
Department: UW Medicine Information Technology Services

Policy Number: SEC-02 – Information and Information System Classification Policy

Effective Date: June 11th, 2007

Review Date: April 27th, 2007

Purpose

This Information and Information System Classification policy defines the basis and criteria by which classifications of information and information systems will be made and the requirements regarding the processes and maintenance of their classifications. Classification ensures the appropriate level of security is applied for information and information systems, based on the identified level of impact to data confidentiality, integrity, and availability.

See UW Medicine Information Security policy: *SEC-REF UW Medicine Information Security Program Glossary of Terms*.

Policy

UW Medicine¹ classifies information and information systems based on a range of impact levels.

Systems with low needs for confidentiality, integrity, and availability protections are eligible for Minimum Requirements for Information Security. All computing devices connected to the UW Medicine network must meet Minimum Requirements for Information Security². Where feasible, Supervisors, System Owners and System Operators should, attempt to, separate the storing of ePHI from other UW Medicine electronic Information to reduce risk.

¹UW Medicine includes the following entities: University of Washington Medical Center and Clinics; Harborview Medical Center and Clinics; UW Medicine Neighborhood Clinics (University of Washington Physicians Network); UW Physicians Sports Medicine Clinic; Hall Health Primary Care Center; University of Washington Physicians; UW Medicine Eastside Specialty Center; as well as certain services and activities that support UW Medicine that are performed by non-healthcare components of the University of Washington as defined within Privacy Policy PP-01 Use and Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

² See the UW Medicine Information Security standard, *Networked System Information Security Standard*, which is included in the UW Medicine Information Security policy: *SEC-05 – Communications and Operations Management Policy*.

Classification of Information and Information Systems

The System Owner assesses the information and information system requirements for confidentiality, integrity, and availability. Systems having requirements greater than the minimum requirements need advanced security. Please see UW Medicine Information Security Policy: *SEC 05 – Communications and Operations Management Policy*.

It is the responsibility of the System Owner to define the appropriate impact level associated with the information or information system. The classification can be a self-assessment or can be based on an Information Risk Assessment. For more information regarding risk, risk management, and risk assessment, see UW Medicine Information Security policy: *SEC 09 - Risk Management Policy*.

The classification of information is not permanent, and may change. Due to its special nature, protected health information³ does not cease to be CONFIDENTIAL.

A) Criteria for Information and Information System Classification

Classification of information and information systems is based on an assignment of appropriate levels of impact (low, moderate, high) to the respective security objective (confidentiality, integrity, availability).

(i) Security Objectives. Security objectives recognize operational needs for sharing or restricting information. UW Medicine's security objectives are:

- **Confidentiality:** ensuring that information is accessible only to those authorized to have access;
- **Integrity:** the property that data or information have not been altered or destroyed in an unauthorized manner;
- **Availability:** ensuring that authorized users have access to information and associated assets when required.

(ii) Impact Levels. The impact levels are low, moderate, and high. These impact levels are based on the potential impact of information asset loss, theft or corruption on UW Medicine operations, assets or public image.

The levels of impact to information and information systems are defined in the following table:

³ Protected Health Information is individually identifiable health information maintained in permanent health records and/or other clinical documentation in any medium, e.g. paper, oral or electronic format.

Impact Levels		
Low	Moderate	High
The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a limited adverse effect on operations, assets or public image.	The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a serious adverse effect on operations, assets or public image.	The unauthorized disclosure of, improper modification or destruction of, or disruption of access to information could be expected to have a severe adverse effect on operations, assets or public image.

B. Documentation Format

The standard format for documenting security classifications, (e.g., in security plans and risk assessments), is as follows:

CLASSIFICATION =
 [(**Confidentiality**, Impact Level),
 (**Integrity**, Impact Level),
 (**Availability**, Impact Level)].

(i) Confidentiality Classification

Based on the confidentiality impact level of the information and information systems, the following definitions and examples are provided:

Confidentiality Classification Examples

<p>LowPUBLIC: This is information that is either approved for general access, or by its nature, is not necessary to protect, and can be shared with anyone. A breach of the confidentiality of information with a low classification for confidentiality is expected to have either a no adverse effect or a limited adverse effect on UW Medicine operations.</p>	<p>ModerateRESTRICTED : This is information that is business data, which is intended strictly for use by designated UW Medicine employees and agents. This classification applies to data less sensitive than CONFIDENTIAL information. Dissemination of this data shall only be made to UW Medicine workforce⁴ with an established "need-to-know." A breach of the confidentiality of restricted information is expected to have a serious adverse effect on UW Medicine operations.</p>	<p>HighCONFIDENTIAL: This classification of information is very sensitive in nature, and requires careful controls and protection. For example Protected Health Information. Unauthorized disclosure of this data could seriously and adversely impact UW Medicine or interests of patients, other individuals, and organizations associated with UW Medicine. A breach of the confidentiality of CONFIDENTIAL information is expected to have a severe adverse effect on UW Medicine operations.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

EXAMPLES

<p>General public information, published reference documents (within copyright restrictions), open source materials, approved promotional information, press releases.</p>	<p>Short-term marketing plans, executive function data, selected research data, intellectual property.</p>	<p>Personally identifiable information, protected health information, workforce records, student records, social security numbers, legally protected University records, selected research data, passwords.</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

(ii) Integrity Classification

The most serious risks involving information integrity occur either when some action is taken that is based on the modified information or the modified information is disseminated to other organizations or the public.

Based on the integrity impact level of the information and information systems, the following examples are provided:

⁴ Workforce: Faculty, employees, trainees, volunteers, and other persons who perform work for UW Medicine, and whose work conduct is under UW Medicine's direct control regardless of whether or not the workforce member is paid by UW Medicine.

Integrity Classification Examples		
Low	Moderate	High
EXAMPLES		
Public comments, customer survey data, IT maintenance records.	Financial asset and liability management, payroll records, product/service design data.	Patient records, passwords, operating room computerized equipment software.

(iii) Availability Classification

Based on the availability impact level of the information and information systems, the following examples are provided:

Availability Classification Definitions		
Low	Moderate	High
EXAMPLES		
Hospital gift shop inventory records, Conference room schedules.	UW Medicine intranet data, policies and procedures, disaster recovery and emergency preparedness information.	Patient information, surgical or ICU computing and electronic equipment, hospital/clinic security cameras and door locks.

References:

- I. 45 CFR Part 164; Section 164.310(d)(1) Device and Media Controls; (2) (iii) Accountability
 - II. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 5, Asset Classification And Control
 - III. Federal Information Processing Standards Publications (FIPS PUBS) 199, Standards for Security Categorization of Federal Information and Information Systems
-

UW Medicine IT Services: _____ Date: _____
James S. Fine, MD., CIO, ISO
