DATE: April 9, 2008

TO: NIH Staff

FROM: Director, NIH

SUBJECT: Encryption and Data Security

This memo provides guidance on the DHHS policy on encryption and data security for all computers and portable electronic and data storage devices. It is critical that you read and save the entire memo.

Today we are faced with two conflicting realities: Technology has enabled us to work in remote locations, away from the office and at any hour. This puts at risk data that we work with on laptop computers and portable storage devices because they can be stolen or misplaced. We cannot change these realities, so we must do a far better job of protecting data contained on the devices.

The theft of an NIH employee's laptop computer in February with sensitive data on human subjects has placed renewed focus on the necessity of encrypting portable electronic devices. The stolen computer was not encrypted, in violation of a government policy. This was a serious violation of our commitment to protect the confidentiality of our patients. We are working with several NIH Institutional Review Boards to deal with the human subjects implications of loss of personal information, as well as with our IT community to protect confidential information.

Given the recent events, I ask each and every one of you to verify your compliance with the following requirements regarding data security. We will begin random audits to be sure of full compliance with this policy. It is important that we do everything possible to reassure the public and our patients that we all take our responsibility regarding protection of sensitive data from loss or misuse extremely seriously in an age of increasing sophistication in information technologies.

By DHHS policy, all DHHS laptop computers must be encrypted with an approved encryption software package. Portable media such as flash drives must be encrypted if they contain sensitive government data, including personally identifiable information (PII). The details of this policy and the definition of sensitive data, as well as helpful examples, are relayed below.

Encryption requires using a "Federal Information Processing Standard 140-2 compliant" whole-disk encryption package. Such encryption packages are available for the Microsoft Windows and Linux operating systems, and one is in the process of being approved for the Macintosh operating system. Given these limitations, this is what is required today:

Windows and UNIX -- All laptop computers with the Microsoft Windows or Linux operating system, regardless of the nature of the files contained within, must be encrypted with approved software, such as the PointSec encryption software. Windows Vista users can also use Microsoft BitLocker.

Exceptions are rare and require a waiver with justification signed by the NIH Chief Information Security Officer (CISO) and the DHHS CISO.

Macintosh -- Macintosh laptop computers cannot be used to store sensitive information including personally identifiable information, due to the lack of NIST-approved encryption software. Mac laptops can be used for sensitive data analysis, however, provided that the data are stored on an encrypted removable device, such as a FIPS compliant encrypted flash drive, and not downloaded to the hard drive. This policy will be reviewed once laptop encryption software is available for the Macintosh.

Mac laptops, for now, can be used to store non-sensitive data or data that is publicly available without names or other personally identifiable information. Note that Mac users privy to personally identifiable information via e-mail attachments must use NIST-approved software to securely delete and remotely archive these files. Details are provided below.

USB Drives (Flash Drives, Portable Storage) -- Personally identifiable information and other sensitive files can be kept only on portable media only if the media are encrypted.

MXI* biometric flash drives work with computers running Macintosh, UNIX or Windows operating systems. Windows users have other choices and should confer with their IC's IT office. NIH employees and contractors are allowed to use unencrypted flash drives, CDs and external hard drives for non-sensitive information only.

BlackBerrys -- All BlackBerry wireless handheld devices must be configured with an access password and other security features provided by the NIH Blackberry Enterprise Server. Anyone who loses a BlackBerry must report the loss immediately to the NIH Helpdesk; the NIH CIT can erase its data remotely. Though the current configuration is very secure, encryption on these devices will be enabled in the near future.

Other computers -- Never, ever use your personal computer or laptop for PII or government information. Even for encrypted government computers of any type, insofar as possible, only coded data should be stored on the device and the code itself be kept safely elsewhere.

In addition to these requirements, any NIH employee or contractor who loses an NIH-issued laptop computer must report the loss within one hour to the NIH Helpdesk (301-496-4357; helpdesk@nih.gov). Any other suspected or confirmed loss of personally identifiable information must also be reported to the NIH Helpdesk within one hour.

A note on sensitive information: Information is considered sensitive if the loss of confidentiality, integrity, or availability could be expected to have a serious, severe, or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

For a more thorough definition, as well as an appreciation for protecting data, refer to the document "NIH Guide for Identifying Sensitive Information" at http://irm.cit.nih.gov/security/NIH_Sensitive_Info_Guide.doc <http://irm.cit.nih.gov/security/NIH_Sensitive_Info_Guide.doc>

Examples of sensitive data include:
* Social security numbers,
* Patient and medical information,
* Contents of employee invention reports prior to submission of a patent application,
* Correspondence that includes proprietary information,
* Grant applications, or
* Manuscripts that have not yet been submitted whose contents have not been publicly presented.

Non-sensitive data might include:
* PowerPoint slides that have been or are about to be publicly presented,
* Material, such as resumes whose contents are available publicly, such as on a website,
* Correspondence without sensitive information that also does not include personal identifiers,
* Laboratory data that will not be used to support an employee invention report, or
* Manuscripts whose contents are not the subject of an employee invention report and whose contents have been publicly disclosed in a lecture or other forum.

A note on encryption: As with many new technologies, encryption works best with newer computers, with faster processors and generous memory. The NIH Help Desk and your desktop support personnel have considerable experience with nearly 11,000 encrypted laptops already at NIH and will be able to install the encryption software and help troubleshoot any issues.

A note on portable devices: The NIH CIT has provided a list of FIPS-certified portable devices approved for the storage of sensitive material at <http://irm.cit.nih.gov/nihsecurity/FIPS_Certified_USB_Drives.doc>.

A note on e-mail encryption: To transmit sensitive information in e-mail, always use approved encryption, either using NIH secure e-mail or for an attachment, using FIPS-certified encryption. If you need a secure e-mail account, please contact the NIH Help Desk. If you receive unencrypted sensitive information via e-mail on an unencrypted laptop computer, you should either mail it to yourself using secure mail or move that information to a FIPS-certified encrypted USB drive. The unencrypted information should be deleted from your mail and unencrypted computer immediately. You should also contact the individual who sent it to let them know the proper method for sending sensitive information.

Encryption technology has its limitations, yet it improves with each passing month as the reality of computer theft and identity fraud settles across the varied disciplines of science and health, defense, and finance. The DHHS is working with the key players in this technology, such as those at Microsoft and Apple, to develop products that ensure data security without compromising computer and employee performance.

As the premier biomedical research institution in the world, the NIH is in the spotlight. We require 100-percent cooperation from you on this issue.

Elias Zerhouni, M.D.