Chief Information Officer
National Institutes of Health
Department of Health and Human Services

Guide for Identifying and Handling Sensitive Information at the NIH

November 08, 2010

Change History

Version	Date of Issue	Author(s)	Description of Change(s)
0.1	01/28/10	Ellen Gadbois, NIH/OD	Original draft publication
0.2	4/30/10	Brent Kopp, OCIO/ISAO	Incorporated comments/feedback and provided comments matrix.
0.3	5/17/2010	Brent Kopp, OCIO/ISAO	Incorporated comments/feedback and provided comments matrix.
0.4	7/30/2010	Ellen Gadbois, NIH/OD	Minor Grammatical changes. Final approval from Dr. Patterson and Exec Sec.
1.0	11/08/2010	OCIO/ISAO	Minor changes as a result of Exec Sec review. Updated links. Removed the reference to HIPAA Privacy Rule requirements per OGC.

Contents

Purpose

The purpose of this **Guide for Identifying and Handling Sensitive Information at the NIH** is to provide NIH Institute and Center (IC) staff with information to help determine what is and is not "sensitive information" to meet the following requirements:

1) Data encryption (including the encryption of laptops and mobile devices); and
2) The reporting of suspected and/or confirmed breaches of sensitive information and personally identifiable information (PII).

Definition of Sensitive Information

Information is considered sensitive if *the loss of confidentiality, integrity, or availability could be expected to have a* ***serious, severe, or catastrophic*** *adverse effect on organizational operations, organizational assets, or individuals.*[1]

Further, the loss of sensitive information confidentiality, integrity, or availability might:

- cause a significant or severe degradation in mission capability to an extent and duration that the organization is unable to perform its primary functions;
- result in significant or major damage to organizational assets;
- result in significant or major financial loss; or
- result in significant, severe or catastrophic harm to individuals that may involve loss of life or serious life threatening injuries.[2]

At HHS, sensitive information is *information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the conduct of HHS programs, or the privacy of individuals entitled under* The Privacy Act *or the* Health Insurance Portability and Accountability Act (HIPAA). Information technology (IT) security personnel and system owners can equate this definition of sensitive information with *data that has a FIPS 199 security impact level of* moderate *or* high *for the*

[1] Federal Information Processing Standard (FIPS) 1999, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

[2] Ibid.

Confidentiality security objective. This definition of sensitive information is media neutral, applying to information as it appears in either electronic or hardcopy format.[3]

Examples of Sensitive Information:

- Personally Identifiable Information (PII) with a confidentiality impact level of moderate or high based on NIST SP 800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).*[4] Examples include:
  - Social security numbers
  - Employee performance ratings and disciplinary actions
  - Employee grievances
  - Employee financial and banking information
- Financial disclosure forms
- Pre-award contract information (including "Source Selection Information" as defined in FAR 2.101, https://www.acquisition.gov/far/html/Subpart%202_1.html)
- Pre-decisional grant information
- Patient records that have not been de-identified
- Genome-wide association study data and whole genome sequence data from humans
- Police and criminal investigation information
- Proprietary information provided to the NIH by outside parties and specified as proprietary, including commercial information and data of collaborators
- Data submitted or expected to be submitted in support of an Employee or Grantee Invention Report or patent filing that has not otherwise been approved for disclosure as a scientific communication or become public
- Any data, manuscripts, memos, unidentified or coded clinical information, or other information that are deemed by the person generating or storing the information or that person's supervisor to be of commercial value, or where it has been determined that loss of such information would cause damage to the NIH, DHHS, or the federal government

This guidance is focused on how sensitive information is protected at NIH. However, NIH recognizes that there are instances in which sensitive data needs to be shared with others, such as in grant review and scientific collaborations with extramural researchers. In such cases, the NIH holders of the data, in consultation with the NIH Chief Information Officer (CIO), will put in place reasonable controls to ensure continued protection of the data, such as data encryption and signed agreements by data users.

Note that information given to the government in a Privacy Act record is subject to the controls of the Privacy Act. Information in records governed by the Privacy Act is considered "sensitive information" if it meets the aforementioned definition. Contact the NIH Senior Official for Privacy for case specific assistance at (301) 451-3426. Similarly, information withheld under the Freedom of Information Act (FOIA) may or not meet the definition of "sensitive," and in some cases "sensitive information" may be released under FOIA. Contact the NIH FOIA Office for case specific assistance at (301) 496-5633.

[3] HHS Memorandum: Updated Departmental Standard for the Definition of Sensitive Information http://intranet.hhs.gov/infosec/docs/policies_guides/HM/Dept_Standard_for_Def_of_Sensitive_Info_5-18-09.doc

[4] http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

Examples of Data NOT Considered to be Sensitive Information

- Primary research data that does not support an employee invention report or patent application and/or does not contain moderate or high PII
- Manuscripts (submitted or in preparation) that are intended for publication in a public archive such as a journal or book
- Presentation materials intended for public disclosure
- Other information that is publicly available or has been made public
- Post award Grant and Contract data
- De-identified patient research data[4]
- Data encrypted using FIPS 140-2 technologies

Encryption transforms information using an algorithm to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted (unreadable) information. This makes the data secure as no one can understand it. Loss of control of encrypted information is NOT considered a breach; thus NIH stresses the use of encryption.

NIH employees are encouraged to use good judgment to protect all information, as appropriate. Some information may not meet the definition of “Sensitive Information” referenced above (and thus encryption is not required) but should still be carefully handled. However, per HHS policy, all laptop computers will be encrypted per the details in the next section.

Encryption of Sensitive Information

The Department of Health and Human Services (DHHS), the Office of Management and Budget (OMB), and the Federal Information Security Management Act (FISMA) require implementation of stringent controls to protect the confidentiality, integrity, and availability of Sensitive Information. The most recent requirement from HHS (December 23, 2008)[5], is as follows:

(1) All HHS laptop computers shall be secured using a Federal Information Processing Standard (FIPS) 140-2 compliant[6] whole-disk encryption solution.

[5] HHS Standard for Encryption
http://intranet.hhs.gov/infosec/docs/policies_guides/1SS/001SEncryption12232008.html
http://intranet.hhs.gov/infosec/docs/policies_guides/1SS/001SEncryption12232008.doc
http://intranet.hhs.gov/infosec/docs/policies_guides/1SS/001SEncryption12232008.pdf

[6] The cryptographic module used by an encryption or other cryptographic product must be tested and validated under the Cryptographic Module Validation Program to confirm compliance with the requirements of FIPS Publication 140-2 (as amended). For additional information, refer to http://csrc.nist.gov/cryptval.

(2) All sensitive information[7] stored on government-furnished desktops and non-government-furnished desktops used on behalf of the Department shall be secured either through a FIPS 140-2 compliant encryption solution or through adequate physical security and operational controls at the desktop's residing location.

> *Informational: Whole-disk encryption solutions are acceptable as are solutions that protect individual files or folders containing sensitive information. The decision to employ physical protections over an encryption solution is a risk-based decision, as these protections cannot completely remove the risk of theft or loss of sensitive data at all offices. The risk-based decision to use any alternatives to encryption shall be formally documented and approved by the appropriate Designated Approval Authority (DAA).*

(3) All mobile devices[8] and portable media[9] that contain sensitive information shall be encrypted, as specified above.

(4) A key recovery mechanism shall be used so encrypted information can be decrypted and accessed by authorized personnel. Use of encryption keys which are not recoverable by authorized personnel is prohibited.[10] OPDIVs/STAFFDIVs shall implement a process that requires approval by senior management or the Chief Information Security Officer to authorize recovery of keys by someone other than the key owner.

(5) Encryption keys shall comply with all HHS and OPDIV/STAFFDIV policies and shall provide adequate protection to prevent unauthorized decryption of the information.[11]

(6) Language shall be included in all contracts to ensure that sensitive HHS data is appropriately encrypted, in accordance with the Federal Acquisition Regulation (FAR), the HHS Acquisition Regulation (HHSAR), and this standard.

Deviations from this standard shall be approved by the OPDIV/STAFFDIV Chief Information Officer (CIO) or by the OPDIV/STAFFDIV Chief Information Security Officer (CISO), if such authority is delegated by the CIO.

[7] The HHS definition of sensitive data is available at http://intranet.hhs.gov/infosec/docs/policies_guides/HM/Dept_Standard_for_Def_of_Sensitive_Info_5-18-09.html This encryption standard only applies to data which has a FIPS 199 security impact level of Moderate or High for the confidentiality security objective. Availability and integrity are not considered in determining if encryption is required under this standard.

[8] Mobile device: Any computer or other apparatus that can store and process data and is designed to be mobile. Examples include laptop computers, iPODs, Blackberries, Treos, Palm Pilots and other Personal Digital Assistants (PDAs).

[9] Portable Media: Any device that can store data electronically and is portable, such as portable hard drives, Universal Serial Bus (USB) drives, secure digital (SD) card media, CD-ROMs, and DVDs.

[10] Key recovery is required by *OMB Guidance to Federal Agencies on Data Availability and Encryption*, November 26, 2001.

[11] See NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography,* and SP 800-57, *Recommendation for Key Management.*

Reporting Breaches

On May 22, 2007, OMB M-07-16 reiterated the requirement that "agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 2) there is a **suspected or confirmed breach of personally identifiable information** regardless of the manner in which it might have occurred."

Per the OMB memo, "the term **"personally identifiable information"** refers to information that 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 that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

NIH employees and contractors must report any breach of sensitive or personally identifiable information by contacting the NIH Help Desk at (301) 496-4357 within one hour of discovery. Loss of sensitive data and/or personally identifiable information includes loss via e-mail sent to the wrong address/individual, paper records, or any other mechanism where unauthorized individuals may potentially have possession of or access to information that was improperly disclosed to them. IT equipment may contain sensitive information. Therefore, NIH staff who discover the loss or theft of a laptop/tablet computer issued by NIH or a contractor on behalf of the government must also report the breach within one hour to the NIH Helpdesk. Loss of NIH-issued IT equipment includes servers, desktops, laptops, Blackberries, PDAs, data storage devices, and any other accountable information processing equipment. In addition to reporting the loss/theft to the NIH Helpdesk, the employee or contractor must also notify the immediate supervisor or contracting official and file a police report with the local jurisdiction, as appropriate.

Contacts & Resources

Encryption Questions: see http://ocio.nih.gov/nihsecurity/encryptionfaq.htm or contact the NIH Help Desk at 301-496-4357

Ethics: http://ethics.od.nih.gov/contacts.htm

FOIA: NIH FOIA Office, 301-496-5633

Privacy Act: NIH Senior Official for Privacy, 301-451-3426

Reporting breach of pre-decisional Grant information:
Carla Flora
301-793-8752
ORISISSO@mail.nih.gov

HHS Human Subjects Regulations, 45 CFR 46:
http://www.hhs.gov/ohrp/humansubjects/guidance/45cfr46.htm

IC Information Systems Security Officers: http://ocio.nih.gov/nihsecurity/scroster.html

IC Privacy Coordinators: http://oma.od.nih.gov/about/contact/browse.asp?fa_id=3

NIH FOIA Officer: http://www.nih.gov/icd/od/foia/index.htm

NIH Privacy Act Officer: http://oma.od.nih.gov/ms/privacy/

Office for Human Research Protections: http://www.hhs.gov/ohrp/

Reporting breach of Sensitive Information or computer/laptop/PDA/Blackberry loss/theft:
NIH Helpdesk
301-496-4357

Reporting breaches of GWAS data obtained from dbGaP:
Laura Lyman Rodriguez, Ph.D.
301-496-0844
gwas-alert@nih.gov