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

HIPAA Security Procedure #5

Security Awarenss and Training Procedure

Last Revised: 3/15/2005	***Approved: 9/13/2005***

Security Awareness and Training Procedures

- Description of procedure for disseminating security reminders, updates and warnings

  Security updates, reminders and warnings will be communicated to the workforce using the Departmental intraweb (HIPAA Security Section), email or direct contact by phone or supervisor. The method depends upon the serverity and immediacy of the threat as determined by the HIPAA liaisons and the OCF.

- Description of determination the appropriate level of HIPAA Security Training for workforce members

  The Security Liaison will determine the appropriate Tier Level of training for each employee in the department per the directives in University HIPAA Security Procedure #5, Security and Awareness Training, which assigns training by job function.

- Description of method of accounting for HIPAA Security Training received for each member of the workforce

  The Privacy Liaison will advise each existing employee (and new employees) of the level of training required and the procedure for completing training. The Privacy Liaison will keep a log containing the name of the employee, job classification, training level required, date the training was completed and date the training log was last reviewed for that employee. The Privacy Liaison will continually track employee training in the log to insure that training is completed in a timely manner and to reevaluate training needs when an employee's job function changes.

Login Monitoring Procedures for system containing medium or high risk EPHI

- Procedures to log and monitor system activity
  (See #14 RO HIPAA Security Procedure: Audit Controls Policy)

- Procedures to review audit logs, activity reports, etc.
  (See #14 RO HIPAA Security Procedure: Audit Controls Policy)

- Procedures to insure that audit logs, activity reports, etc. are reviewed at an interval of no more than 90 days
  (See #14 RO HIPAA Security Procedure: Audit Controls Policy)

- Procedures to document the set of systems and applications that require auditing and review (See #14 RO HIPAA Security Procedure: Audit Controls Policy)

- Procedures for the creation, maintenance, and implementation of a formal Audit Control and System Activity Review Plan (Note: a formal Audit Control and System Activity Review Plan must also be submitted to the HIPAA Security Office) (See #14 RO HIPAA Security Procedure: Audit Controls Policy)

Virus, Worm, and other Malicious code Detection and Prevention Procedures

- Description of the virus detection system(s) implemented on all appropriate systems

  For Windows systems, the latest version of McAfee (or equivalent) antivirus available from the NTS software library is used.

- Description of mechanisms to ensure all virus detection systems are kept up-to-date

  For Windows systems, RO will use remote inventory/update software to check versions of operating system and virus detection software when a system connects to the network. Unprotected systems will not be authenticated to the network.

- Description of the reporting and notification process for any identified viruses, worms, or other malicious software and the appropriate entities to receive those notifications

  (See Procedure #6 Incident Response and Reporting)

- Description of plan to ensure that all systems that become affected by a virus, worm, or other malicious software are repaired in a timely fashion or isolated from the network

  RO procedure and practice is to immediately disconnect an infected computer from the network, clean and test before reconnecting to the/a network. An OCF technician is either directly involved in the cleaning/testing activity or the technician will track the cleaning/testing process.

- Description of plan to insure that a system is free of viruses, worms, or other malicious software before that device is moved or transferred to a new network or location

  RO practice is to immediately disconnect an infected computer from the network, clean and test before reconnecting to the/a network. An OCF technician is either directly involved in the cleaning/testing activity or the technician will track the cleaning/testing process. Departing staff must allow computer equipment checkout by OCF technicians before departure.

- Description of plan to make all workforce members aware of your virus detection systems and procedures

  The Departmental intraweb (HIPAA Security Section) will detail department policies/procedures regarding virus detection and reporting.

Password Management Procedures for systems and networks containing EPHI

- Description of plan to insure that all workforce members who access networks, systems, or applications used to access, transmit, receive, or store EPHI are supplied with a unique user identification and password

  System managers of systems that manage EPHI are tasked with management of access by unique user identifier and password according to the policy prescribed in University HIPAA Security procedure #13, Technical Safeguards, Access Control Policy. User requests for access must be directed to the appropriate system manager and must originate from proper authority (Supervisor, Department Manager of Administrative Services, etc).

- Description of plan to insure that workforce members are required to supply password in conjunction with their unique user identification to gain access to any application or database system used to create, transmit, receive, or store EPHI

  By department policy, all desktop computers, portable computers and servers in Radiation Oncology are set up to utilize username/password security to access the local computer as well as the departmental network.

- Description of plan to insure that passwords used to gain access to any network , system, or application used to access, transmit, receive or store EPHI meet your minimum password structure

Password structure on Windows systems is enforced automatically by an algorithm. Password structure on VMS and Unix (Linux) systems is enforced by the system manager at set up time.

- Description of plan to train your internal password policies including password structure, timeouts and proper password safeguard procedures

Password timeout policy and safeguard policies will be posted on the departmental intraweb for all workforce members. Password structure should be communicated only on a need-to-know basis by the system manager at set up time or by the change-password feature of the particular system.