BEFORE THE BOARD OF COUNTY COMMISSIONERS
FOR MULTNOMAH COUNTY, OREGON

RESOLUTION NO. 05-050

Adopting Multnomah County HIPAA Security Policies and Directing the Appointment of Information System Security Officers

The Multnomah County Board of Commissioners Finds:

a. Multnomah County is a "hybrid covered entity" under the federal Health Insurance Portability and Accountability Act. (HIPAA).

b. As a hybrid covered entity, Multnomah County must adopt and implement policies regarding the protection of electronic protected health information.

c. Multnomah County is required by HIPAA to appoint a central person as the "Security Officer" for the County.

The Multnomah County Board of Commissioners Resolves:

1. To adopt the attached set of HIPAA Security Policies for implementation in Multnomah County and directs the Clerk of the Board to maintain a complete set, including any amendments.

2. To direct affected covered components within the "hybrid covered entity" to develop procedures, as needed, specific to their work sites implementing these policies and to submit all procedures, including revisions, to the designated Information Systems Security Officer in the Department of Business and Community Services, DBCS.

3. To direct covered components to designate a "security official" for that component who will be the component's contact for all matters relating to HIPAA security.

4. To direct the Chief Information Officer of DBCS to designate one or more employees of that department to serve as Information System Security Officers.

ADOPTED this 7th day of April, 2005.

BOARD OF COUNTY COMMISSIONERS
FOR MULTNOMAH COUNTY, OREGON

Diane M. Linn, Chair

REVIEWED:

AGNES SOWLE, COUNTY ATTORNEY
FOR MULTNOMAH COUNTY, OREGON

By _____
Jacqueline A. Weber, Assistant County Attorney

Multnomah County HIPAA Security Policies

Table of Contents

Multnomah County HIPAA Security Policies

Introduction

Multnomah County is a "hybrid covered entity," as set forth in Board Resolution 93-006, under the federal Health Insurance Portability and Accountability Act (HIPAA). The following policies are designed to protect the confidentiality, integrity and availability of individuals' electronic Protected Health Information (ePHI) when it is stored, maintained or transmitted and to fulfill Multnomah County's obligations under HIPAA's Security Rule.

1. Data Classification, Storage, Backup and Recovery, 45 CFR 164.308

Definitions:

- *Electronic Protected Health Information (ePHI)*: Individually identifiable health information (past, present or future physical or mental health or condition, or provision of health care) including demographic data that can identify an individual, maintained or transmitted using electronic media.
- *Source Record*: Source systems or files contain one or more data items that are original input and not contained in other systems or files within the County. Source data is often entered via a keyboard by a system or file user.
- *Derivative Record*: All records not classified as source records. These records can be reconstructed in their entirety from other systems or records.
- *Critical Record:* Records without which an individual work unit would be unable to do its work.
- *Mission Critical Record:* Records whose loss would result in large numbers of County employees being unable to do their work, or where highly critical and urgent services required by the public would not be able to be performed.

General Requirements:

a. Each Multnomah County covered component will assess its electronic records to identify the data as:

   - containing or not containing ePHI;
   - source or derivative;
   - not critical nor mission critical or critical or mission critical.

b. Records containing ePHI must be stored securely to prevent unauthorized access to them. Normally this means they will be stored on a server or on a shared network storage device in an access controlled area and not on a computing device in the work area.

c. Records containing ePHI that are also source records must be backed up in a manner that will allow them to be restored if they are lost or damaged.

d. Source records that are critical or mission critical records must also be the objects of a disaster recovery plan.

e. Source records that are mission critical records will be scheduled for restoration before critical records.

2. Network Communication Encryption, 45 CFR 164.312

To protect external ePHI transmissions, Multnomah County will:

- encrypt or password-protect any file, document, or folder containing ePHI before transmission, or, as an alternative, the transmission data stream itself may be encrypted.
- take reasonable precautions to authenticate the receiving party and ensure there is a business need for the requested ePHI; transmissions of ePHI should include only the minimum amount of PHI necessary to accomplish the business need.

To protect internal ePHI transmissions, Multnomah County will encrypt all internal wireless data transmissions.

3. Access Control - Passwords, 45 CFR 164.312; Application Ownership, 45 CFR 164.308

Multnomah County will implement technical procedures for electronic information systems that contain ePHI to uniquely identify and track users for the purpose of access control to all networks, systems, and applications that contain ePHI and for monitoring that access. These will include standards for password creation, maintenance, and protection and application ownership and access.

4. Employment Termination, 45 CFR 164.308

All workforce members must follow the procedures developed by the Security Officer and the covered component's security official to safeguard the County's computing resources when an employee, volunteer, or contractor terminates their service with the County whether such termination is voluntary or for some other reason.

5. Portable Devices, 45 CFR 164.308

Portable computing devices and removable media connecting to Multnomah County network resources must meet all requirements applicable to non-portable computing devices at the County with respect to ePHI.

6. Security Sanctions, 45 CFR 164.308

Multnomah County will impose the following sanctions for any violation of County's policies or procedures implementing HIPAA security rules, including any attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system:

a. Employee disciplinary sanctions will be proportional to severity of the violation and will be determined in the same manner and by the same authorities as other personnel rule violations.

b. Non-Employee (including volunteers, students, external business partners and contractors) sanctions will be specified by contract or if not specified may include restricted or terminated access to County facilities and/or the County Wide Area Network (WAN) as determined by the Security Officer in consultation with the Director of the Department in which the violation occurred. The severity of the consequences to the non-employee workforce member must be proportional to the severity of the violation.

7. External Business Partner Access, 45 CFR 164.308

Multnomah County will develop procedures to ensure access to County WAN resources and systems provided to external business partners complies with the following County security policies.

a. WAN access for external business partners (as well as any exceptions to any part of this external business partner access policy) must be requested in writing and approved by the IT Division in a manner set forth in the procedure.

b. All agreements between a sponsoring department and an external business partner that result in provision of County WAN access to the external business partner must be in writing.

c. The sponsoring department must require external business partners to:

- undergo and pass the same (or enhanced) procedures used to ensure network and information security as are practiced by the sponsoring department's employees. These may include but are not limited to criminal history or required background checks for access to the Oregon Law Enforcement Data System or the National Crime Information Center and signing of confidentiality or non-disclosure agreements.
- run anti-virus software on all desktop or laptop computers that have Multnomah County WAN connectivity.
- comply with County Personnel Rule 3.35 for appropriate use of information technology, complete the sponsoring department's HIPAA training requirements; and comply with all policies (including those that apply specifically to HIPAA regulations, if applicable) and procedures developed to ensure the security and integrity of the County's network, applications, and information.
- immediately notify the sponsoring department when network login IDs are no longer in use or required; and sponsoring departments must immediately notify the County's Help Desk.

d. Personal Computers or laptops used by the external business partners must not have connections to any other network unless through the central County firewall or through a local firewall, router or Virtual Private Network device managed by IT WAN Services.

This hardware, and the software loaded thereon, is subject to approval by the IT Division's Senior IT Manager for Infrastructure.

e. All devices, switches, routers, and all other non-desktop hardware required to support the connectivity of external business partners and the traffic segmentation thereof must be provided by County IT WAN Services. County IT WAN Services is solely responsible for management of these devices.

8. Business Associate Agreements, 45 CFR 164.314

a. Multnomah County covered components may share ePHI among all other covered components for any purpose permitted by HIPAA rules, state and federal laws, and county HIPAA policies, without formal agreements.

b. No covered component of Multnomah County may share ePHI with entities other than Multnomah County covered components without a written agreement that includes HIPAA business associate requirements, except as allowed by HIPAA rules.

9. Information Security Program, 45 CFR 164.306; 164.308; 164,310; 164.312; 164.316

a. Multnomah County will protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and uses or disclosures of such information that are not permitted by law.

b. The Multnomah County Chief Information Officer will appoint or designate one or more Security Officers for the County. The Security Officers are responsible for developing and implementing an information security program based upon the County's HIPAA policies, including:

- Performing a county-wide information security risk assessment at least once every three years, including HIPAA training program review for completeness and continuing relevance. The assessment shall include any necessary updates to the County's information processing emergency procedures, backup and recovery, and disaster plans;
- performing and analyzing random application security audits at least annually;
- preparing action plans;
- evaluating vendor products;
- participating in system development projects;
- assisting with control implementations;
- investigating information security breaches; and
- performing other activities necessary for a secure information handling environment.

c. The Security Officers will work closely with security officials within the covered components, facilitating regular Security Team meetings. The Security Officers are authorized to have direct access or communication with department directors and the Chief Operating Officer.

10. Email Encryption, 45 CFR 164.312

All email containing ePHI sent externally must be encrypted using County provided automated tools. These requirements shall take effect immediately upon the IT Division making such tools available in the production environment.

a. Transmission of ePHI from Multnomah County to a client by email or messaging system is permitted if the sender has ensured that the following conditions are met:

- The client or personal representative has been made fully aware of the risks associated with transmitting ePHI via email or messaging systems.
- The client or personal representative has authorized Multnomah County in writing to use an email or messaging system to transmit ePHI to them. This authorization shall be stored in the client's record.
- The email or message contains only the minimum ePHI necessary to accomplish the business purpose of the email.

b. The transmission of ePHI from Multnomah County to an outside entity other than a client or personal representative via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

- The receiving entity has been authenticated, is aware of the transmission and is ready to receive said transmission.
- The sender and receiver are able to implement a compatible encryption mechanism.
- All attachments containing ePHI are encrypted or password protected and the password is conveyed to the recipient by a separate communication.

11. Information Security Incident Response, 45 CFR 164.308

Multnomah County will implement procedures to address security incidents, including:

- identifying and responding to suspected or known security incidents;
- mitigating, to the extent practicable, harmful effects of known security incidents; and
- documenting security incidents and their outcomes.

12. Policies and Procedures Requirements, 45 CFR 164.308 and 164.316

Multnomah County will implement and maintain policies and procedures to comply with the requirements of the Health Insurance Portability and Accountability Act and its Security Rule. The County may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this policy.

All such policies and procedures will be reviewed for completeness, continuing appropriateness in their response to environmental or operational issues affecting the security of electronic protected health information, and continuing compliance with law at a

minimum of once every two years and updated as needed. This review must occur no less frequently than every two years and shall be directed or arranged for by the Security Officer.

Documentation: (Note that all written documentation may be in electronic form.)

The policies and procedures implemented to comply with the HIPAA Rule shall be documented. All actions, activities, or assessments performed to comply with the HIPAA Rule shall be documented. Multnomah County will retain records relating to the HIPAA Security Rule in compliance with federal and state laws and retention schedules. Records referenced in this policy shall be retained for a minimum of six years from the date of their creation, or the date when last in effect, whichever is later.

13. Workstation and Disposal of Information, 45 CFR 164.308; 164.310; 164.312

Multnomah County will develop procedures to implement workstation security measures which will:

- prevent accidental data disclosures;
- protect the integrity of ePHI; and
- delineate requirements for disposal of ePHI and the hardware on which it was stored; and
- ensure the County's compliance with HIPAA.

14. Access Control and Physical Security, 45 CFR 164.308; 164.310; 164.312

Multnomah County recognizes the HIPAA Security Rule requires that access to sensitive data, particularly ePHI, be restricted to known users with a business need to access the information. Multnomah County staff seeking access to any network, system, or application that contains ePHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, token/fob or a user identification smart card to verify their authenticity.

Physical access to all facilities containing servers shall be controlled by means consistent with the procedures the County will develop for the purpose.

15. HIPAA Privacy and Security Awareness and Training, 45 CFR 164.308

All County workforce members in the hybrid covered entity must receive HIPAA training. Contractors who have no access to ePHI or whose contract already requires them to possess HIPAA security knowledge are exempt from this policy. HIPAA training which meets minimum requirements to be detailed in administrative procedure must be documented either in Business Associate Agreements for contractors or in SAP.

Tracking non-employee training is the responsibility of the employing County Department. Such records must be maintained for the duration specified in County record retention schedules.