



NIH Renews Focus on Protecting Sensitive Data and Information Used in Research

The recent theft of an NIH employee's laptop computer with sensitive data on human subjects has placed renewed focus on data security at NIH.

Technology enables people to work on portable electronic devices in remote locations where these devices can be stolen or misplaced thus putting sensitive data at risk. This notice serves to reconfirm the National Institutes of Health's commitment to protect sensitive personal data and information generated by NIH-supported extramural institutions that conduct research to advance the health and well being of all Americans. (NOT-OD-07-054)

All information systems, electronic or hard copy, which contain federal data, must be protected from unauthorized access. Congress and the Office of Management and Budget (OMB) have instituted laws, policies and directives that govern the creation and implementation of federal information security practices that pertain specifically to grants and contracts. The current regulations are pursuant to the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002 Pub. L. No. 107-347 (beginning on page 48) (NOT-OD-08-032).

Although FISMA applies to grantees only when they collect, store, process, transmit or use information on behalf of HHS or any of its component organizations, recipients of NIH funds are reminded of their vital responsibility to protect sensitive and confidential data as part of proper stewardship of federally funded research, and take all reasonable and appropriate actions to prevent the inadvertent disclosure, release or loss of sensitive personal information. NIH advises that personally identifiable, sensitive, and confidential information about NIH-supported research or research participants not be housed on portable electronic devices. If portable electronic devices must be used, they should be encrypted to safeguard data and information. These devices include laptops, CDs, disc drives, flash drives, etc. Researchers and institutions also should limit access to personally identifiable information through proper access controls such as password protection and other means. Research data should be transmitted only when the security of the recipient's systems is known and is satisfactory to the transmitter.