

Hope Hammond

From: Hope Hammond
Sent: Thursday, September 15, 2011 12:56 PM
To: Brian Brannman; Chief Bertral Washington; Ed Finger (Clark County); George Stevens; Laura Fucci (LFucci@co.clark.nv.us); Mary-Anne Miller (Mary-Anne.Miller@ccdandv.com); Michael Smith (Clark County); Timothy Burch (Clark County); Yolanda "Yoli" Jones; Angela Darragh; Brooke Lancaster (Clark County); Imad Bachir (Clark County); Jan Piestrak (Piestrak@co.clark.nv.us); Jennifer Lances (Clark County); JHannom@co.clark.nv.us; Maria Gudewicz; Pamela Theriault (Clark County); Soley Eggertsson; Tom Wilson; Troy Tuke (Clark County); Trudy M. Harper; Yolanda Givens, Chief Deputy DA
Cc: Ernie McKinley; Hope Hammond; Jeff Wells; Mark Wood DDA
Subject: Revised HIPAA Charter

Attached is the agenda item and the revised Charter approved by the Board of County Commissioners on September 6, 2011.

Hope Hammond, Chief Privacy Officer
Clark County / UMC
702-383-3854 office
702-383-3666 fax

**CLARK COUNTY BOARD OF COMMISSIONERS
AGENDA ITEM**

Issue:	Approve a revision to the HIPAA Program Management Office Charter	Back-up:
Petitioner:	Angela M. Darragh, Acting Audit Director	Clerk Ref. #
Recommendation: That the Board of County Commissioners and the Board of Hospital Trustees approve a revision to the HIPAA Program Management Office Charter.		

FISCAL IMPACT:

None

BACKGROUND:

On April 1, 2003, the Board of County Commissioners approved and adopted a resolution to designate Clark County as a Hybrid Entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and designated its Health Care Components. Those Components, including University Medical Center, are covered under HIPAA mandates and regulations. In order to monitor compliance with HIPAA the HIPAA Program Management Office was established with responsibilities over all covered departments and UMC. The HIPAA Program Management Office consists of an Executive Steering Committee appointed by the County Manager, Program Manager, Privacy Officer and Security Officer.

This revision reflects the addition of designated liaisons appointed by the covered department heads to be responsible for the HIPAA compliance efforts within their department.

Respectfully submitted,

Don G. Burnette
County Manager

Cleared for Agenda

9/6/2011

Agenda Item #

46

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 a HIPAA Program Manager who works with the Chief Privacy Officer and the Information Technology Security Administrator, who serves as the mandated HIPAA Security Officer. The Information Technology Security Administrator will work closely with the UMC Information Security Officer to ensure compliance with the HIPAA Security 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:

- Development, implementation and on-going management of the County's HIPAA Compliance Program and governance process
- Oversight of development and implementing HIPAA Compliance policies and procedures
- Development and monitoring of HIPAA Compliance education and training programs
- Development and implementation of effective lines of HIPAA Compliance Program communications and reporting mechanisms

- Development and implementation of appropriate oversight committees to enforce sanctions and disciplinary actions for violations of HIPAA regulations or County policies
- Investigation 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 committee will include representatives from pertinent areas of Clark County as appointed by the County Manager.

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 compliance activities

Program Manager

- Establish PMO
- Oversee, facilitate, and coordinate activities of workgroups
- Provide regular communication regarding compliance activities
- Identify, develop, and implement HIPAA related best practices
- Manage documentation of compliance activities
- Oversee Privacy Officer and Security Officer HIPAA duties

Privacy Officer

- Receive and investigate privacy related complaints and data breaches
- Perform scheduled audits of areas
- Advise on privacy issues
- Recommend changes to Privacy policies and procedures
- Oversee general Privacy training
- 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

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

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

Additionally, due to the size of the department, the assigned UMC Departmental Liaison will be responsible for coordinating, with the assistance of the HIPAA PMO, a subgroup of UMC departmental liaisons.