Protecting strictly personal data

Rapid advances in computer technology offer us new ways to work with information, preserve it, and share it with others. But these "advances" also have their perils, and one of them is concern over the unwanted and illegal access to information, especially personally identifiable information, or PII, as it is called.

Last year, we reminded NARA employees, contractors, volunteers, and others who do work for us that records with PII should not be removed from NARA offices or stored on personal computers without specific authorization from the proper NARA official. Simply put, loss of personally identifiable information can cause substantial harm, embarrassment, and inconvenience.

A recent incident involving a former NARA employee working at home with records containing personally identifiable information illustrates this danger. The home computer in use had file-sharing software, which allows others to share files, such as downloaded music. In this case, the software shared the entire hard drive of the computer, including NARA files with PII that had not been deleted from the computer when the employee left NARA.

Needless to say, the release of personally identifiable information can do serious harm to the individuals whose information becomes available to others, especially Social Security numbers, bank account numbers, credit card information, driver's license numbers, and medical information. This information represents the "mother lode" for those involved in identity theft.

Other information that can be useful to identity thieves includes home addresses, e-mail addresses, phone numbers, and other personal information, such as date or place of birth or mother's maiden name or birthdate. This information is often used for identity verification questions by software applications and helpdesk organizations and, in some cases, for passwords to access bank accounts and other sensitive information.

Release of PII, however inadvertent or accidental, can impact not just NARA employees, but also our customers and others. Researcher application files may contain some of this information, as do reference request files and order forms for

NARA materials.

Any employee could be affected through unlawful access to travel vouchers, personnel actions, performance evaluations, and any related documents.

So, how do we guard against having PII released inadvertently and without authorization?

First, if you do your work at NARA, it's easy to take safeguards:

- Before leaving your workstation unattended, properly file any records or other materials containing PII.
- If you leave your computer while PII data is visible or accessible, use Control-Alt-Delete and choose "Lock Workstation" to lock your screen.
- Seal and mark appropriately any envelope containing PII that you send, in order to limit the information being received by someone other than the intended recipient.
- Destroy materials with PII, as authorized by schedule, by shredding, burning, or deleting.
- Where possible, limit the collection and use of PII.
- Avoid using Social Security numbers on employee forms whenever possible, because there are other means to ensure an employee's identity. NARA has ended this requirement on a number of forms.

At home, under flexiplace, the most important thing is to be sure you can control access to information. If you download and revise a document including e-mail attachments, be sure the computer you use has current anti-virus protection, a basic firewall in place, and restricted access so that others cannot inadvertently change your security settings.

If you are temporarily saving work documents on your home computer, make sure the directory you are using is not shared with other computers on your network. The secure use of file sharing software, such as Kazaa or Morpheus, is a challenge even for experts. Delete this software from any PC you intend to use for work purposes.

In short, download only what you need to complete your task, and as soon as you finish, place the work documents on a secure NARA network file server and delete any local copies that are on your personal computer or thumbdrive.

If you work with PII data at home, contact the Privacy Officer or NHI security for guidance on how to manage and transport this information. The best way to avoid having PII fall into the wrong hands would be to do all the work involving personally identifiable information at NARA on NARA computers.

We are continuing to look for ways to further protect PII. For example, a "privacy page" has been launched on the *NARA@work* web site that contains instructions, guidance, and resources for staff dealing with PII. It is at *www.nara-at-work.gov/staff_resources_and_services/employee_resources/privacy.html.*

Other ways to protect this information may be developed in the future.

ALLEN WEINSTEIN
Archivist of the United States

This column originally appeared in the May 2007 issue of the NARA Staff Bulletin.