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

HIPAA Security Procedure #2

Risk Assessment and Management

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

- Description of process to inventory EPHI and reassess inventory

Department policy requires each employee to complete a Database/Repository form listing all EPHI repositories for which the employee serves as custodian (see attached). All forms are returned to the Privacy Liaison. Using the Risk Algorithm (below), the Privacy Liaison and Security Liaison review and determine a risk factor for each repository listed on the forms. Employees may challenge the risk factor which can ultimately be arbitrated by the RO HIPAA Security task force composed of RO systems managers. The Privacy Liaison will log each multi-user repository in the WU common catalogue. New employees complete the Database/Repository form at orientation. These forms are retained for six years by the Privacy Liaison.

In April of each year, every employee in the department will be required to reassess the databases and repositories for which they serve as custodian. The previous year's form will be reviewed, updated and forwarded to the Privacy Liaison. The above procedure of reviewing, assigning a risk factor and logging into the WU common catalogue will be followed for new and modified entries. Deleted entries will be updated in the WU common catalogue. These forms will be retained for six years by the Privacy Liaison.

Risk Algorithm: Sensitive data is always high risk. A high number of users and a high number of records is high risk. A low number of users and a low number of records is low risk. A high number of records or a high number of users is medium risk. One or more mitigating factors can reduce the risk of the database/repository.

- Description of parameters for classifying EPHI repositories
    - Number of users
    - Number of records
    - Sensitivity of data (AIDS test results, etc.)
    - Mitigating factors
        - Requires special software/hardware to access/interpret
        - Requires special training/knowledge to interpret
        - Other mitigating factors

- Description of potential THREATS to EPHI repositories
    - Natural Disaster
        - Fire
        - Earthquake
        - Storm
    - Misuse (intentional or accidental)

    - Environmental
        - Power Interruption
        - Communications Interruption
        - HVAC Interruption

- Description of VULNERABILITY to potential threats named above

    - Natural Disaster
        - Fire
        - Earthquake
        - Storm

    Discussion: Vulnerability: MEDIUM. Network authentication and basic service is not yet available in each work location. Contingency plans are not fully defined to HIPAA specificity.

    - Misuse (intentional or accidental)

    Discussion: Vulnerability: MEDIUM. Although backup policy is operational, workforce is not yet trained for HIPAA Security. All ROC HIPAA Security procedures are not yet formalized and in place.

    - Environmental
        - Power Interruption
          Vulnerability: LOW. Power Distribution Units, Uninterruptible Power Supplies and backup generator(s) are in place.

        - Communications Interruption
          Vulnerability: MEDIUM. A redundant backup communications path is not yet in place between 4511 Forest Park and CSRB.

        - HVAC Interruption
          Vulnerability: LOW. Steps can be taken to decrease the cooling requirement. Service is dependable and local.

- Description of RISK (Threat X Vulnerability X Impact) associated with each vulnerability

    - Natural Disaster   Risk: MEDIUM
        - Fire
        - Earthquake
        - Storm

    - Misuse (intentional or accidental)   Risk: MEDIUM

    - Environmental

Power Interruption	Risk: LOW
Communications Interruption	Risk: MEDIUM
HVAC Interruption	Risk: LOW

- Description of safeguards used to mitigate identified risks

    - Natural Disaster
        - Fire
        - Earthquake
        - Storm

      1. Review and update disaster and contingency plans to HIPAA specificity.
      2. Add network authentication and basic computing services in each work location so users in location can function if wider LAN communication is interrupted.

    - Misuse (intentional or accidental)

      1. Develop RO HIPAA Security Procedures to implement WU HIPAA Security policy
      2. Implement RO HIPAA Security Procedures
      3. Train workforce on WU HIPAA Security policy as well as RO HIPAA Security Procedures

    - Environmental
        - Power Interruption
        - Communications Interruption
        - HVAC Interruption

      1. Install and configure a redundant backup network communications path between the 4511 Forest Park location and the CSRB location.

Audit Control and System Activity Procedures for systems containing medium and 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)