HIPAA PROGRAM MANAGEMENT OFFICE

CHARTER

PURPOSE

The purpose of the County HIPAA Program Management Office (HIPAA PMO) is to manage Clark County's HIPAA compliance governance requirements in accordance with the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH) included in the American Recovery and Reinvestment Act (ARRA) of 2009 and regulations put forth by the United States Department of Health and Human Services (DHHS). This compliance effort covers all areas of HIPAA compliance requirements including Privacy, Security, Electronic Transactions, Unique Identifiers, Data Breach Notification and the County's HIPAA-defined Business Associates.

The mission of the County HIPAA PMO is to effectively and efficiently manage support staff to meet all applicable HIPAA privacy, security, electronic healthcare transaction, unique identifiers and data breach notification compliance regulations; oversee, coordinate, and facilitate the activities of various compliance/implementation workgroups; report on compliance project progress, and provide effective communication about the County's HIPAA Program to internal and external stakeholders.

ORGANIZATION

The HIPAA PMO consists of the HIPAA Program Manager, the Privacy Officer and the Information Technology Security Operations Administrator, who serves as the mandated HIPAA Security Officer. The Privacy Officer and Information Technology Security Operations Administrator will work closely with the UMC Privacy Officer and UMC Information Security Officer to ensure compliance with the HIPAA Regulations. Other team members from various departments that are needed to support project activity will be called upon when necessary.

PROGRAM MANAGEMENT OFFICE ROLES

The major roles of the HIPAA PMO are as follows:

- On-going management of the County's HIPAA Compliance Program and governance process
- Maintain effective lines of HIPAA Compliance Program communications and reporting mechanisms
- Oversight for investigations of reported/detected non-compliance incidents and development of corrective action initiatives

AUTHORITY

The HIPAA Compliance Program Management Office has authority to:

- Coordinate and manage HIPAA related projects
- Direct audits of compliance with regulations
- Conduct investigations into allegations of non-compliance
- Seek any information it requires from employees or external parties.
- Document compliance activities
- Develop HIPAA training curriculum
- Develop committees and workgroups for HIPAA compliance

HIPAA Executive Steering Committee

This voting members of the committee will include representatives from pertinent areas of Clark County/UMC to include:

Clark County Assistant County Manager
Clark County Senior Attorney, DA – Civil
Clark County CIO
UMC CIO
UMC Compliance Officer or Privacy Officer

The HIPAA Executive Steering Committee will meet on a regular basis and receive an update on the following:

- Recommendations for changes to policy
- Types, frequency, and outcomes of investigations
- HIPAA compliance progress reports
- Status of HIPAA compliance activities

The HIPAA Executive Steering Committee also acts as a venue for communication and collaboration between UMC and the County for HIPAA purposes.

Program Manager

- Oversee, facilitate, and coordinate activities of workgroups
- Provide regular communication regarding compliance activities
- Identify and recommend HIPAA related best practices
- Manage documentation of compliance activities for the County
- Oversee County Privacy Officer and Security Officer HIPAA duties

Privacy Officer

- Perform scheduled audits of County areas
- Advise on privacy issues
- Recommend changes to privacy policies and procedures

- Identify and recommend HIPAA related best practices related to Privacy
- Initiate, facilitate, and promote activities to foster privacy awareness within the organization
- Disseminate information on changes to HIPAA

The UMC Privacy Officer has complete control and responsibility for the UMC HIPAA Compliance Program, and reports regularly to the HIPAA Executive Steering Committee.

Security Officer

- Implement Information System Security policies and procedures
- Recommend changes to Information System Security policies and procedures
- Oversee Security training
- Oversee information security risk assessments
- Oversee the preparation of disaster recovery and business continuity plans
- Advise on Security issues
- Initiate, facilitate, and promote activities to foster information security awareness within the organization
- Serve as the information security liaison for users
- Review all information system related security plans throughout the organization
- Track developments in information systems security
- Receive and investigate security related complaints and data breaches

The UMC Information Security Officer serves as the mandated HIPAA Security Officer for that entity. The UMC Information Security Officer will report regularly to the HIPAA Executive Steering Committee.

Hybrid Entity Departmental Liaisons

The HIPAA PMO will interact with departmental appointed liaisons to assist in departmental HIPAA Compliance. The HIPAA PMO will be available to assist Department Liaisons in carrying out their duties as required. The Departmental Liaison will be responsible for:

- Developing and implementing departmental policies and procedures
- Completing departmental risk assessments
- Developing and coordinating the implementation of departmental risk mitigation plans
- Conducting an annual departmental HIPAA evaluation
- Disseminating information provided by the HIPAA PMO to department personnel as appropriate
- Developing and implementing department specific HIPAA training programs

The UMC Privacy Officer will serve as the UMC liaison. Additionally, due to the size of the department, the assigned UMC Departmental Liaison will be responsible for coordinating a subgroup of UMC departmental liaisons.