VOLUME 1, ISSUE 4

THE NIH EYE ON PRIVACY

JUNE–JULY 2008 OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

INSIDE THIS ISSUE

PRIVACY PRACTICE	1
HELP PROTECT PII	1
PRIVACY AWARENESS TRAINING	1
IN THE NEWS	2
SPOTLIGHT ON OMB MEMOS	2
ISSO CORNER	2

PRIVACY PRACTICE: EMAIL ENCRYPTION—YES, NO, MAYBE SO?

As many of you know, the requirement to protect Personally Identifiable Information (PII) is tightening, not loosening. Email is not currently a secure means of communicating PII, Sensitive and/or Privacy Act protected data. What does one do when needing to communicate this type of data?

First, you need to know that PII cannot be disseminated unless it is encrypted, ever! Second, you need to conduct a local, risk-based assessment as to whether PII should be sent via email; i.e., does your IC want to assume the risk of losing it or having it fall into the wrong hands? Do you personally want to assume that risk? Assuming you've determined PII will be sent via email, you must encrypt it. How can you do that?

If you wish to send encrypted email internally within HHS, the only available solution is to acquire an HHS Public Key Infrastructure (PKI) certificate. It allows you to encrypt and digitally sign email and exchange it with other HHS staff who also have a PKI certificate. If you were issued a certificate prior to May 30th, it will work through September 30th. If you don't yet have a certificate, expect a new process from HHS shortly on how current users can renew their certificates, and new users can obtain one. HHS PKI info can be found at: https://www.pki.hhs.gov/hhspki/home/how_to_guides.htm#quick.

There is no great solution at this time to send encrypted email outside of HHS. Phone calls are the only secure way to communicate data that are personally identifiable in form. Although not officially in full production at NIH, you can sign up to receive an account and test an

encryption service at https://secureemail.nih.gov.

Another alternative is a commercially available product called SecureZip. A free trial version of Secure Zip, as well as licenses, is available through PKWARE at www.securezip.com.

Still have questions? FAQs on encryption can be found at http://cit.nih.gov/Support/FAQ/EncryptionFAQ/default.htm

Karen Plá
NIH Senior Official for Privacy

CALENDAR OF EVENTS

Privacy Management Committee (PMC)
July 16, 1:00–2:00 p.m.
6011 Executive Boulevard
Suite 601, Room 647B

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

HELP PROTECT THE PII OF THE SUMMER INTERNS YOU HIRE

It's that time of year! Students are flooding into the NIH Summer Internship Program in Biomedical Research. To register students and prepare them for their internship, IC Summer Student Program Coordinators will be asking students to provide their date of birth, home address, social security number, banking information, and home/cell telephone numbers. Without these pieces of information, students will not receive payment and the information needed to ensure they have a successful internship. All of the data elements mentioned above constitute Personally Identifiable Information (PII) and must be protected whether the data is stored in a computer, received in paper form via the mail system, or received via email. After the information is collected and used for its intended purpose, only that information which needs to be retained for business purposes should be kept. Remember: PII cannot be stored on a laptop nor sent out via email unless encrypted. If you are an IC Summer Student Program Coordinator and have questions about PII and the importance of protecting it, please talk with your IC Privacy Coordinator listed here at: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

NIH PRIVACY AWARENESS TRAINING

New Training Class!

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

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

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

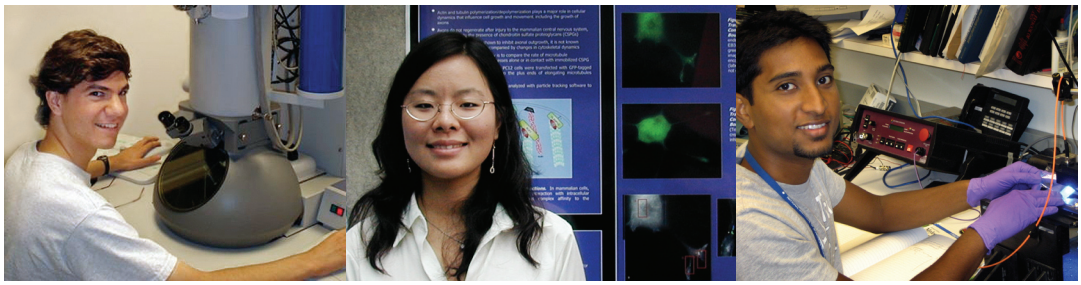
Next month, you'll be contacted by your IC to ask that you complete the course this summer!

Remember:

Inspect. Don't suspect.

Do not assume PII is protected.

Inspect your records system or IT system.



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

VOLUME 1, ISSUE 4

THE NIH EYE ON PRIVACY

JUNE–JULY 2008 OFFICE OF THE SENIOR OFFICIAL FOR PRIVACY

IN THE NEWS

Proliferating HIPAA complaints and medical record breaches
Sue Marquette Poremba
May 23, 2008, *SC Magazine*

The number of complaints regarding violations of the U.S. Health Insurance Portability and Accountability Act (HIPAA) continue to increase each year in tandem with an increase in breaches of medical records, according to one security professional.

In addition, a growing number of these complaints are going unresolved.

The protected health information (PHI) security and privacy goals of HIPAA in spirit and intent are good, Herold, leader of the Realtime IT Compliance Community, told *SC Magazine* on Friday. The regulatory oversight of the U.S. Department of Health and Human Services (HHS), however, has been underwhelming, she said.

The statistics provided about Privacy Rule complaints clearly show the numbers increasing on an annual basis, she added. This is a result not only of the growing numbers of privacy breaches, but also of the public's growing awareness of the risks involved with PHI breaches, and the fact that covered entities clearly have a law requiring them to protect PHI, but it is a law that is not being enforced. Read more: http://www.scmagazineus.com/Proliferating-HIPAA-complaints-and-medical-record-breaches/PrintArticle/110555/

SPOTLIGHT ON OMB MEMOS

OMB Memo 08-09:

Released in January 2008, this memorandum outlines new Federal Information Security Management Act (FISMA) privacy reporting requirements for FY 2008. This memo allows agencies to begin preparation to report on some of the following privacy areas:

- Number and type of privacy reviews conducted
- Information about the advice provided by the Senior Agency Official for Privacy
- Number of written complaints for each type of privacy issue allegation received by the Senior Agency Official
- Alleged privacy violations
- Number of complaints the agency referred to another agency with jurisdiction

Read more: http://www.whitehouse.gov/omb/memoranda/fy2008/m08-09.pdf

CHECK OUT:

"The Beginner's Guide to 508 Compliance or How to Make Your Website More Accessible to Everybody in Eight Easy Steps." http://www.nih.gov/catalyst/2008/08.05.01/page5.html

OnGuardOnline.gov provides practical tips from the federal government and the technology industry to help you protect against Internet fraud, secure your computer, and safeguard your personal information. Visit http://onguardonline.gov

ISSO CORNER: COMPLETE SECURITY AWARENESS TRAINING BY JUNE 30

FY-08 Computer Security Awareness Training is mandatory for all HHS/NIH users who use a computer connected to the HHS/NIH network.

Remote Access Training is required for all Remote Access users (Parachute and VPN) and covers proper use of remote access and the dangers of having an unprotected computer. *Note that this course is only required if you use VPN or Parachute.*

Both courses are located at http://irtsectraining.nih.gov/. You can verify if you have taken training by entering your NIH Badge number and looking at the "Completed" line next the name of the appropriate course.

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

NIH Office of Management Assessment

6011 Executive Boulevard, Suite 601
Phone: (301) 451-3426
Fax: (301) 402-0169
Email: privacy@mail.nih.gov

Tip of the Month:

If you don't need it, don't keep it!

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