Fred Hutch Information Classification and Handling Standard

Fred Hutchinson Cancer Research Center
www.fredhutch.org

Revision 1.0 of Document
Content Revision Date: October 13, 2017 Effective Date: 11/2/2017 Approval Date: 10/26/2017
Document Number 120 in Repository
For all Fred Hutch information security standards, click on the following link:
https://centernet.fredhutch.org/content/dam/centernet/u/center-it/ISO/Fred-Hutch-Information-Security-Standards-Reference.pdf

Table of Contents

Information Classification and Handling Standard Overview

Purpose

This document assists authorized users in classifying and handling Fred Hutch information based on its level of sensitivity and value to Fred Hutch.

Adherence to this standard will assist in complying with the **Fred Hutch Information Security Policy**. The policy is available here:

https://centernet.fredhutch.org/cn/p/information-security-policy.html

Specifically, this standard:

- Establishes the classification levels of Fred Hutch information
- Establishes the requirements in support of securely handling Fred Hutch information of varying classifications. These requirements include media protection and access controls around information.
- Specifies how systems and software must be implemented with an appropriate level of security controls to protect Fred Hutch information

Scope

Authorized users are accountable and responsible for complying with this standard. This standard applies to every existing or planned implementation of technology or paper-based processes that will handle, process, or store information.

This standard covers the following:

Information Classification Standards

- Level I: Public Domain/Low to No Risk from Disclosure
- Level II: Confidential/Moderate Risk from Disclosure
- Level III: Strictly Confidential/High Risk from Disclosure

Information Handling Requirements

This standard does not specify detailed baselines for implementing recommended security features. See any supporting departmental procedure documentation for instruction.

This standard does not address Fred Hutch record retention requirements. To see the **Fred Hutch Record Retention and Destruction Policy**, go to:

https://centernet.fredhutch.org/cn/p/record-retention-and-destruction-policy.html

Accountability

Fred Hutch authorized users are accountable and responsible for complying with this standard. Teams that design, operate, implement, and/or use these information security controls have the responsibility of ensuring that the controls are implemented and remain effective.

In the event authorized users are required to transmit information to third parties, steps must be taken to ensure that the requisite handling standard applies to such transmission and use of the information in a manner as rigorous as required here. In some case, data access and use agreements will be necessary to accomplish this objective. The Fred Hutch Office of the General Counsel can be consulted for assistance with establishing any necessary agreements.

Violations of this standard are referred to HR and may result in discipline, up to and including termination of employment or loss of access privileges.

Exceptions

A written statement requesting an exception to this document may be submitted to the Information Security Office (ISO) for review and potential approval. Those requesting an exception may also collaborate with the ISO to propose an alternative solution to meet the requirement or standard in question.

The ISO or its delegates, at their discretion, have the authority to grant exceptions.

Information Classification Standards

Fred Hutch recognizes three levels of information classification. Classification is based on the sensitivity and value of the information, with Level I being the least confidential and Level III being the most confidential.

- Level I: Public Domain/Low to No Risk from Disclosure
- Level II: Confidential/Moderate Risk from Disclosure
- Level III: Strictly Confidential/High Risk from Disclosure

All the information that is input, stored, processed, and/or output by a system or process must be reviewed to identify classification levels.

It is expected that information processed or stored will be classified according to the three (3) levels within 18 months of the effective date of this **Fred Hutch Information Classification and Handling Standard** or once a toolset (a combination of manual processes and technical solutions) facilitating such classification is implemented, whichever occurs later. Exceptions to this schedule will be considered in cases where compliance is dependent on third parties.

Level I: Public Domain/Low to No Risk from Disclosure

The Public Domain/Low classification applies to Fred Hutch information suitable for public consumption. This level of information is not considered confidential or strictly confidential in nature and can be released to the public.

The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operation, organizational assets, or individuals. No safeguards or protective measures are needed to protect this category of information from disclosure.

Examples include, but are not limited to, the following:

- Published research results
- Fred Hutch publications and communications [e.g., marketing materials, annual financial statements (after release), press announcements (post publication), public record documents, job postings, etc.]
- Open source configuration lists
- Open source code and recipes (e.g., https://github.com/FredHutch/galaxy_ftp)
- Reference genomes
- Released datasets

Level II: Confidential/Moderate Risk from Disclosure

The Confidential/Moderate classification applies to information for which unauthorized disclosure, destruction, or alteration of which reasonably could be expected to cause minor to moderate harm to Fred Hutch, its property, or its personnel, including financial loss, legal liability, or harm to reputation.

Confidential/Moderate information is made available only to individuals with the need and authorization to access it. The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Access is provided to staff only with a confidentiality agreement/pledge or information access and use agreement. See Table 1 on page 9 for controls applied this type of information.

Examples include, but are not limited to, the following:

- Pre–publication research information and analyses
- Medical expense information
- Invoices
- Legal instruments or agreements
- Transaction documents and reports
- Fast file and economy file server names
- Building plans and information about the physical plant
- De-identified research participant information
- Donor information

Level III: Strictly Confidential/High Risk from Disclosure

The Strictly Confidential/High classification applies to information for which unauthorized disclosure, destruction, or alteration reasonably could be expected to cause serious to catastrophic harm to Fred Hutch, its property, or its personnel, including severe financial loss, legal liability, public distrust, or harm to reputation. Access is provided to staff only with a confidentiality agreement/pledge or information access and use agreement. See Table 1 on page 9 for controls applied to this type of information.

Examples include the following:

- Protected Health Information (PHI), Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), and Personally Identifiable Information (PII)
- Passwords and encryption keys
- Proprietary information, including that belonging to entities other than Fred Hutch

Information Handling Requirements

- All systems, upgrades, or processes developed after the initial approval of this document must be compliant prior to go-live
- It is expected that information processed or stored will be protected at the requisite level as set forth in Table 1 on page 9 within 18 months of the effective date of this **Fred Hutch Information Classification and Handling Standard** or once a toolset (a combination of manual processes and technical solutions) facilitating such protection is implemented, whichever occurs later. Exceptions to this schedule will be considered in cases where compliance is dependent on third parties.

Table 1. Information protection and handling requirements by activity and classification level.

Activity↓	Classification Level I	Classification Level II	Classification Level III
Classification / De-classification Authority	Information owner/delegate.	Information owner/delegate.	Information owner/delegate.
On-Premise System Storage[1]	No special requirements.	• Information must be subject to administrative control by Fred Hutch personnel • Access to electronic information must require authentication • Access to information must be logged (date, time, user, activity) if storage system has automated capability or if reasonable manual processes allow	• Information must be subject to administrative control by Fred Hutch personnel both on and off Fred Hutch premises • Information must be encrypted in storage and in transit • Access to electronic information must require authentication • Access to information must be audited semi-annually • Access to information must be logged (date, time, user, and activity)
Paper Marking[2]	No special requirement.	Should be marked "Confidential."	Should be marked "Strictly Confidential."

[1] Access logging for Level II is intended to reasonably account for access to documents. It is not expected where it is impractical relative to the security gain. For example, manually logging access, such as physical access to Level II paper invoices, would not be expected or desired.

[2] Existing paper documents are considered grandfathered until such documents are revised for reasons other than marking the classification level. Once modified, the documents should then meet the paper marking requirements.

Activity↓	Classification Level I	Classification Level II	Classification Level III
Mailing/ Shipping within Fred Hutch	No special requirements.	Routing envelope/container with confidential label.	Tamper-proof envelope with confidential label.
Mailing/ Shipping outside of Fred Hutch to approved recipients	No special requirements.	• Sealed envelope/ container with confidential label • Delivery instructions	• Tamper-proof envelope with confidential label • Registered mail • Receipt of delivery with authorized signature
Cloud-based or other Off-premise Storage and Processing	No special requirements.	• Information must be encrypted in transit • Information must be protected by authentication • Access to information must be logged (date, time, user, activity) if storage system has automated capability	• Information must be encrypted in transit and in storage • Cloud provider and Fred Hutch must have agreement with sufficient security requirements • Access to information must be logged and authenticated
Email	No special requirements.	Information must be sent through Fred Hutch supported email systems.	• Email must be encrypted • Information must be sent through Hutch approved email systems • Email must contain delivery instructions[3]

[3] Use this text for email delivery instructions: “This electronic message transmission contains information which may be confidential or privileged. The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the contents of this information is prohibited. If you have received this electronic transmission in error, please notify the sender by telephone or by electronic reply, and delete this message.”

Activity↓	Classification Level I	Classification Level II	Classification Level III
Electronic Transfer Between Systems	No special requirements.	• Information must be encrypted when transferred outside the Fred Hutch computing network • Recipient system must meet the Classification Level II system storage requirements in this table (may require MOU or data use agreement)	• Information must be encrypted in transit • Recipient system must meet the Classification Level III system storage requirements in this table
Paper or Electronic Media Storage	No special requirements.	• Paper or electronic storage media (portable hard drives, CDs, etc.) with information must be stored securely within a controlled area[4] • Access to paper or electronic media must be limited to authorized individuals[5]	• Paper or electronic storage media (portable hard drives, CDs, etc.) with information must be stored securely within a controlled area • Information on electronic media must be encrypted • Access to paper or electronic media must be limited to authorized individuals
Transport of Media	No special requirements.	When paper or electronic storage media with information is transported, it must be done so in a secure manner and only by specifically authorized personnel.	• When paper or electronic storage media with information is transported, it must be done so in a secure manner and only by specifically authorized personnel • All such transport must be documented

Activity↓	Classification Level I	Classification Level II	Classification Level III
Media Reuse/ Disposal	No special requirements	Once an information medium is no longer needed to store or transport information, it must be completely sanitized before reuse or destroyed before retirement.	Once an information medium is no longer needed to store or transport information, it must be completely sanitized before reuse or be destroyed before retirement.
Logging of Access	No special requirements.	Record of each access required (date, time, user, activity) if the information system has automated capability.	Record of each access required, including access to physical media where specified (date, time, user, and activity).

[4] For example, documents should be placed in cabinets instead of left out on desks, documents should be printed on secure printers (contact your IT dept. for a list), printouts should be picked up *promptly* if a secure printer is not available, etc.

[5] For example, a "whitelist" of authorized persons could be maintained and periodically reviewed.

Appendix

Definitions

Term	Definition
Authorized User	Fred Hutch employees and Fred Hutch agents, contractors, and other non-employees, including any individual or entity that has authorization from Fred Hutch to access, store, or transmit Fred Hutch Information. Authorized Users include users in possession of, or access to, Fred Hutch Information located at facilities not owned or operated by Fred Hutch, and to circumstances in which non-Fred Hutch devices, processes, or technologies are utilized to obtain access to Fred Hutch systems and/or Fred Hutch Assets or Information.
De-identified Information	To qualify as de-identified, information must have the following elements (the 18 HIPAA PHI fields) removed or otherwise obfuscated in accordance with Privacy Rule regulations and guidance[6] for de-identified information: • Names • Locations; all geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes • Dates (all dates related to the subject of the information, e.g., birth dates, admission dates, discharge dates, encounter dates, surgery dates, etc.). Only year is allowed, or all patient events associated with a date must have the date of the event obfuscated. • Telephone numbers • Fax numbers • Electronic mail addresses • Social security numbers • Medical record numbers • Health plan beneficiary numbers

[6] These can be found at www.hhs.gov

Term	Definition
	• Account numbers • Certificate / license numbers • Vehicle identifiers and serial numbers, including license plate numbers • Device identifiers and serial numbers • Web Universal Resource Locators (URLs) • Internet Protocol (IP) address numbers • Biometric identifiers, including finger and voice prints • Full face photographic images and any comparable images • Any other unique identifying number, characteristic, or code (e.g. pathology accession numbers)
Individually Identifiable Information (III)	Information that contains elements that either identify an individual or could be used in combination with other easily accessible information to identify an individual in either paper based or electronic format.
Individually Identifiable Health Information (IIHI)[7]	A subset of health information, including demographic information collected from an individual, and: Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and 1) identifies the individual; or 2) there is reasonable basis to believe the information can be used to identify the individual.

[7] Covered Entities generally include health care facilities, health care providers and health insurance companies. For example: Fred Hutch's self-insured employee health plans are considered to be covered entities and as such their IIHI is PHI and the plans are subject to the requirements of HIPAA Rules. The University of Washington, SCCA, and Seattle Children's Hospital are also covered entities.

Term	Definition
Information	Any information or processed data, including words, numbers, images, and sounds that Fred Hutch owns, hosts, licenses, stores or manages in any form, for any length of time including employee records, financial reports, and research data.
Information Classification	A designation used to determine the level of safeguards necessary to protect the confidentiality and integrity of various types of information.
Personally Identifiable Information (PII) aka Restricted Information	A category of Individually identifiable information containing one or more of the following in either paper based or electronic format: • Social Security number • Name • Driver's license number • Account number(s) issued by financial, credit or investment organizations including, for example, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
Protected Health Information (PHI)	Individually Identifiable Health Information (in either paper or electronic format) generated and/or maintained by a Covered Entity as defined by HIPAA. Covered Entities typically include, but not limited to health care providers, health care facilities, and health insurers.
Sanitize	A general term referring to the actions taken to render information written on media unrecoverable by both ordinary and extraordinary means.
System	The combination of software (application), information, and platform needed to deliver a service to the end user.
Transmission Method	The process by which information is transported.

References

FIPS 199

NIST 800-53

Controls Addressed in this Standard

Table 2. NIST Controls. Due to the length of the descriptions, this table provides links instead of the description text. Contact the ISO for clarification if needed.

Control	Description
Technical Access Control AC-3 Access Enforcement LOW_MODERATE_HIGH P1	https://nvd.nist.gov/800-53/Rev4/control/AC-3
Technical Access Control AC-4 Information Flow Enforcement MODERATE_HIGH P1	https://nvd.nist.gov/800-53/Rev4/control/AC-4
Operational Media Protection MP-4 Media Storage MODERATE_HIGH P1	https://nvd.nist.gov/800-53/Rev4/control/MP-4
Operational Media Protection MP-6 Media Sanitization LOW_MODERATE_HIGH P1	https://nvd.nist.gov/800-53/Rev4/control/MP-6
Operational Personnel Security PS-3 Personnel Screening LOW_MODERATE_HIGH P1	https://nvd.nist.gov/800-53/Rev4/control/PS-3

Revision History

These entries describe the general revision history of the document.

Rev. #	Rev. Date	Authors	Change Description
1.0	10/13/2017	Lisa Coleman, Gerianne Sands, Mary Gardner, Ric Testagrossa, Glenn Kaleta, Chris Briggs	Initial version.