VOLUME 1, ISSUE 2

THE NIH EYE ON PRIVACY

OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

APRIL 2008

INSIDE THIS ISSUE

CALENDAR OF EVENTS

PIA Training:

April 17, 22, 28 and 29

May 7 and 23

10401 Fernwood Road
Lower Level Classroom
Room 1NW-02
Bethesda, MD 20817

CIT Online Training:

http://training.cit.nih.gov

Keyword search: PIA

Privacy Coordinator Group Meeting:

April 30, 9:30–11:30 a.m.
Building 31, C Wing
6th Floor
Conference Room 6

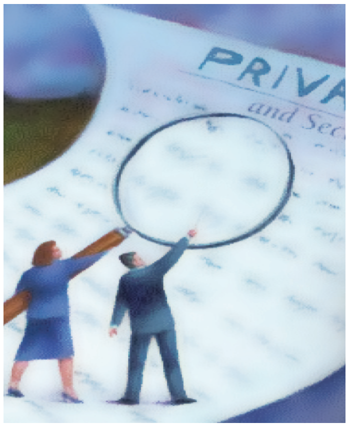
PRIVACY PRACTICE: RECENT PRIVACY INCIDENT

This month, NIH made the front page news of *The Washington Post*. A Government laptop computer issued to an NIH employee was stolen from his car. The laptop contained unencrypted clinical trial data, including the names, medical diagnoses and details of patient heart scans for more than 3,000 patients.

This incident is a serious violation of NIH computer security and acceptable use policies as well as standard computer security practices. Appropriately, it is of utmost concern because NIH policy requires that all NIH laptops be encrypted. In addition, all mobile devices and portable media that contain sensitive NIH or HHS agency data must be encrypted. 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, assets, or individuals.

In accordance with the Privacy Act of 1974, as amended (5 U.S.C. § 552a), we are required to ensure the security and confidentiality of data contained in systems of records and to protect the security and integrity of those records against threats or hazards. The Privacy Act applies to all data stored in paper format and on all computers, regardless of the operating system used on the computer (Windows or Mac).

At this time, Macintosh laptops are waived from the encryption requirement because there is currently no encryption software for the Mac that complies with HHS policy. This includes File Vault, the native Mac encryption software. Thus, the encryption waiver under which Mac laptops currently operate, DOES NOT ALLOW the storage of personally identifiable information (PII) or sensitive and Privacy Act protected data. There are no exceptions to this policy. New, federally compliant software to encrypt the Mac is in development. When it is available, all personally identifiable information on Macs must be encrypted.



This unfortunate incident highlights the importance of ensuring the integrity, privacy and security of PII, sensitive and Privacy Act protected data.

Karen Plá
NIH Senior Official for Privacy

Personal Identifiable Information (PII) Protection Policies can be found at: http://irm.cit.nih.gov/security/PIIProtection.html.

For the most recent *Washington Post* article regarding the breach, please visit: http://www.washingtonpost.com/wp-dyn/content/article/2008/04/09/AR2008040903680.html.

NIH PRIVACY AWARENESS TRAINING—COMING SOON!

Frequent privacy breaches have prompted increased Federal privacy training requirements. To help educate you on how to protect privacy, we will launch NIH Privacy Awareness Training in two phases (first to those who have Privacy Act responsibilities and later, to remaining employees and contractors). We will announce training in the *NIH Record* and our May issue!

Let's say you're an NIH scientist who uses a Macbook. You are asked to speak at an upcoming conference. In preparation, you move patient research data from the secure server on which it's stored, to your Macbook to take with you, *in violation of HHS and NIH policy.* While waiting to board your flight, the Macbook is stolen.

There are a dozen thoughts that *should* be racing through your mind about whether you properly safeguarded the information you were entrusted to protect, and whether you have now exposed yourself to legal liability. NIH Privacy Awareness Training will provide valuable knowledge of your responsibilities to protect all forms of personally identifiable information, whether it belongs to an employee, grantee, or patient of the NIH. You will also hear about what you can do in the event of a breach of data to mitigate the risk of harm to individuals whose information has been compromised.

It is the responsibility of each and every employee to protect the privacy of the individuals whose information we collect, store, use, maintain and disclose, and to comply with all applicable laws, regulations and policy.

We look forward to rolling training out to you where you will learn about the Privacy Act, federal statutes relevant to privacy, roles and responsibilities, PIAs and more! Stay tuned!

QUESTIONS, COMMENTS, SUGGESTIONS? EMAIL US AT: PRIVACY@MAIL.NIH.GOV

We are on the web!

http://oma.od.nih.gov/ms/privacy

The Office of the Senior Official for Privacy serves as the chief NIH privacy governance entity whose mission is to ensure the highest level of scientific integrity, public accountability, and social responsibility in the area of privacy management.

NIH Office of Management Assessment

6011 Executive Blvd, Suite 601

Phone: (301) 451-3426

Fax: (301) 402-0169

Email: privacy@mail.nih.gov

TRAINING: PRIVACY IMPACT ASSESSMENTS

Calling all IT System Owners/Managers, IC Privacy Coordinators, ISSOs, IT Administrators (networks, servers, databases), Webmasters/Administrators, OMB Project Clearance Liaisons and other NIH staff involved in the Privacy Impact Assessment (PIA) process! Do you know about the responsibility to complete PIAs for all NIH IT systems? Are you new to NIH? Join us for training that will be offered in the coming weeks on conducting PIAs on IT systems. *Completion of Privacy Impact Assessments (PIAs) using the HHS Security and Privacy Online Reporting Tool (SPORT)* will provide an overview of the HHS requirement to conduct a PIA on IT systems, how to access and use the online reporting tool called SPORT, and how to complete a PIA. This will be an informative opportunity to ask questions related to PIAs and NIH privacy requirements, and network with others across NIH with similar responsibilities. For dates and locations, please see the Calendar of Events on Page 1.

Privacy Points of Contact

Find contact information for NIH IC Privacy Coordinators at the following site: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

SPOTLIGHT ON OMB MEMOS

There are two OMB memos commonly cited for privacy training requirements for agency employees. To learn more about NIH Privacy Awareness Training, see Page 1. OMB memo M-05-08 *"Designation of Senior Agency Officials for Privacy"* establishes the Senior Agency Official for Privacy role and responsibility to ensure that all employees of the agency receive appropriate privacy awareness training (http://www.whitehouse.gov/omb/memoranda/fy2005/m05-08.pdf, Paragraph 4). Additionally, OMB memo M-07-16 *"Safeguarding Against, and Responding to the Breach of Personally Identifiable Information"* reminds agencies of their requirement to provide appropriate security and privacy awareness training prior to granting access to agency information and IT systems (http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf, Attachment 1, Section 2(d)).

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

IN THE NEWS—PRIVACY GROUP AIMS FOR MODEL STATE LAW

From Government Health IT
By Brian Robinson
February 24, 2008

A multistate collaborative seeking ways to align its health information privacy rules to make it easier to share data across health information exchanges is aiming for a demonstration law that states could use as a model in 2009.

The target for the Harmonizing State Privacy Law Collaborative (HSPLC) this year is to develop a set of priority recommendations for reforming state laws, with the goal of producing a 2009 demonstration law, officials said.

The HSPLC is a working group operating under the Health Information Security and Privacy Collaboration (HISPC), a project sponsored by the Health and Human Services Department to investigate ways of dealing with privacy and security issues associated with HIEs. "Federal solutions [for interstate privacy] are not inevitable, despite some good proposals," said Carolyn Turner, a contract manager with Florida's Agency for Health Care Administration, and a HISPC project manager. "And there are still issues at the state level" that need to be addressed.

For the complete article, click: http://www.govhealthit.com/online/news/350234-1.html.

Did You Know?

According to the Federal Times, nearly 13,000 incidents were reported in which sensitive information on computer systems may have been compromised in federal agencies last year, more than double that of the previous year.

QUESTIONS, COMMENTS, SUGGESTIONS? EMAIL US AT: PRIVACY@MAIL.NIH.GOV