The Restricted Data Environment: Issues Relating to Network-Connected Clients

Last change: May 30, 2014

The most secure (and by far the easiest to manage) environment for using restricted data files is a standalone workstation: a computer with no wired, wireless, or dial-in/out network connectivity. However in certain circumstances a researcher might need to connect her/his workstation an institutional network to in order to access a resource such as a secure server.

This document suggests procedures for improving restricted data file security and integrity in a network-connected workstation environment. Restricted data applicants should be aware that maintaining security in a network environment is complicated and can require considerable technical skill and experience. Before formulating a restricted data plan that requires a network environment, be sure to consult your local network administrator.

Step 1. *Visit Data Products » Restricted Data*. This section of the HRS Web site provides background information for researchers who wish to obtain access to Health and Retirement Study restricted data. Be sure to review Developing a Data Protection Plan .

Step 2. *Think carefully about whether or not you really need network access*. Modern desktop computers are capable of supporting all but the most esoteric and complex statistical software routines. In addition, the plummeting cost of disk storage space makes it possible to maintain large (multi-terabyte) data structures on a local machine rather than a network server. It may well be that you do not need any network resources to analyze your restricted data. *The preferred environment for analysis of restricted data is a standalone workstation.*

Step 3. *Do some research on security issues relating to your workstation*. Begin by consulting your network administrator to determine the security strengths and weaknesses of the network. It would be useful for you to review one or more of the security references listed at the end of this section. Remember that a personal computer running Windows 7, Macintosh OS-X, or Linux/Unix is really a multiple-user system with **you** as the system administrator. As such you will need to acquaint yourself with a rudimentary knowledge of system management issues: password management, system backups, emergency recovery procedures, printer installation and management, security reviews, anti-virus/anti-adware software installation, local firewall configuration, intrusion detection.

Step 4. *Limit access from the network to the workstation*. The goal of this step is to reduce the attack footprint by minimizing exposure of local workstation resources to the network. *Access limitation* should include, but not be limited to the following actions:

1. Talk with your local IT support person about configuring your system so that you do not run programs with administrator privileges. Windows 7, Macintosh OS-X, and Linux/Unix systems will let you do this out of the box.

2. Remove or limit domain-user authentication to the workstation. Example: if a Windows workstation has a trusted relationship with the network Primary Domain Controller, it is possible for users other than the workstation's owner to login and use workstation resources. Make sure that if you can login as a domain user, others can't.

3. Make sure that local workstation resources are not shared across the network. Example: Windows 7 supports sharing of local folders with other users on the network. If permissions on these folders are not set properly, folder contents could be accessed by unauthorized users. In a Unix environment make sure that client mounted file systems are not visible across the network.

4. If other people must use this workstation (a bad thing), you will need to review directory and file permissions as well as encryption procedures in order to ensure that restricted data areas are protected. These users will also need to sign the *Supplemental Agreement with Research Staff for Use of HRS Restricted Data*.

5. Disable all Internet services on the workstation. This means that your workstation should not be acting as a Web server, FTP server, or peer-to-peer network node. It should also not support inbound telnet connections, UUCP connections, remote desktop connections, or network services such as RPC and NFS.

6. Disable any type of Web-active software that sends information about you and your local machine back to a central server (see Step 6, below).

7. Disable Voice Over IP (VOIP) software (**Skype** or **Vonage** or ...).

8. Disable any type of peer-to-peer network/media-sharing software (**BitTorrent** or **eDonkey** or **Gnutella** or **kaaza** or **iMesh** or **Limewire** or **Soulseek** or ...) that may be running on your workstation. Do not use social networks such as **Facebook, Linkedin,** or **MySpace**.

9. Keep your e-mail and instant messenger clients updated to minimize the possibility that they might provide an avenue for intrusion. **Don't open attachments emailed to you from unknown sources**. In fact, don't open any attachment unless you are absolutely sure of what it contains.

10. If you are using a Web browser, make sure that you limit the ability of Web servers to launch applications on your workstation. If you are using Firefox/Mozilla/Netscape, disable Java, Javascript, and Auto-install unless one of these features is absolutely required. You may also wish to install the NoScript and AdBlock Plus plug-ins. NoScript is quite useful since it lets you establish a whitelist of web sites for which you can enable Javascript. If you are using Internet Explorer upgrade to the latest version if you have not already done so. Set IE browser security options to their most secure level. For example, IE allows you to set security levels on unknown Internet computing sites to "High", limiting execution of active content.

11. Disable other forms of connectivity. Turn off all wireless capabilities for your desktop machine and any attached peripherals. If you have a modem attached to the workstation for FAX or dial-out use, disable it during the period when you are working with restricted data. Do not use the network printer; instead use a local printer that is not shared over the network.

12. Choose an approved workstation operating system: Windows 7 (Professional, Ultimate and Enterprise), Mac OS-X (10.4.x and above), and all flavors of Unix including Linux. When properly configured, these operating systems are approved for use with HRS restricted data in both standalone and networked modes. If you wish to use a Windows client as part of a domain, be sure to review your use of Encrypting File System services with your network administrator. If you have questions on this issue, contact the HRS Help Desk.

13. If your workstation is running any version of the Windows OS earlier than Windows 7, it should be updated. Data protection plans that reference versions of Windows earlier than Windows 7 will not be approved.

14. Do not use Web services such as Google Desktop (or Yahoo Toolbar or, even worse, fake spyware toolbars) that may expose your local resources to external users.

15. As a general note, HRS recommends the use of secured desktop systems with wireless access removed or permanently disabled. The use of laptop or tablet computers is strongly discouraged and will be approved only in extraordinary circumstances.

Step 5. *Install file and network encryption software.* By encrypting restricted data files that when they are not in use, you will make it almost impossible for an intruder to view/remove confidential data, even if the intruder is able to access your workstation. Look for software that uses a strong encryption scheme (static key size of 256 bits or more; public/private key size of 2048 bits or more) for file encryption. Be aware that encryption schemes based on 40 or 56 bit key sizes are not secure. Examples of software packages suitable for use in research environments that meet the strong encryption requirement are:

- Bitlocker Drive Encryption. You may find the Step-by-Step Guide for Windows 7 useful.
- Get Started with the Encrypting File System in Windows 7: Information from Microsoft Support on using EFS in Windows 7 (Professional and above). Once it is properly configured, EFS allows Windows users to enable encryption for any file or folder that resides on an NTFS partition. Once the encryption property is set for a folder, any file within that folder is automatically protected, and the encryption/decryption process is transparent to the user.
- PGP (Pretty Good Privacy) is available for all flavors of operating system; contact the Symantec Corporation.
- BestCrypt, from Jetico at http://www.jetico.com/: Data encryption packages for Windows and Linux environments.
- Check Point Software (http://www.checkpoint.com/products/full-disk-encryption/index.html): Source for full-disk encryption plus access control for PCs and laptops.

Step 6. *Install anti-virus software, anti-adware/malware software, and firewall software.* Your Internet connection serves as an excellent delivery system for malicious software. Although e-mail macro viruses with various payloads are currently in the news, hostile applications can be introduced into your computer system through any open IP port. Anti-virus software packages provide an additional line of defense against Internet intrusions. You should obtain, install, and keep current, an anti-virus software package suitable for your computing environment. If you plan to use restricted data on a network-connected workstation with Internet access, you must install firewall software on your workstation. Depending on your local environment, it may also be necessary for you to re-configure your LAN to provide hardware firewall protection. Contact your network manager and HRS for details. You may wish to visit the following Web sites for more information on anti-virus, anti-spyware, and firewall software products:

- http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml: Operating system configuration guidance from the National Security Agency
- http://safecomputing.umich.edu/antivirus/: Anti-Virus Protection at The University of Michigan
- http://isc.sans.org: *SANS Internet Storm Center*
- http://www.firewallguide.com: Home firewall guide, including software reviews

HRS Restricted Data Applicants: Any anti-virus, anti-adware, encryption, local firewall software (or hardware), network firewall configurations, and network intrusion detection systems that you employ should be documented in your Data Protection Plan.