Washington
WASHINGTON · UNIVERSITY · IN · ST · LOUIS
School of Medicine
Department of Radiation Oncology

HIPAA Security Procedure #15

EPHI Integrity and Authentication Procedure

Last Revised: 3/15/2006	*Approved: -*

Scope of Procedure
The scope of this procedure is to outline the appropriate data authentication measures implemented to insure that EPHI is not improperly altered or destroyed. Data authentication is the process used to validate data integrity, verify that the data sent is the same data that is received and insure the integrity of data stored and retrieved.

1) Transmission Integrity and Authentication

Mechanisms utilized to corroborate that EPHI is not altered or destroyed during transmission are described in OCF HIPAA Security Procedure # 17 – Transmission Security.

2) System Integrity

Mechanisms utilized to protect EPHI from alteration or destruction by a virus or other malicious code are described in OCF HIPAA Security Procedure # 11 – Server, Desktop, and Wireless Computer System Security).

3) Data at Rest Integrity

Mechanisms utilized to protect EPHI integrity during storage include: 1) Redundancy in data storage by using an appropriate RAID configuration; 2) A backup regimen appropriate to the application criticality and risk (For more detail, see OCF HIPAA Security Procedure # 7 – Data Backups and Contingency Planning).