



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

Completion Date: September 14, 2012 (or earlier, as determined by your IC)

- Visit <http://irtsectraining.nih.gov> (go thru NIH Login)
- Enter the Personal Identifier from the back of your ID badge (ex. 012-3456-789)
- Login to take the 2012 Annual Privacy Awareness Refresher

Prevent Privacy Incidents

The HHS Privacy Incident Response Team (PIRT) has recommended efforts be improved for real-time training of employees after a privacy incident.

What is a privacy incident? The loss of control, compromise, unauthorized disclosure, acquisition, access or potential access to physical or electronic information that can personally identify an individual (i.e., contact information, date/place of birth, race, gender, financial data).



Big Breach at MD Anderson Cancer Center:

A laptop stolen from a physician's home in April 2012 contained data for approx. 30,000 patients. One third of the records included names, SSNs, medical record numbers, and treatment and/or research information.

Is there a risk to mishandling NIH data? Yes, both to the affected individuals and our agency. The 2011 Annual HHS PIRT Report analyzed 176 incidents and reported internal actors are the largest cause of privacy incidents. The number is expected to increase due to misuse and abuse of resources and privileges such as the loss and theft of portable devices and e-mails containing PII sent outside of the agency without encryption.

What can you do? Encrypt files that contain personal identifiers. Do not store personal data on your home work station or laptop. Use VPN to access data from a remote location.

Immediately upon discovery of a privacy incident, contact the [NIH IT Service Desk](#)

---- Phone (301) 496-4357 ---- Toll Free (866) 319-4357 ---- TTY (301) 496-8294 ----

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