TITLE:	**Health Insurance Portability And Accountability Act (HIPAA) Security Rule Requirements**	**PROCEDURE #:**	**521-A**
DEPT:	**Business Services**	**DIVISION:**	**Risk Management**
EFFECTIVE DATE:	**8/08**	**REVIEWED:**	**REVISED:**

OBJECTIVE: To establish procedures in compliance with the *Health Insurance Portability and Accountability Act (HIPAA)* Security Rule regulations to protect the confidentiality, integrity, and availability of our electronic protected health information.

REFERENCE: Policy # 521

POLICY STATEMENT: Marion County will follow the administrative, physical and technical standards for electronic protected health information as promulgated in the U.S. Department of Health and Human Services Security Rule regulations. Accordingly, Marion County will:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information we create, receive, maintain, or transmit.

2. Ensure that EPHI is protected against any reasonably anticipated threats or hazards to the security or integrity of EPHI and reasonably prevent any possible uses or disclosures of EPHI that are not permitted by law.

3. Establish an Information Security Program that complies with *HIPAA* Security and Privacy regulations, State privacy regulations and State DHS policies (required under contract).

4. Provide for enforcement of and sanctions for violations of Administrative Policy 521 and these procedures or those of a covered component.

These procedures are intended to be consistent with Marion County HIPAA Security Rule Policy Guidelines, which are based upon International Standards Organization (ISO) standards, initially adopted by Board of Commissioners Resolution No. 05-14R on April 18, 2005.

APPLICABILITY: These procedures are in addition to all other state or federal guidelines, statutes, administrative rules, covered component departmental policies, or other provisions relating to personal health information. In general, the provision that provides the greatest degree of confidentiality, integrity and

security prevails. HIPAA provides exemptions from its provisions for certain personal health information, for example information regarding applicants or employees held by an employer for employment purposes, or personal health information regarding inmates in the correctional facility; however, these records are still protected by other laws. Any ambiguities in these procedures, or conflicts between these procedures and another procedure, shall be construed so as not to be conflicting with HIPAA, the Privacy or Security Rules.

These procedures apply to all information resources that are owned or leased by Marion County and that use, store or transmit electronic protected health information. The same administrative, physical and technical security measures will be implemented for non-mobile, mobile and remote computers.

Persons who have been granted access to county information systems and information assets, including but not limited to, full and part-time employees, temporary employees, volunteers, contractors, those employed by others to perform county work, are covered by and will comply with these procedures and other associated policies, procedures and guidelines.

Transmissions of protected health information on paper, or by fax, voice, and telephone (voice) are not considered to be electronic in nature and are not covered by *this* policy. Rather these types of non-electronic PHI and these types of conveyance are covered in the Marion County Administrative Policy and Procedures G-13 and other related privacy policies.

PROCEDURES:

In compliance with the Health Insurance Portability and Accountability Act of 1996, the Marion County Board of Commissioners adopted, the Marion County HIPAA Security Rule Policy.

The following procedures establish the Marion County Information Security Program for purposes of complying with the Health Insurance Portability and Accountability Act of 1996, Security Rule.

A. Administrative, Technical and Physical Safeguards

Each Marion County covered component will ensure that consistent with the "Marion County HIPAA Security Rule Policy Guidelines," appropriate administrative, technical and physical safeguards are taken to ensure the confidentiality, integrity, and availability of all electronic protected health information created, received, maintained, or transmitted on behalf of the entity and that EPHI is protected against any reasonably anticipated threats or hazards to the security or integrity of EPHI and reasonably prevent any possible uses or disclosures of EPHI that are not permitted by law.

In particular, each covered component will address the following in relation to safeguarding protected health information:

Administrative Safeguards:

1. Analyze their risks to security and implement policies and procedures that prevent, detect, and correct security violations.

2. Identify the individual responsible for overseeing development of the organization's security policies and procedures.

3. Adopt policies and procedures to ensure that members of the work force have access to information appropriate for their jobs and clear termination procedures.

4. Implement procedures authorizing access to EPHI.

5. Implement security awareness and training programs for all members of the workforce, including management.

6. Adopt policies and procedures for reporting and responding to information security incidents.

7. Adopt policies and procedures for responding to an emergency or occurrence (such as fire, vandalism, or natural disaster) that damages equipment or systems containing EPHI such that information is not available to caregivers when and where it is needed.

8. Periodically monitor adherence to security policies and procedures, document the results of monitoring activities, and make appropriate improvements in policies and procedures.

9. Ensure that contracts between a covered component and business associates provide satisfactory assurance that appropriate safeguards will be applied to protect the EPHI created, received maintained or transmitted on behalf of the entity.

Physical Safeguards:

1. Limit physical access to equipment and locations that contain or use EPHI.

2. Specify the proper functions to be performed, the manner in which those functions are to be performed and the physical attributes of the surroundings of a specific workstation or class of workstation.

3. Specify how workstations permitting access to EPHI are protected from unauthorized use, including portable workstations such as laptops and PDAs.

4. Address the receipt and removal of hardware and electronic media that contain EPHI including the use, reuse and disposal of electronic media containing EPHI both within and outside the organization.

Technical Safeguards:

1. Specify how access to EPHI will be limited to persons or software programs requiring the EPHI to do their jobs.

2. Ensure hardware, software or manual mechanisms are installed to examine activity in systems containing EPHI.

3. Ensure that EPHI is protected from unauthorized modification or destruction.

4. Implement measures to prevent unauthorized users from accessing EPHI.

5. Ensure EPHI is protected when being transmitted electronically from one organization to another.

Organizational Requirements:

1. Document that business associate contracts or other arrangements comply with information security measures when handling EPHI.

2. Comply with safeguard requirements specified in group health plan documents.

B. Training of Workforce

Marion County will train its employees concerning Marion County's policies and procedures regarding the security of protected health information, as necessary and appropriate depending on the duties and responsibilities of the employee. Each covered component will train its employees on the more specific policies and procedures of that covered component if applicable. In addition, all new employees or employees who are promoted or transferred into a position with access to protected health information will be trained on the relevant policies and procedures. Completion of training will be documented.

C. Review and Resolution of Security Complaints

Each Marion County covered component will provide a process for individuals to make security complaints concerning Marion County's compliance with HIPAA and the Security Rule. All security complaints received will be investigated and appropriate follow-up measures taken.

D. Enforcement and Sanctions Against the Covered Entity and Its Employees

HIPAA provides for civil penalties and sanctions, as well as criminal penalties, for violations both against the covered entity and the county's officers, employees or agents. Sanctions can include loss of federal funding.

1. Civil Penalties and Sanctions - A civil penalty of up to $100 per violation and $25,000 per year for identical violations may be imposed against the covered entity or any person who violates HIPAA or the Security Rule regulations, and for general failure to comply with the requirements and standards. Other civil sanctions may include injunctive relief or loss of federal funding.

2. Criminal Penalties - Criminal penalties may be imposed for knowing and wrongful disclosures in violation of HIPAA. Depending on the category of the offense, criminal fines can be up to $50,000, $100,000 or $250,000, and imprisonment of up to 1 year, 5 years or 10 years.

3. Disciplinary Actions - Marion County as a hybrid covered entity must apply appropriate disciplinary sanctions against an employee who fails to comply with the county or covered component's HIPAA security policies and procedures, up to and including termination.

    a. Just Cause - Failure to comply with the county's or covered component's HIPAA security policies and procedures is considered just cause for disciplinary action under the Marion County Personnel Rules, Article 9, Section 3.

    b. Disciplinary Process - Employees who fail to comply with the county's or covered component's HIPAA security policies and procedures shall be disciplined pursuant to the applicable Personnel Rules and collective bargaining agreements up to and including termination.

E. Documentation of Policies and Procedures

Written or electronic records of policies and procedures implemented to comply with the Security Rule shall be maintained for a period of six years from the date of creation or the date when last in effect.