

Administrative Order



Administrative Order No.: 10-11

Title: Privacy Standards

Ordered: 7/8/2003

Effective: 7/18/2003

AUTHORITY:

Section 4.02 of the Miami-Dade County Home Rule Amendment and Charter

POLICY:

It is the policy of Miami-Dade County and all its departments to protect the privacy and confidentiality of all customers' identifiable, personal, confidential information including, but not limited to, protected health information as required by federal, state, and local laws.

SCOPE:

Miami-Dade County, in the effort to protect all identifiable, personal and confidential information including, but not limited to, protected health information shall:

- Develop and maintain policies and procedures to ensure confidentiality and security as required by federal, state, and local laws, and to ensure the appropriate handling, maintenance, dissemination and sharing of all identifiable, personal, confidential, and protected health information;
- Educate its employees regarding appropriate policies and procedures regarding the protection of all identifiable personal and confidential information including, but not limited to, protected health information;
- Require full compliance from its business associates and trading partners with applicable federal and state regulations regarding identifiable personal and confidential information including, but not limited to, protected health information; and
- Inform the public of their rights to protection of all identifiable personal and confidential information including, but not limited to, protected health information.

GENERAL TERMS, AS USED IN THIS ORDER SHALL MEAN:

- **Customer:** is any individual or group served either directly or indirectly (e.g., by Memoranda's of Understanding (MOU's), contracts) by Miami-Dade County, or employed by Miami-Dade County.
- **Privacy:** provides the customer with the right and ability to control and access his/her identifiable personal and confidential information including, but not limited to, protected health information.
- **Confidentiality:** provides a means of protecting any customer's identifiable and personal information that has been received by an entity (e.g., Miami-Dade County), by safeguarding it from unauthorized disclosure.
- **Security:** applies to the spectrum of physical, technical, and administrative safeguards, including physical storage and maintenance, transmission, and access to individual health information, that are put in place to protect the integrity, availability, and confidentiality of information.
- **Chief Privacy Officer:** is the designated, Countywide-level individual responsible for the monitoring and enforcement of departmental privacy policies and procedures, responsible for providing assistance to departments regarding privacy issues, responsible for developing and implementing privacy complaint resolution process policies and procedures, responsible for receiving and handling privacy complaints, and who is able to provide further information about matters covered by the Notice of Privacy Practices (NOPP).
- **Departmental Privacy Liaison:** is the designated, department-level individual who is responsible for the development and implementation of the department's privacy policies and procedures; and who is responsible for receiving and handling complaints referred by the Chief Privacy Officer, and who is able to provide further information about matters covered by the provider's Notice of Privacy Practices (NOPP).
- **Identifiable, Personal, Confidential Information:** includes, but is not limited to name, social security number, date of birth, marital status, address, phone number, demographic information, and diagnosis.

HIPAA RELATED TERMS, AS USED IN THIS ORDER SHALL MEAN:

- **Health Insurance Portability and Accountability Act:** of 1996 (Public Law 104-191), known as HIPAA, is designed to improve the efficiency and effectiveness of the healthcare system through: (1) security standards protecting the confidentiality and integrity of past, present or future "individually identifiable health information"; (2) standardization of electronic patient health,

administrative and financial data; (3) unique health identifiers for individuals, employers, health plans, and healthcare providers.

- **Business Associate:** is a person or entity who performs a function or assists a Covered Entity (e.g., Miami-Dade County) with a function or activity involving the use or disclosure of “individually identifiable health information” (IIHI). Examples of functions include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, proactive management, and repricing; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.
- **Covered Entity:** is one or more of the following: a Health Plan, a Healthcare Clearinghouse, or a Health Care Provider who transmits any health information in electronic form (e.g., e-mail, fax) in connection with a transaction covered by HIPAA.
- **Protected Health Information (PHI) or Individually Identifiable Health Information (IIHI):** is any information related to a customer’s health, health care, or payment for health care that identifies the individual.

PHI/IIHI may be:

- oral or recorded, in any form or medium (including information maintained on laptops, floppy disks, and at an employee’s home);
 - created or received by a Healthcare Provider, Health Plan, public health authority, employer, life insurer, school or university or Healthcare Clearinghouse; and
 - related to the past, present, or future physical or mental health or other condition of any customer; the provision of healthcare to a customer; or the past, present or future payment of healthcare to a customer.
- **Healthcare Provider:** is a provider of medical, mental health, substance abuse and/or social services including: institutional providers (e.g., hospitals, skilled nursing facilities, home health agencies, ambulance services, comprehensive outpatient rehabilitation facilities); facilities and practitioners (including clinics and centers, physicians, clinical laboratories, pharmacies, nursing homes, licensed/certified health care practitioners and suppliers of durable medical equipment); and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business,

related to the health of an individual.

Health Plan: is the customer's individual or group plan that provides, or pays the cost of, medical/social service care.

A Health Plan includes the following, singly or in combination:

- a group health plan,
- a health insurance issuer,
- an HMO,
- a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals, and
- any other individual or group plan, a combination of individual or group plans, that provide or pay for the cost of medical care.

A Health Plan excludes:

- small employee health plans (less than 50 participants that are self-administered),
 - Worker's Compensation Carriers,
 - Government funded programs that incidentally provide or pay for the cost of health care, or the making of grants to fund health care, and
 - Government funded programs that have as their principle purpose other than the provision of health care.
-
- **Healthcare Clearinghouse:** is a private or public entity that processes or facilitates the process of health information received from another entity, either to or from the standard format that is required for electronic transactions.
 - **Trading Partner:** is a person or organization that exchanges health information via electronic transmission with a Covered Entity (e.g., Miami-Dade

County).

ROLES AND RESPONSIBILITIES OF ALL COUNTY DEPARTMENTS:

To facilitate compliance with the above policy, all County departments shall implement the following specific requirements or instructions:

1. Develop and maintain formal, written privacy policies and procedures. The policies and procedures must be updated and maintained according to a defined process, given the needs of the individual department.
2. Designate a departmental Privacy Liaison as the designated person to receive privacy complaints, provide further information about privacy practices, and liaises with the County's Chief Privacy Officer.
3. Develop and implement policies and procedures for dealing with Privacy policy and procedure violations. These policies and procedures shall include:
 - A process for handling privacy infractions;
 - A definition of sanctions; and
 - A mitigation strategy to counter potential harmful effects resulting from violations.
4. Establish and implement a training program to provide initial and ongoing privacy policy and procedures training for all employees.
5. Develop and maintain policies and procedures to protect the integrity, availability, and confidentiality of all personal, identifiable and confidential information including, but not limited to, PHI/IIHI. These policies and procedures must have the following features:
 - Describe the system for the physical storage of information;
 - Describe the system for the physical maintenance of information;
 - Describe the system for transmitting (e.g., faxing, e-mail, computer based) information;

- Describe the levels of personnel that have access to information.

ROLES AND RESPONSIBILITIES OF COUNTY DEPARTMENTS THAT PROVIDE HIPAA-COVERED SERVICES:

Miami-Dade County is a covered entity pursuant to the HIPAA. To facilitate compliance, County departments that provide services covered by the HIPAA standards shall implement the following specific requirements or instructions:

1. Implement a Notice of Privacy Practices (NOPP). The NOPP shall be provided to all customers and visibly posted at service sites. The NOPP shall be written in plain language and contain all of the following:
 - Information regarding the uses and disclosure of PHI;
 - A statement of an individual's privacy rights;
 - A description of the organization's responsibilities under HIPAA;
 - The title, and phone number of the Chief Privacy Officer for more information;
 - Instructions on how to file complaints with the Chief Privacy Officer; and
 - The effective date of the notice.

A signed acknowledgement of the provision of the NOPP will be obtained from each customer.

2. Develop and maintain policies and procedures related to the obtaining of consent from a customer to release PHI for the purposes of treatment, payment, and business operations.
3. Develop and maintain policies and procedures related to the obtaining of authorization from a customer to release PHI for purposes other than treatment, payment, and business operations. This Authorization form shall:
 - Describe the PHI to be released;

- Identify the person making the request;
 - Contain the expiration date of the authorization;
 - Contain a statement of the individual's right to revoke the authorization;
 - Describe the possibility of re-disclosure;
 - Contain areas for signature and date;
 - Permit a description of the signing-authority, if a representative.
4. Develop and maintain policies and procedures to handle requests for access to PHI. These policies and procedures shall include:
- Requests for restriction of PHI;
 - Requests for communication of PHI;
 - Grant individual access to PHI;
 - Right to amend individual PHI; and
 - Provide accounting of PHI disclosures.
5. Develop and implement a system to ensure receipt of updated information regarding state and federal privacy requirements, rights and responsibilities.
6. Develop contracts or MOU's, pursuant to Department of Procurement Management guidelines, with Business Associates and Trading Partners that incorporate HIPAA mandates for privacy, security and electronic transfer standards that shall include:
- The use of information only for performing services required by the contract or as required by law;
 - The use of appropriate safeguards to prevent non-permitted disclosures;
 - The reporting to Miami-Dade County of any non-permitted use or disclosure;

- Assurances that any agents and subcontractor agree to the same restrictions and conditions that apply to the Business Associate; and get reasonable assurances that it will be held confidential;
- The making of PHI available to the customer for review and amendment; and incorporating any amendments requested by the customer;
- The making of PHI available to Miami-Dade County for an accounting of disclosures; and
- The making of its internal practices, books and records related to PHI available to Miami-Dade County for audits of the Covered Entity's compliance.

7. Develop and maintain policies and procedures to ensure that management information systems are compliant with privacy regulations.

PREEMPTION:

Where State law is more stringent or affords an individual greater privacy rights, State law preempts HIPAA requirements. Under Florida state law, most customer identifiable, personal and confidential information is exempt from disclosure (Florida Statutes, Chapter 395.3025 (4), (7), (8)).

EXCEPTIONS:

1. The following information should be handled in a private and confidential manner, however, it is not considered protected information pursuant to HIPAA and is exempt from HIPAA compliance:

- Information obtained directly from an employee or other sources unrelated to the group/employment health plan. For example, sick leave and family medical leave.
- Information for purposes of Worker Compensation administration. The regulations allow for disclosure of PHI information between a health care provider and employer regarding the evaluation of a work-related injury or illness and the findings of the evaluation of a work-related injury or illness.
- On-site medical services.
- Short- and Long-Term Disability Plans.

2. Personal, confidential and protected information may be disclosed under the following circumstances/exceptions:

- Use and disclosure required by law, for example, child abuse/neglect, elder abuse/neglect.
- Use and disclosure to avert a serious threat to health or safety, for example, in the event of a serious and imminent threat to the health and safety of a person or the public. The disclosure must be made to a person who is reasonably able to prevent or lessen the threat, or for identification and apprehension of an individual.
- Use and disclosure for public health activities, for example, birth records, deaths records, public health investigations, public health interventions.
- Use and disclosure for health oversight activities, for example, audits, criminal investigations, inspections, licensure or disciplinary actions, or other activities necessary for the oversight of the health care system, government benefit programs, compliance with governmental regulation or compliance with civil rights laws.
- Use and disclosure for law enforcement purposes, for example, to a law enforcement officer for certain law enforcement purposes.

ENFORCEMENT:

Enforcement of the Administrative Order will be the responsibility of the County's Chief Privacy Officer. The Chief Privacy Officer will work closely with Department Directors to ensure the implementation of privacy policies and the individual departmental Privacy Liaisons in the investigation of complaints.

This Administrative Order is hereby submitted to the Board of County Commissioners of Miami-Dade County, Florida.

George M. Burgess

County Manager