SECTION:	**Health, Safety & Security**			**POLICY #:**	**521**
TITLE:	**Health Insurance Portability And Accountability Act (HIPAA) Security Rule Requirements**			**PROCEDURE #:**	**521-A**
				ORDER #:	**08-114**
DEPT:	**Business Services**			**DIVISION:**	**Risk Management**
ADOPTED:	**8/06**	**REVIEWED:**	**7/08**	**REVISED:**	**8/08**

PURPOSE:

The *Health Insurance Portability and Accountability Act (HIPAA)* Security Rule regulations require the county, as a "hybrid covered entity" to comply with standards to protect the confidentiality, integrity, and availability of our electronic protected health information. This policy and its corresponding procedures will form the basis of our response to protect electronic protected health information and to comply with the federal regulations.

The county will implement security measures that work well with the HIPAA Privacy Rule measures already implemented, and therefore both sets of measures and policies will be supportive and complementary in nature.

AUTHORITY:

Authority for this policy is 45 CFR Parts 160, 162 and 164 and is named the Health Insurance Portability and Accountability Act which includes Security Standards; Final Rule, published on 2/20/2003, including any modifications of the Security Rule published at a later date. The HIPAA Security Rule became effective for Marion County on April 20, 2005.

APPLICABILITY:

This policy is 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 this policy, or conflicts between this policy and another policy, shall be construed so as not to be conflicting with HIPAA, the Privacy or Security Rules.

This policy applies to all information systems, computers and other digital and peripheral equipment as defined in this policy 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, and those employed by others to perform county work, are covered by this policy and will comply with this 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 conveyances of PHI are covered in the Marion County Administrative Policy and Procedures 517 and other related privacy policies.

DEFINITIONS:

"Administrative Safeguards" means administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information and to manage the conduct of the county's workforce in relation to the protection of that information.

"**Business Associate**" means an outside entity or individual that performs, or assists in the performance of, the functions or activities of a covered entity involving the use or disclosure of individually identifiable health information.

"Confidentiality" means the property that data or information is not made available or disclosed to unauthorized persons or processes.

"**Covered component**" means a part of the county that provides health care (e.g., the Health Department) and engages in certain electronic transactions, or has access to or uses protected health information, and as such is directly subject to HIPAA. Departments or positions that are not involved in providing health care and do not have access to or use protected health information of clients or customers are generally not subject to HIPAA.

"EPHI (Electronic Protected Health information)" means individually identifiable health information (information about the past, present or future physical or mental health or condition, or provision of health care) including demographic data (but excluding data maintained by an employer in its role as employer) that can identify an individual, maintained or transmitted using electronic media.

"**Hybrid covered entity**" means an entity, the primary function of which is other than to provide health care, although some of its departments provide health care. Marion County is a "hybrid covered entity."

"Information Resources" means any and all online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it means the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

"Information Security Incident" means emergencies, attacks, and unauthorized access, use, disclosure, modification or destruction of information, or interference with system operations in any information system, as well as disasters that may or have affected the confidentiality, availability or integrity of electronic protected health information whether attempted or successful. This includes:

(1) Unauthorized physical entry into a department or the county's IT facilities, or attempted unauthorized physical entry to such facilities;

(2) Unauthorized electronic entry or attempted unauthorized electronic entry, into information processing systems, networks, or information storage, or information transmission resources;

(3) Situations which appear to have risked unauthorized disclosure of information as well as confirmed disclosure;

(4) Any violation of department or county information security policies.

"Integrity" means the property that data or information have not been altered or destroyed in an unauthorized manner.

"Protected Health Information (PHI)" means individually identifiable health information that is transmitted or maintained electronically or by using any other medium.

"Physical Safeguards" means physical measures, policies, and procedures to protect electronic information systems and related buildings and

equipment, from natural and environmental hazards, and unauthorized intrusion.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

"Technical Safeguards" means the security controls (i.e., safeguards and countermeasures) applied to an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

"Unauthorized Use" means any unauthorized action that damages or disrupts the computer system, alters its normal performance, causes it to malfunction or results in unauthorized access, use, disclosure, modification or destruction of information.

"User" means a person or entity with authorized access to information systems.

"Violation" means any act that is inconsistent with or against a department or county policy or procedure established pursuant to the implementation of the Security Rule regulations of the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, including, but not limited to, any attempted or successful unauthorized access, use, disclosure, modification or destruction of EPHI or interference with operations in an information system.

GENERAL POLICY: 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 this policy, its related procedures or policies and procedures of a covered component.

This policy and its related 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.

POLICY GUIDELINES:

1. Responsibilities:

Elected officials, department heads, managers and supervisors have the overall responsibility for the security of information and for providing the necessary resources and support for the program.

Covered components will assist in determining the data's sensitivity and classification levels and should have an active role in designing access controls for their systems. They should be accountable for the accuracy of the information. Covered components should also assist in designing audit systems for their systems.

Covered components cannot disclose protected health information to non-covered components except as permitted by this policy. Covered components can only disclose protected health information as permitted under HIPAA. Certain non-covered components may have obligations under HIPAA as "business associates."

Information systems security professionals have the technical expertise and knowledge of options available to ensure security. They are responsible for implementing and maintaining information security within the organization's current configuration.

Users are responsible for following established policies and procedures and for alerting managers, supervisors, or security officers of security breaches or information security incidents.

2. Exceptions:

The county's Security Officer will be authorized to approve or deny policy exceptions regarding any requirements of this policy and related procedures. The security officer appointed for a covered component will be authorized to approve or deny policy exceptions regarding that covered component's information security policies and related procedures. Policy exception requests will be submitted by a supervisor electronically in writing or in writing on hard copy form to the county or covered component's Security Officer. Policy exception requests for policies of a covered component will be processed according to policies adopted by the covered component.

3. Implementation:

Security Officers for the county and the Health Department, a covered component of the county, will be designated by order of the Marion County Board of Commissioners. Security Officers are responsible for ensuring compliance with the HIPAA Security Rule through the implementation, management and monitoring of county security policies and any applicable department policies.

The county, its officers, employees and agents may be subject to civil penalties and fines for violations of HIPAA, or may be subject to criminal penalties for knowing, wrongful violations. Employees may be subject to discipline, up to and including termination, or business associates may have their contracts terminated.

4. Periodic Review:

This policy and its related procedures will be reviewed at least once every two (2) years to accommodate organizational or environmental changes.