

---

Department: UW Medicine Information Technology Services

Policy Number: SEC-01.02 Information Security Policy Exemption Procedure

Effective Date: June 11<sup>th</sup>, 2007

Review Date: April 27<sup>th</sup>, 2007

---

### **Purpose**

This procedure is in place to help System Owners file a policy exemption when no other solution can be found to meet the security policy.

### **Definitions**

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

### **Procedure**

#### **I. Policy Exemption Requests**

A System Owner, System Operator, or Supervisor will submit requests for an exemption to UW Medicine Information Security Policy to the HIPAA Program Office, [hipaa@u.washington.edu](mailto:hipaa@u.washington.edu), using the attached Policy Exemption Request Form. The requestor must maintain all documentation related to the exemption in compliance with UW Records Retention policies. Potential exemptions identified by general workforce members are to be reported to the respective System Owner or Supervisor.

#### **II. Policy Exemption Approval Process**

The following steps explain the required process for implementing, storing or using information or information systems within UW Medicine that represent exemptions to any established UW Medicine Information Security Policy or Standard.

The following are the stages of the exemption approval process:

1. Requestor (System Owner or Supervisor) completes the *Policy Exemption Request* Form and sends it to the HIPAA Program Office, [hipaa@u.washington.edu](mailto:hipaa@u.washington.edu). If approved then a Help Desk ticket will be opened and assigned to SIT.
2. The Security Infrastructure Team (SIT) reviews the exemption request. If SIT determines the situation does not produce an exemption or if

compliance with the policy or standard is achieved in another manner, the request is closed and the exemption issue is resolved. If the issue can not be resolved, the SIT conducts and documents a risk assessment of the requested exemption. The exemption request and the SIT analysis is submitted to the IT Services Director of Information Security.

3. The IT Services Director of Information Security and the Requestor evaluate the exemption request for validity, documenting their findings.
4. The IT Services Director of Information Security assesses the risks and makes a recommendation to the UW Medicine Chief Information Officer and the UW Medicine Information Security Officer.
5. The UW Medicine Chief Information Officer and the UW Medicine Information Security Officer evaluate the exemption request, the risk assessment, and the recommendation of the IT Services Director of Information Security. If they find that the exemption is not supportable, the exemption is denied. If they find that the exemption has merit, the exemption is sent to the Confidentiality and Access Steering Committee.
6. Confidentiality and Access Steering Committee reviews the exemption request. If CASC finds that the exemption is valid, the exemption is approved in writing. If CASC finds that the risk created by the exemption is unacceptable, the exemption is denied.
7. The Requestor maintains the documentation of the policy or standard exemption request and its disposition.

---

---

**References:**

- I. University of Washington Information Systems Security Policy (Security Policy)
- II. 45 CFR Part 164; Section 164.308(a)(1) (i) Security Management Process
- III. 45 CFR Part 164; Section 164.316 Policies and Procedures and Documentation Requirements
- IV. International Organization for Standardization /International Electrotechnical Commission (ISO/IEC) 17799 Section 3, Security Policy

---

---

UW Medicine IT Services: \_\_\_\_\_ Date: \_\_\_\_\_



**Policy Exemption Request Form**

This form is to be completed and maintained by the System Owner or Department Manager.

Date: \_\_\_\_\_

Name of System: \_\_\_\_\_

Department: \_\_\_\_\_

UW Medicine Entity: \_\_\_\_\_

Helpdesk ticket: \_\_\_\_\_

Informal Compliance Review (ICR) Survey Number: \_\_\_\_\_

---

A) Details regarding the System or Department in question:

B) The specific policy or standard for which the exemption is being requested:

C) The situation that has prompted the request:

D) The reason for the exemption request:

System Owner: \_\_\_\_\_

System Operator: \_\_\_\_\_

or

Department Manager: \_\_\_\_\_

**Exemption Request Process Tracking**

1) SIT/System Operator Assessment:

Completed on date: \_\_\_\_\_

Comments/Results:

If solutions can not be found to resolve the security issue, attach the risk assessment for the requested exemption

IT Services SIT Member: \_\_\_\_\_

2) Director of Security/ System Owner:

Completed on date: \_\_\_\_\_

Comments/Results:

IT Services Director of Security: \_\_\_\_\_

3) CIO/UW Medicine ISO/CASC:

Completed on date: \_\_\_\_\_

Comments/Results:

Exemption Status (Requested/Pending/Approved/Denied): \_\_\_\_\_

ISO: \_\_\_\_\_