



This is a reminder to take the Annual Privacy Refresher training! The course is mandatory.

Completion Date: June 21, 2013 (or earlier, as determined by IC)

- Visit <http://irtsectraining.nih.gov/> (go thru NIH Login)
- Enter the NIH ID number from the back of your HHS badge (ex. 012-3456-789)
- Login to take the 2013 Annual Privacy Awareness Refresher

Privacy Awareness training provides you with valuable information about your responsibility to secure NIH resources and protect all forms of personal information, whether it belongs to you, a member of the public, grant applicant, or a research study participant.

Last 4 Digits of a Social Security Number Are Personally Identifiable

Office of Management and Budget (OMB) Memorandum (M)-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, defines PII as “information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information.”

It is rare to find a SSN without some other identifier linked to it. Therefore, any use of the SSN (to include masking) is considered PII. The full or partial SSN can increase the risk of identity theft or fraud (i.e., access to bank accounts, driving records, tax and employment histories, and other private information). Given the sensitivity of the SSN, the following are some recommendations:



- ✓ Collect SSN as a primary identifier only if permitted by law;
- ✓ Reduce and/or eliminate the use of SSNs not required for a business purpose;
- ✓ Use an alternate identifier (unique, randomly generated number not derived from PII);
- ✓ Per NIH Policy, transmit SSN electronically only through an encrypted means!

Encryption Questions? Contact the IT Service Desk or call (301) 496-HELP.

Privacy Questions? Contact the OSOP at privacy@mail.nih.gov or call (301) 451-3426.