



Online Privacy Resources

NIH Privacy Page:

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

NIH Information Security & Privacy Awareness Training:

<http://irtsectraining.nih.gov>

NIH IT Privacy Program Policy:

<http://www3.od.nih.gov/oma/manualchapters/management/1745/>

NIH Privacy Impact Assessment Policy:

<http://www3.od.nih.gov/oma/manualchapters/management/1745-1/>

NIH Web Page Privacy Policy:

<http://www3.od.nih.gov/oma/manualchapters/management/2805/>

SPORT Help Desk:

secureone.hhs@hhs.gov

Secure One HHS Intranet:

<http://intranet.hhs.gov/infosec/>

Secure One HHS PIA Website:

<http://www.hhs.gov/pia/nih/index.html>

Office of Management Assessment
6011 Executive Blvd, Suite 601
Rockville, Maryland 20892-7669
Phone: (301) 451-3426
Email: privacy@mail.nih.gov

Office of the NIH Senior Official for Privacy (OSOP)

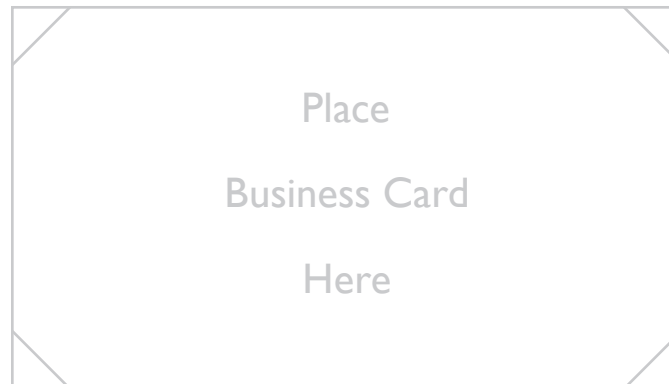
The OSOP serves as the NIH privacy governance entity whose mission is to ensure the highest level of scientific integrity, public accountability, and social responsibility in the area of privacy management.

Privacy Coordinator Group (PCG)

The PCG serves as a forum in which the NIH Senior Official for Privacy (SOP) can ensure that IC Privacy Coordinators are aware of evolving privacy requirements, the NIH Privacy policies, and their roles and responsibilities with respect to privacy implementation. The PCG also allows Privacy Coordinators to discuss privacy implementation strategies within their respective ICs.

Privacy Management Committee (PMC)

The PMC serves as a management entity, providing oversight to the PCG in all issues related to privacy and ensuring that ICs are aware of evolving privacy requirements, NIH privacy policies, and their roles and responsibilities with respect to privacy implementation. The PMC also provides direction and strategy for the future of privacy at NIH.



Protecting Privacy at NIH



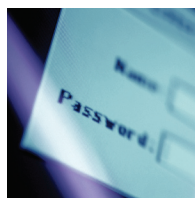
U.S. DEPARTMENT OF HEALTH
AND HUMAN SERVICES
NATIONAL INSTITUTES OF HEALTH

Privacy at NIH: What It Means To You

Privacy means different things to different people. It is vital to understand the significance and importance of privacy in our environment. This brochure arms you with information that is most important to protect your privacy, and the privacy of those whose personal information has been entrusted to NIH.

▶ **Ignoring privacy can cost you.** If ignored, NIH employees and research participants can be put at risk of identity theft. In addition, civil remedies and criminal penalties can be assessed for Privacy Act violations.

▶ **Protect all of your passwords.** Do not share them or store them in a vulnerable location.



▶ **Think before you email.** Email is not a secure communication vehicle, so please use discretion when emailing and receiving information internally and externally.

▶ **Be mindful of what you are accessing.** Know the type and amount of information to which you have access.

▶ **Secure your data.** Ensure that all computers containing PII and all mobile devices (e.g., memory sticks, disks, CDs) are encrypted.

▶ **Handle information with care.** Comply with policies for physical transportation of information, retention, and disposal of data.

▶ **Collect and keep only what you need.** You should not be collecting or keeping personal information from individuals unless you have a valid business need to collect/use/store it.

▶ **Report all breaches immediately.** All confirmed and suspected breaches should be reported to supervisors and your ISSO upon discovery.

▶ **Destroy all non-pertinent information.** Individuals should contact their IC Records Liaison regarding the planning, controlling, directing, organizing, training, promoting, and managerial activities related to the creation, maintenance and use, and disposition of records. Your IC Records Liaison can be found at the following link: <http://oma.od.nih.gov/ms/records/contact.html>

Did you know?

The Federal Trade Commission reports there are approximately **10 million identity theft victims** in the U.S. each year.



What should you do if you suspect a privacy incident or breach?

Contact your IC ISSO!
<http://irm.cit.nih.gov/nihsecurity/scroster.html>

Need to find your IC Privacy Coordinator?

Use the following site! http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

Spotlight on Frequently Used Terms

▶ **Personally Identifiable Information (PII):** Any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records.

▶ **Privacy Act Records System:** A group of more than one record (paper or electronic) which contains information about an individual and is designed to be retrieved by a name or other personal identifier assigned to that individual.

▶ **Privacy Impact Assessment (PIA):** A process for IT security and privacy professionals to assess whether privacy policies, procedures, and business practices, as well as applicable administrative, technical and physical security controls, have been implemented to ensure compliance with federal privacy regulations.

▶ **Incident:** A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.