The NIH Eye on Privacy

August–September 2008 Volume 1, Issue 5 Office of the Senior Official for Privacy

Inside this Issue

Note from the Senior Official 1
Survey 1
Awareness Training 1
In the News 2
Spotlight on OMB Memos 2
ISSO Corner 2
Privacy Points of Contact 2

Calendar of Events

Privacy Coordinator Group (PCG) Meeting

August 27, 9:30–11:30 a.m.
Building 31, C Wing, 6th Floor
Conference Room 6

September 24, 9:30–11:30 a.m.
Executive Plaza North (EPN)
Conference Room H

Privacy Management Committee (PMC)

August 20, 1:00–2:00 p.m.
6011 Executive Boulevard
Suite 601, Room 647B

September 17, 1:00–2:00 p.m.
6011 Executive Boulevard
Suite 601, Room 647B

Note: Effective in October, we will alternate the schedule of both meetings to be held every other month (PCG begins November, PMC begins December).

Navigate—IAPP Forum

August 18–20, 2008

A forum of privacy leaders coming together to think differently, ask questions, challenge beliefs and drive consensus—shaping the future of privacy. Moderated by Jonathan Zittrain and John Palfrey of Harvard's Berkman Center for Internet and Society. Two days by the sea with room to think…More information coming soon.

IAPP Privacy Academy

September 22–24, 2008
Orlando, FL

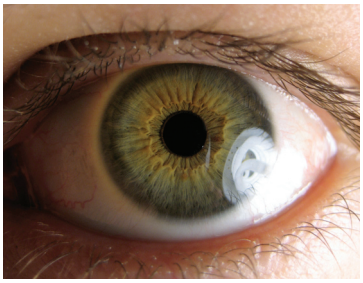
Please see the IAPP web site for details: https://www.privacyassociation.org.

Introducing the HCG Information Security Committee

Information security is in the forefront of everyone's mind today, and the NIH Human Capital Group (HCG) Information Security Committee is working hard to keep the OD well informed. The HCG Information Security Committee is led by Tim Newman, Chief of the Core Systems Branch in the Strategic Programs Division and consists of staff from all HCG divisions and our office in OMA, OM, OD. The committee was established in September 2007 to ensure that the HCG serves as a model of excellence in information security practices as it relates to human resource records. The HCG manages volumes of very sensitive and private employee and organizational information, so how this information is handled is of critical importance to both the HCG and NIH communities. As part of its charge, the HCG Information Security Committee is in the process of developing policy, standard operating procedures (SOPs) and related educational information for employees and managers. The HCG Information Security Committee will be featured in the September edition of the HR Systems Spotlight newsletter. Information security will be an important part of that article. Please be on the lookout for that newsletter. Meanwhile, to view information about the HCG and other information on the HR portal community, please take a look at: http://hr.od.nih.gov/About/HCGInfoSecurity/default.htm.

Karen Plá, NIH Senior Official for Privacy

Survey: What's your eye on privacy?



Check out our new look! Please let us know your thoughts on the *NIH Eye on Privacy* via email: privacy@mail.nih.gov.

- How do you use the newsletter?
- What are your favorite and least favorite features of the newsletter?
- Do you forward the newsletter, and if so, to whom?
- How could the newsletter be improved?

NIH Privacy Awareness Training Reminder

This mandatory online training course is packed with useful information and downloadable resources on:

- The Privacy Act
- Federal Statutes
- Roles and Responsibilities
- Privacy Impact Assessments

The course is available at:
http://irtsectraining.nih.gov

Visit the website URL listed above to log onto the left side of the screen as an NIH staff member and complete the course prior to the deadline established by your IC. If you log on to the right side of the screen as a General Public User, your progress will not be tracked by the system. The course will take approximately 30–60 minutes to complete. If you are short on time, you can disable the audio. Note: Although recommended, modules 1 and 6 are not tracked by the system and are not required in order to obtain a certificate of completion. To check to see whether you already completed the course, you can go the page that lists all of the security and privacy courses and click on the button to View Your Student Record.

The NIH Eye on Privacy

August–September 2008 Volume 1, Issue 5 Office of the Senior Official for Privacy

In the News…

Medical Identity Theft: Your Money or Your Life

By Allan Pomerantz, posted in *Cybercrime* on June 19, 2008

http://www.bloginfosec.com/2008/06/19/medical-identity-theft-your-money-or-your-life/

What could be worse than ID theft of your financial identity? After all, you could lose thousands of dollars, spend days on the phone with financial institutions, credit bureaus, and merchants. Your interest rates could climb on your credit card debt due to the practice of "universal default" used by credit card companies which means that all creditors can raise your rates based on one reported late payment. You might even be turned down for insurance or even a job. So is this as bad as it can get?

Unfortunately, the answer is no. The above issues can cause you financial pain while medical identity theft can cost you your life, hence the old robber's ultimatum—your money or your life.

Medical identity theft is a growing, if under reported problem. But what makes it so serious? As we move to electronic medical records, think of the impact of someone posing as you having their medical records entered as yours. If you were rushed to the hospital unconscious, you could die from being given the wrong blood type. Or you could have needed medicine withheld because of an allergy you don't have. It can also cut the other way. For example, you may be in diabetic shock, but you records don't indicate you have diabetes.

With over 40 million people in the United States without medical insurance, this is a crime even honest (but desperate) people will commit. Further, it is probably much more difficult to correct this type of ID theft than financial ID theft because there are no central reporting authorities such as the credit bureaus. There are some signs that at least the bigger medical providers are becoming alert to the problem because they now ask for proof of identity, usually via a driver's license but these are easily forged.

There are a few things that you can do to protect yourself. First, read all EOBs (Explanation of Benefits) you receive from your health insurance company. Guard your health insurance card like your credit card. Beyond that, we must depend on our health care providers for protection.

Spotlight on OMB Memos

Revised reporting instructions have recently been released by OMB as memorandum (M) 08-21, "FY 2008 Federal Information Security Management Act (FISMA) and Agency Privacy Management." There are several changes to note from last year's instructions (OMB M-07-19). Some of the changes include, but are not limited to, security and privacy policy related to OMB Memorandum M-07-16, of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." The FY08 Memo requires that NIH provide in an appendix to its annual report, the following items:

- Breach notification policy;
- Implementation plan and progress update on eliminating unnecessary use of SSNs;
- Implementation plan and progress update on review and reduction of holdings of PII; and
- Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules.

Read the new reporting instructions at http://www.whitehouse.gov/omb/memoranda/fy2008/m08-21.pdf

Here's a good GAO report and news article for reference on the requirement for laptop encryption:

GAO-08-525, *Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains,* June 2008. Full Report: http://www.gao.gov/new.items/d08525.pdf.

ISSO Corner

The CIO Council is sponsoring the 2008 Federal IT and Privacy Summits October 22–23, 2008. The IT and Privacy professional training will bring together hundreds of Federal IT and Privacy professionals who strive every day to strategically, efficiently and effectively use IT to serve and protect the public, including serving as stewards of one of the Federal Government's greatest assets, the public's personal information. Come to one or come to both! The event is free! Registration will begin in September 2008. Visit http://www.cio.gov to learn more!

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

U.S. Department of Health and Human Services
National Institutes of Health

For more information about the OSOP, the Privacy Act, PIAs and privacy at NIH, please visit us at: http://oma.od.nih.gov/ms/privacy
To obtain more information about IT security at NIH, please visit: http://www.cit.nih.gov/security.html