

Greetings from the OSOP! This summer while enjoying some well deserved time off, NIH employees may choose to access their NIH email remotely by using government issued cellular devices or smart phones. In support of maintaining the integrity of NIH's information technology (IT) resources and to prevent compromising data, we would like to provide some guidance on the responsible use of smart phones and cellular devices.



Over the last few years, the use of cell phones in the U.S. has increased dramatically: eight out of ten adults today (82%) are cell phone users. Cell phones have proven to be an invaluable resource that may also serve as a global positioning system (GPS), game console, and computer. Coupled with these technological leaps has come the possibility of an invasion of one's privacy.

Recent news reveals that cellular devices provided by industry giants such as Google, Inc. and Apple, Inc. gather detailed user data, including the user's

location, age, and gender, that is later shared with outside advertisers without user knowledge. By accessing your email from the NIH server and downloading NIH documents to your Government cellular device, you are risking not only the physical loss of NIH data if your device is stolen or broken, but also that NIH data could be inadvertently transmitted to hackers, and other unknown sources.

To protect NIH data, please keep in mind the following:

- NIH staff are authorized to use NIH-owned resources, such as **electronic mail**, for **limited personal use only**. This policy applies to the use of NIH IT resources, regardless of location (e.g., office, home, on travel, field locations, telecommuting sites). Limited personal use is a privilege and staff are expected to use professional judgment, follow rules and regulations and be responsible for their own personal and professional conduct while using these IT resources. One way to mitigate the risk of compromised data is to make sure your cellular device is locked with a password.
- **Outside of limited personal use**, government staff, contractors, or other non-government staff are not permitted to use any non-government furnished IT equipment (non-GFE) to connect to NIH IT resources or any other resources to do official government work. This policy applies to all types of IT systems and devices, including **Blackberries, personal digital assistants (PDAs), and smart phones**.
- Remote and direct logical access to NIH IT resources that include the use of non-GFE will be phased out and **prohibited by the end of calendar year 2013**; therefore, you should begin to slowly reduce the use of your cellular devices to access NIH e-mail and other IT resources.

For more information, please visit:

- [NIH Manual Chapter 2806: Limited Authorized Personal Use of NIH Information Technology \(IT\) Resources](#)
- [NIH Manual Chapter 2814: NIH Policy on the Prohibited Use of Non-Government Furnished \(Non-GFE\) IT Equipment](#)

Feedback/Questions? Please contact the OSOP at: privacy@mail.nih.gov or (301) 451-3426.