



THE PRIVATE EYE

OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

MARCH 2008

INSIDE THIS ISSUE

DIRECTOR'S CORNER	1
DE-MYSTIFYING PRIVACY LINGO	1
IN THE NEWS	2
SPOTLIGHT ON OMB MEMOS	2
UNDERSTANDING NEW LEGISLATION	2
PRIVACY POINTS OF CONTACT	2
DID YOU KNOW?	2

CALENDAR OF EVENTS

- 2008 American Society of Access Professionals (ASAP) 1st National Training Conference: 3/4-3/6/08, Lake Buena Vista, FL, www.accesspro.org
- International Association of Privacy Professionals (IAPP) Privacy Summit: 3/25-3/28/08, Renaissance Washington D.C. Hotel, <https://www.privacyassociation.org>
- Privacy Coordinator Group Meeting: 3/26/08, 9:30-11:30 am, Executive Plaza North (EPN), Conference Room G

DIRECTOR'S CORNER: STATE OF THE PRIVACY PROGRAM

Every day you safeguard your privacy. You may not even realize you are doing it, but undoubtedly, you protect your wallet, shred mail that may carry personal information about your identity, and secure your computer with a password. Protecting your own privacy is an essential part of your life.

Protecting the privacy of NIH employees, patients, grantees and visitors to our campus is *the* essence of the Office of the Senior Official for Privacy. It is our business to ensure that your privacy, and the privacy of those with whom we do business, is protected. We protect your privacy through education and

training, assessing the impact of privacy on information technology, responding to OMB and HHS data calls, working with privacy points of contact in the ICs, training them on their roles and responsibilities, reviewing Departmental privacy policy and issuing NIH privacy policy and guidance.

In keeping an eye on privacy, we help to sustain the NIH mission. If the personal privacy of the people we aim to protect is breached, the ability of NIH to engage in ground-breaking research is compromised. Additionally, a privacy breach could conceivably damage the reputation of NIH, cost

thousands to millions of dollars to remedy, and erode the public's trust and confidence in our ability to protect personal information.

It is our hope that this monthly newsletter will provide you with much needed privacy information and answers to your questions. Please do not hesitate to contact us by email at: privacy@mail.nih.gov or by phone at (301) 451-3426.

Your privacy is important to us...



DE-MYSTIFYING PRIVACY LINGO

Privacy terms can be confusing. Each month we will focus on a variety of terms to help you make sense of the "lingo."

This month, we feature three interrelated, often misused terms.

When confused about privacy terms, policies or procedures, please do not hesitate to

email us or contact your IC Privacy Coordinator.

- **Privacy:** Freedom from unauthorized and unwarranted intrusion. Personal data should be kept private.
- **Security:** Measures taken to limit access to

information and protect it from attack or theft. Data can be secure, but not private.

- **Data Integrity:** Assurance of reliability and accuracy of information. Data can be private and secure, and yet have no integrity.

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

IN THE NEWS: PRESIDENTIAL DIRECTIVE



President Bush recently signed a directive (classified and not available for public viewing) which expands the role of computer network monitoring within all federal agencies. The purpose of the directive is to protect government networks from cyber attacks. The directive authorizes the intelligence agencies, namely the National Security Agency, to monitor internet activity, email content, and investigate intrusions in federal networks. Received with controversy, some feel

that NSA, as an intelligence gatherer for foreign entities, should not monitor the U.S. government networks. Policy debates over government authority over the Internet are likely to ensue.

SPOTLIGHT ON OMB MEMOS

The Office of Management and Budget recently released a memorandum (OMB M-08-09: New FISMA Privacy Reporting Requirements for FY 2008) which states that Federal agencies will be responsible for reporting annually new privacy information under the Federal Information Security Management Act (FISMA). The new reporting requirements will include privacy reviews, information about advice provided by the Senior Agency Official for Privacy, the number of written complaints for privacy issue allegations and other comprehensive privacy and security data. The memo can be found at: <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-09.pdf>.

UNDERSTANDING NEW LEGISLATION

The U.S. House of Representatives has proposed a bill (H.R. 4791) entitled the Federal Agency Data Protection Act, which would amend some of the privacy and information security provisions of the E-Gov Act. Currently, Title II of the E-Gov Act and OMB require the completion of privacy impact assessments (PIAs) prior to developing or procuring information technology systems that collect, maintain, or disseminate personally identifiable information (PII). To learn more about the E-Gov Act, see:

<http://www.whitehouse.gov/omb/egov/g-4-act.html>.

If passed, the bill will:

- Give OMB authority to establish information security policies and procedures;
- Outline Federal agency responsibility for information security, including notification;
- Require agencies to develop and implement plans that include protection of data from risks posed by peer-to-peer file sharing;
- Require an independent

annual audit of agency security procedures rather than the current "evaluation";

- Require agencies to assess the privacy impact of their use of commercial information services (aka "data brokers") that use personal information;
- Prohibit certain contracts with such data brokers; and
- Authorize appropriations for E-Gov activities through FY 2012.

We'll keep you posted.

Privacy Points of Contact

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



U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES
National Institutes of Health

Did You Know?

There are *9 million* identity theft victims in the United States each year, according to the Federal Trade Commission.

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