain details here: <http://help.unc.edu/5662>

**PC Laptops:**

1. Encrypted with PGP Whole Disk Encryption – all laptops used in human subject research are required to be encrypted.
	1. Contact Lori\_Mahaney@med.unc.edu to have PGP installed
	2. Sensitive information can be stored on an encrypted laptop. Network storage is still recommended for backup purposes.
2. Configured to automatically update Windows Security Patches
	1. Most machines are configured this way. Ask OIS Tech Support if unsure.
	2. If you are on the AD domain, this is done automatically
3. Symantec Endpoint Protection installed and configured for automatic updates
	1. Most machines are configured this way. Ask OIS Tech Support if unsure.
	2. If you are on the AD domain, this is done automatically
4. Always accept updates for third party applications such as Adobe Reader, Firefox, Thunderbird, Java, etc. If you are not sure if an update is legit or a ‘spoof’ please contact OIS
	1. Secunia PSI is a useful tool that can help with updates of most products we use. It can be found at: <http://secunia.com/products/consumer/psi/>
	2. \*\*Specific to DAHS – a new system called CSSM will be rolled out to DAHS (we are the first department to get it) – this will allow OIS to automatically manage ALL software updates.
5. Do not store sensitive information on laptops unless they have been encrypted (see #1 above)
6. Do not configure any applications to store password locally.
7. Password protected screen saver with automatic logout.
	1. Logoff or screen lock when leaving the desktop: [instructions here](http://www.it.cornell.edu/security/howto/screenlockhowwin.cfm)
8. Iron Mountain backup installed for important machines. This can be helpful if you store information on your local machine – note item #7 above about sensitive information. See Iron Mountain details here: <http://help.unc.edu/5662>

**Macs: (Reference and detailed instructions:** <http://help.unc.edu/6409>)

In addition to the items above for desktops and laptops, Mac users should:

1. Make sure that your Mac is password protected.
2. Make sure all passwords are strong: [more info here](http://www.microsoft.com/security/online-privacy/passwords-create.aspx)
3. Download and install Symantec Endpoint Protection from [shareware.unc.edu](file:///C%3A%5CUsers%5Cschmidtd%5CAppData%5CLocal%5CMicrosoft%5CWindows%5CTemporary%20Internet%20Files%5CContent.Outlook%5CQSWLM2T9%5Cshareware.unc.edu)
4. Turn on the built-n firewall: <http://support.apple.com/kb/HT1810>
5. Update your Mac often. View Apple's article for instructions on how to run updates. (<http://www.apple.com/support/?artnum=106704>)

**E-mail:**

1. The campus email system has been approved for sending and storing sensitive information.
2. To send secure email to an address outside of the campus system, place the word Secure in parentheses at the beginning of the subject line. This will show you an example of your users will receive. Example Subject Line: (Secure) This is a sensitive message.
	1. Before sending an actual secure message, we recommend that you send a test secure message to an outside account, such as your Gmail or Hotmail account to ensure that you are doing it correctly.
3. Secure mail sent to on campus addresses does not need (Secure) in the subject.
4. Recipients of secure messages cannot submit an encrypted reply to the message. So, users should not ask the recipient to reply to the message.
5. Never open email attachments unless you know both the sender AND that the person intended to send it to you (this is also true for Instant Messages, if you don't know the sender or the intended, do not click on any links in an Instant Message).

**Server Management:**

1. If you are the systems administrator for your own server (typically running Windows 2008, Linux, Unix, etc.) and if that server is storing sensitive information, then it must be registered in the campus System Administration Initiative (SAI). Requirements for SAI can be found here: <http://help.unc.edu/CCM3_032197>
2. Most people do not need to manage their own server. Centralized services are available to provide most services that were provided by local servers. Using centralized services is typically far more cost effective and secure than “building your own”. If you have questions about central services, send an email to help@med.unc.edu and somebody will meet with you to discuss your needs.

**Memory Keys:**

1. Encryption required for sensitive information
2. Recommend using memory keys with built-in hardware encryption
	1. Kingston DataTraveler Vault Privacy: [more info here](http://www.kingston.com/us/usb/encrypted_security)
	2. IronKey: [more info here](http://www.ironprotector.com/?gclid=CLfS_afhprMCFRRynAodPSgA8w)

**External Hard Drives:**

1. Encryption required for storing sensitive information
2. Recommend using TrueCrypt (Free) to encrypt
	1. Contact OIS for details on how to set this up
3. CAUTION: Protect the password. The help desk will not be able to recover the data if the password is lost.

**Fax Machines:**

1. Fax machines that typically receive sensitive faxes should not be located in unattended public spaces or unlocked office areas.
2. Fax machines should be checked regularly for any faxes that might have been received.
3. Faxes should be removed from the machine as soon as possible.
4. Fax servers should not be left logged in while unattended. Passwords to fax servers should not be posted on or near the machine.

**Password Management:**

1. We recommend using a password management tool to safely manage the many passwords that most people must maintain. Two that have been used include:
	1. Keepass ([www.keepass.info](http://www.keepass.info)) – Free open source product with versions available for most platforms.
	2. Roboform ([www.roboform.com](http://www.roboform.com)) – Commercial product. Free version will allow up to 10 passwords. Commercial version costs about $10 per year.

**Cloud Storage and Cloud-based Applications:**

1. Cloud applications such as gmail, Google Docs, Dropbox, Mozy, Carbonite, etc. are not approved for storage of sensitive information, unless a signed Business Associates Agreement (BAA), approved by University Counsel, is in place.
2. Most of these services have not or will not sign a BAA. Iron Mountain is currently the only one that has signed.

**Physical security:**

1. Unencrypted sensitive information, whether paper or electronic, should be provided adequate physical security.
2. Items that require protection might include cameras, memory cards, photographs, memory keys, paper files, video and audio tapes, CDs, visitor logs, etc.
3. There are no written general policies that specify minimum physical security requirements for sensitive information. However, due diligence and common sense should prevail. Like information security, physical security should done in layers. Examples include:
	1. Locked file cabinet
		1. Who has access to the space?
		2. Are there emergency access procedures?
	2. Locked office space
		1. Do cleaning crews have unlimited access to the space?
	3. Card swipe building access
	4. Is the office off campus? Who else has access to the building?

**Business Associate Agreements (BAA):**

1. Before entering into any agreements with outside vendors or organizations to store, access, or process any of the University’s or Health Care System’s Protected Health Information, there must be a signed BAA in place which has been approved by the Office of University Counsel. Contact security@med.unc.edu for more information.