

---

Department:	UW Medicine Information Technology Services
Policy Number:	SEC-05.03 – Encryption Standard
Effective Date:	December 18 <sup>th</sup> , 2007
Review Date:	December 4 <sup>th</sup> , 2007

---

### **Purpose**

In some situations, the risk associated with CONFIDENTIAL information is sufficiently high to justify use of special safeguards in addition to standard access controls. Encryption and related cryptographic techniques can provide the extra level of protection needed in these cases. This UW Medicine<sup>1</sup> standard provides the requirements for use of encryption.

### **Definitions**

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

### **Standard**

System owners are required to analyze the risks to their systems and to ensure that adequate security controls are in place. If such an analysis indicates high residual risk to CONFIDENTIAL information despite deployment of all reasonable physical security measures and logical access controls, then encryption of the information is required.

Workforce members that use mobile computing devices (e.g. laptops, tablet computers, PDAs, smart phones) or mobile data storage devices (e.g. floppy disks, CDs, DVDs, flash memory, portable hard drives) are responsible for the protection of the data on those devices. This responsibility includes the use of encryption as outlined below, whether the devices are personally owned or furnished by UW Medicine.

---

<sup>1</sup> For purposes of HIPAA, UW 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; UW Physician's Eastside Specialty Center; Hall Health Primary Care Center; University of Washington Physicians; 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 & Disclosure of Protected Health Information – Organizational Requirements. UW School of Medicine is subject to the UW Medicine Information Security Program.

## I. Special Requirements for Passwords, PHI, and PII

UW Medicine has identified situations involving certain classes of confidential information that have elevated risks and for which encryption is required.

### A. Passwords

1. Passwords must be encrypted during transmission over any networks.
2. Passwords must be encrypted at rest on any computers, computerized devices, or digital storage systems.

### B. Protected Health Information (PHI)

1. PHI must be encrypted during transmission over networks not owned and/or operated by the UW, UW Medicine, or its affiliates.
2. PHI must be encrypted during transmission over any wireless networks (see *SEC-05.02 Wireless Networking Standard*).
3. PHI must be encrypted at rest on any mobile computing devices (e.g. laptops, tablet computers, PDAs, smart phones) and on any mobile data storage devices and media (e.g. floppy disks, CDs, DVDs, flash memory, portable hard drives).

### C. Personally Identifiable Information (PII)

1. PII must be encrypted during transmission over networks not owned and/or operated by the UW, UW Medicine, or its affiliates.
2. PII must be encrypted during transmission over any wireless networks (see *SEC-05.02 Wireless Networking Standard*).
3. PII must be encrypted at rest on any mobile computing devices (e.g. laptops, tablet computers, PDAs, smart phones) and on any mobile data storage devices and media (e.g. floppy disks, CDs, DVDs, flash memory, portable hard drives).

## II. Encryption Protocols

Whenever the use of encryption is required, the algorithms and methodology employed must be based on open standards which have undergone thorough analysis and which are currently deemed satisfactory by the cryptography community. See *SEC-05.03.01– Encryption Guideline* for current information.

## III. Protection of Passwords and Private Keys

Encrypted information is decrypted and made readable by use of a password (symmetric encryption systems) or a private key (public key or certificate-based systems). Passwords and private keys must be protected from unauthorized access or the encrypted information may also be accessible to unauthorized persons. If passwords or private keys are stored on disk or other forms of digital media, special care must be taken to provide logical access controls (e.g. file system permissions) and/or physical security measures (e.g. key stored on flash memory in a safe) that prevent access by persons other than its intended user(s).

#### **IV. Protections for the Availability of Encrypted Data**

If the keys, passwords, or other mechanisms used for decryption of information are forgotten, lost, or corrupted, the original information will be unrecoverable. Such an event could have a significant or severe impact on UW Medicine operations if the unrecoverable information is the only source of an important institutional data set. System owners planning to use encryption in this situation must ensure availability of the original information by implementing appropriate fault tolerance in their design. Fault tolerant designs may involve secure storage of multiple keys in several locations and ensuring that multiple staff members trained in recovery procedures are always available.

---

---

#### **References:**

- I.** 45 CFR Part 164; Section 164.308 (a) (5) (ii) (D) Password Management
- II.** 45 CFR Part 164, Section 164.312 (a) (2) (iv) Encryption and Decryption
- III.** 45 CFR Part 164; Section 164.312 (e) (2) (i) Integrity Controls, (ii) Encryption

---

---

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

Jim Fine M.D., CIO, ISO

---

---