



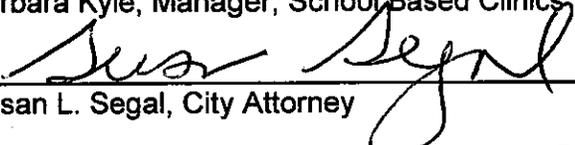
**Request for City Council Committee Action
From
the Department of Health & Family Support, the Office of the City Clerk,
the Human Resources Department, the Minneapolis Fire Department,
the Department of Business Information Services and the Office of the City Attorney**

Date: June 22, 2011
To: Public Safety, Civil Rights & Health Committee
Referral to: Ways & Means/Budget Committee
Subject: The City as HIPAA Hybrid Entity

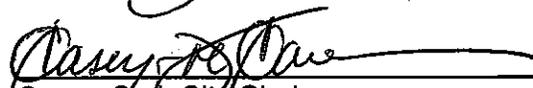
Recommendation: Council approval of resolution declaring the City a HIPAA Hybrid Entity, the School Based Clinics as the City's Health Care Components and the creation of a HIPAA Steering Committee.

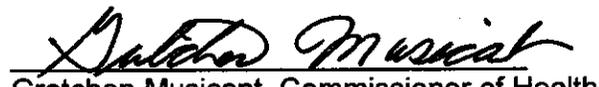
Previous Directives: None

Prepared or Submitted by: Susan Trammell, Assistant City Attorney
 Craig Steiner, MGDPA Responsible Authority
 Joyce Traver, Benefits Manager
 Barbara Kyle, Manager, School Based Clinics

Approved by: 
 Susan L. Segal, City Attorney

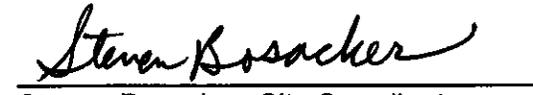

 Alex Jackson, Fire Chief


 Casey Carl, City Clerk


 Gretchen Musicant, Commissioner of Health


 Otto Doll, Chief Information Officer


 Pam French, HR Director


 Steven Bosacker, City Coordinator

Permanent Review Committee (PRC): Approval _____ Not Applicable X
Policy Review Group (PRG) Approval _____ Date of Approval _____ Not Applicable X

Presenters in Committee: Susan L. Trammell, Assistant City Attorney

Financial Impact (Check those that apply)

X No financial impact (If checked, go directly to Background/Supporting Information).

Background/Supporting Information

I. HIPAA & THE CITY – 2002 HIPAA ASSESSMENT

The Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and regulations promulgated thereunder, the Health Information Technology for Economic and Clinical Health (“HITECH”) Act and regulations promulgated thereunder, are, in part, consumer protection laws intended to protect individually identifiable information, whether in paper or electronic form, relating to the physical or mental health of an individual, (“Protected Health Information” or “PHI”), the provision of health care to the individual, and the payment of benefits for health care. HIPAA applies to “Covered Entities,” which include health plans, health care clearinghouses and health care providers that conduct specified transactions electronically. HIPAA requires Covered Entities to provide for the electronic and physical security of PHI.

The HIPAA Standard for the Privacy of Individually Identifiable Health Information (“Privacy Rule”) was published by the U.S. Department of Health and Human Services (“HHS”) on August 14, 2002 and its effective date was April 14, 2003. The Privacy Rule is designed to ensure that the savings from standardizing the interactions between payers and providers were not accompanied by the wholesale loss of privacy. The Privacy Rule mandates that Covered Entities implement policies and procedures with respect to PHI.

The HIPAA Standard for the Security of Individually Identifiable Health Information (“Security Rule”) was published by HHS on February 20, 2003 and its effective date was April 20, 2005. The Security Rule covers electronic protected health information (“ePHI”) and focuses on such things as unauthorized network access, breaches of network firewalls, hackers, computer viruses and compromised passwords that could disrupt the flow of ePHI. The Security Rule establishes a series of 18 security standards, or baseline security requirements, covering administrative, physical and technical safeguards and, for some of the standards, prescribes implementation features which explain how to go about satisfying the requirements.

The 2009 HITECH Act strengthened the privacy and security provisions of HIPAA. HITECH, among other changes, requires notification to individuals about unauthorized disclosures of unsecured PHI and direct regulation of entities providing services to Covered Entities. The Interim Final Rule for Breach Notification for Unsecured Protected Health Information (“Breach Notification Rule”) was published on August 24, 2009, and had various effective dates, the first of which was September 23, 2009.

In 2002, the City conducted an assessment of all of its divisions, programs and departments for applicability of HIPAA requirements. Through the assessment process it was determined:

1. The City sponsors employee welfare benefit plans which meet the definition of group health plans under HIPAA;
2. The only components of the City providing health care services were the Minneapolis Fire Department (“MFD”) and the School Based Clinics (“SBC”) of the Minneapolis Department of Health and Family Support (“MDH&FS”);
3. Neither the MFD nor the SBC transmitted any health information in electronic form in connection with a transaction covered by HIPAA and therefore neither the MFD nor the SBC were health care providers subject to HIPAA.

II. CITY OF MINNEAPOLIS HEALTH PLANS AND HIPAA

A. HIPAA Requirements related to Group Health Plans

While employers are not Covered Entities under HIPAA, certain employee benefit plans sponsored by employers are Covered Entities, and in many cases, the plans are subject to full spectrum of HIPAA compliance requirements. The Employee Retirement Income Security Act ("ERISA") treats Group Health Plans as separate legal entities and HIPAA continues this treatment. Although the plans are considered separate from the employer, the plans themselves are subject to HIPAA and the employer, as the plans' sponsor, is indirectly impacted by HIPAA compliance requirements.

The relationship between an employer and the Group Health Plans it sponsors creates two main categories of issues for the employer under HIPAA:

1. Ensuring compliance with HIPAA by the Group Health Plan itself; and
2. Ensuring compliance with HIPAA by the employer in its role as sponsor with respect to its receipt of PHI from the Group Health Plan.

HIPAA requires adequate separation between a Group Health Plan and its employer sponsor and sets forth requirements necessary for a Group Health Plan and the employer to certify separation. An employer may never use information that it obtains in its capacity as a sponsor of a Group Health Plan for any purpose other than plan administration.

1. Privacy Rule

Group Health Plans with insured benefits are subject to the HIPAA Privacy Rule. When the benefits, however, are provided by an insurance issuer or HMO and the only PHI created or received by the plan or the sponsor of the plan are summary health information and enrollment and disenrollment information, the statutory obligations of the plan are minimal. In the fully insured summary health information and enrollment/disenrollment information only situation, the plan's statutory obligations under the Privacy Rule are to:

1. Refrain from retaliation or intimidation if an individual seeks to exercise rights under the Privacy Rule; and
2. Refrain from requiring individuals to waive their rights under the Privacy Rule as a condition of treatment, payment, enrollment or eligibility for benefits.

Fully insured Group Health Plans (or the sponsor of the plans on the plans' behalf) receiving additional protected health information from the insurance issuer or HMO must amend their plan documents and comply with plan sponsor requirements.

A self-insured Group Health Plan must comply with all HIPAA privacy requirements. If the sponsor of a self-insured plan receives additional protected health information from the insurance issuer or HMO, the Group Health Plan must amend their plan documents and comply with plan sponsor requirements.

2. Security Rule

The Security Rule establishes a national set of security standards for protecting a subset of information covered by the Privacy Rule, which is all individually identifiable health information a covered entity creates, receives, maintains or transmits in electronic form ("ePHI"). The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical

and non-technical safeguards that Covered Entities must put in place to secure individuals' ePHI. Specifically, covered entities must:

1. Ensure the confidentiality, integrity, and availability of all ePHI they create, receive, maintain or transmit;
2. Identify and protect against reasonably anticipated threats to the security or integrity of the information;
3. Protect against reasonably anticipated, impermissible uses or disclosures; and
4. Ensure compliance by their workforce.

3. Breach Notification Rule

The Breach Notification Rule implements section 13402 of HITECH requiring Covered Entities and their business associates to provide various notifications following a breach of unsecured protected health information. The Breach Notification Rule provides that should PHI be acquired, accessed, used or disclosed in violation of the Privacy Rule and in a manner that poses a significant risk of financial, reputational or other harm to the individual, a breach has occurred. Covered Entities and their business associates must notify the individual whose PHI has been compromised, self-report the breach to the HHS and in some cases notify the media. This notification requirement applies to both electronic and paper PHI.

B. The City's Group Health Plans HIPAA Compliance Actions

The City sponsors the various group health plans offered to employees that are considered Covered Entities. The City's HIPAA covered plans ("City Plans") include:

- Fully-insured plans:
 - the City of Minneapolis Medical Plan ("Medical Plan");
 - the Employee Assistance Program ("EAP");
- Self-insured plans:
 - the City of Minneapolis Dental Plan ("Dental Plan"); and
- Plans that are neither fully-insured nor self-insured ("Other Plans"):
 - the City of Minneapolis Medical Expense Reimbursement Plan ("Medical Flex"); and
 - the City of Minneapolis Health Care Reimbursement Arrangement Plan ("HRA/VEBA")

Staff have carefully analyzed the City Plans to determine compliance responsibilities of both the Health Plans and the City, as the employer sponsor, and developed and implemented a compliance program. The following are some of the steps taken related to City Plans:

- Designated the City's Government Data Practices Responsible Authority as the City's Privacy Officer.
- Designated the Human Resources Director as the Health Plans' Privacy Officer.
- Developed and distributed a Notice of Privacy Practice ("NPP").
- Created an authorization form for use by the City, as a plan sponsor, and for use by the Health Plans.
- Developed, implemented and documented privacy policies and procedures and provided training to City employees working with the Health Plans and handling PHI.

- Amended Health Plan documents to include provisions required by the Privacy Rule and the Security Rule permitting the Health Plans to disclose PHI to the City for limited, administrative purposes.
- Executed business associate agreements on behalf of the Health Plans with plans' third party administrators performing duties involving PHI.
- Met periodically with BIS to discuss assessment and action plan implementation for required electronic security steps.

III. MINNEAPOLIS FIRE DEPARTMENT

The 2002 assessment of the MFD activities revealed that one of the MFD's lines of business is to provide medical care to persons in emergency trauma and emergency medical situations through the department's 400 plus Emergency Medical Technicians. The department's 29 emergency response apparatus respond to between 21,000 and 23,000 Emergency Medical Service calls yearly.

The 2002 assessment revealed that the MFD does not bill for the health care services it provides nor does it conduct any of the HIPAA specified transactions electronically. As a result it was determined through the 2002 Assessment that the MFD would not constitute a Covered Entity if it were a separate legal entity.

The status of the MFD was reassessed in 2011 as a result of a Star Tribune article stating that the MFD was "collecting fees for providing care during vehicle accidents." Again, the assessment revealed that although the MFD provides medical care in emergency trauma and emergency medical situations, the fees collected do not relate to the medical care furnished and the MFD is not otherwise conducting any HIPAA specified transactions electronically.

The status of the MFD with regards to HIPAA needs to be evaluated on a regular basis to ensure that if either future HIPAA amendments or changes at the MFD operations result in HIPAA applying to the MFD, the City can then take the steps necessary to designate the MFD a health care component of the City and to fully implement the required HIPAA actions.

IV. SCHOOL BASED CLINICS

A. Privacy Standards implemented after 2002 Assessment

Like the MFD, the 2002 assessment of the SBC revealed that SBC provide healthcare services. The HIPAA Privacy Rule, however, did not apply to the SBC because the SBC did not conduct any of the HIPAA specified transactions electronically.

Even prior to the 2002 assessment, the SBC took multiple actions to protect the privacy of client records. Since the SBC collects client PHI, it has been the SBC practice to inform every student at the time of their first clinic visit of how their PHI is used by the clinic. Every student is provided with a Tennessee Warning and is required to read and sign the form prior to receiving any clinic care. In addition, the SBC staff explains the current MN State Minor Consent Law and the minor's rights related to this law. The SBC provides training to SBC employees related to MN privacy requirements for health records. When requests are made for their health information the SBC requires a student client's written consent for release of any paper records or verbal information to anyone outside the SBC. In addition to the MN Data Privacy Act, the SBC has followed the MN Medical Records Act law. Medical records are stored in locked file cabinets and client PHI is not stored on individual computers or emailed.

Even though the HIPAA Privacy Rule did not apply to the SBC, the SBC adopted a number of HIPAA compliant practices, including:

- Procured the 10-digit National Provider Identifier ("NPI").
- Developed and used a Notice of Privacy Practices.
- Created an authorization form for the release of PHI.
- Executed business associate agreements with the SBC contractors performing duties involving PHI.

B. Minnesota Electronic Health Record System Requirement

Minnesota Statutes Section 62J.495-497 requires that all hospitals and health care providers have an interoperable electronic health record system by 2015. In response to this mandate, the SBC will be transitioning to an electronic health record system in August 2011. This change in records management requires the City to be in compliance with HIPAA as well as state laws and regulations for the privacy and security of health information.

Once the SBC begin using the electronic health record system, the SBC will be conducting HIPAA covered transactions related to the provision of health care. The SBC would be Covered Entities if the SBC were not components of the City but rather separate legal entities. Because the SBC are a part of the City, the City becomes the Covered Entity due to the activities of the SBC.

C. HIPAA Hybrid Entities

HIPAA provides flexibility to entities like the City which engage in both Covered Entity activities and other activities that are not Covered Entity functions. HIPAA permits the City to either 1) comply city-wide with HIPAA regulations; or 2) declare itself a "Hybrid Entity". To become a Hybrid Entity, the City must formally declare itself a Hybrid Entity and designate in writing all divisions or departments that would meet the definition of a covered entity if those health care components were separate legal entities. With a Hybrid Entity designation, most of the HIPAA requirements apply only to the health care components, although the City, as a Covered Entity, retains certain oversight, compliance and enforcement obligations.

D. Impact Upon Other City Departments

Non-health care divisions and departments of a Hybrid Entity are affected because HIPAA limits how a health care component shares PHI with the non-health care components. In a Hybrid Entity precautions need to be taken to ensure separation between the health care components and the components of the Hybrid Entity which are not involved in the health care operations.

In addition to the components providing health care services, HIPAA requires that components performing "Business Associates" activities comply with all HIPAA regulations. A Business Associate is person or an organization that performs or assists a Covered Entity in the performance of a function that involves the use of disclosure of PHI on behalf of the Covered Entity.

The other departments performing functions on behalf of the SBC are: legal, finance, audit, human resources and BIS. The functions of these other City departments have been examined to determine if any of them perform activities that would make the department a Business Associate of the SBC if it were a separate legal entity. Because the electronic health record keeping system to be implemented by the SBC is designed to be entirely separate from the City's network and because the system is maintained by a contractor independent of the City, BIS will not have any responsibilities for the system and BIS employees will not have any

access to the PHI stored on the system. In addition, the new electronic record system will be operated such that no PHI will be shared with any other City department performing activities on behalf of the City. At this time, the SBC do not anticipate the sharing of any client PHI with any other department of the City. (HIPAA specifically excludes employment records maintained in the employer capacity so employee records are not at issue here.) No other City departments or divisions need to be designated at this time. The status of other departments and/or divisions as Business Associates will be reviewed periodically and designation as Business Associate components will be sought should circumstances change.

V. NEXT STEPS FOR HIPAA COMPLIANCE

The Departments are requesting approval of the attached resolution designating the City of Minneapolis as a Hybrid Entity, the SBC as a health care component, the creation of a HIPAA Steering Committee and delegation of authority related to HIPAA decisions to the Steering Committee.

RESOLUTION OF THE CITY OF MINNEAPOLIS
DECLARING THE CITY A HIPAA HYBRID ENTITY, THE SCHOOL BASED CLINICS AS THE
CITY'S HEALTH CARE COMPONENTS AND THE CREATION OF A HIPAA STEERING
COMMITTEE

By Council Member Samuels

WHEREAS, the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and regulations promulgated thereunder, the Health Information Technology for Economic and Clinical Health Act ("HITECH"), and regulations promulgated thereunder, require public and private entities that provide certain health care services to comply with regulations related to the collection, use, disclosure and security of individually identifiable health information;

WHEREAS, the City of Minneapolis (the "City") is committed to compliance with all applicable laws and regulations relating to data privacy and security, including, but not limited to HIPAA and HITECH;

WHEREAS, in 2002 the City conducted an assessment of its divisions, programs and departments for applicability of HIPAA requirements and determined that the City is a sponsor of employee welfare benefit plans and that the only components of the City providing health care services were the School Based Clinics ("SBC") of the Minneapolis Department of Health and Family Support ("MDH&FS") and the Minneapolis Fire Department ("MFD");

WHEREAS, the City's group health plans ("City Plans") are separate Covered Entities under HIPAA, and although the City Plans are not business lines of the City, the City, as an employer sponsor of group Health Plans, is indirectly impacted by the HIPAA health plan requirements.

WHEREAS, the 2002 HIPAA assessment of the health care services activities of the MFD was that the MFD did not transmit any health information in electronic form in connection with a transaction covered by HIPAA and therefore the MFD was not subject to HIPAA;

WHEREAS, the 2002 HIPAA assessment of the health care services activities of the SBC was that the SBC did not transmit any health information in electronic form in connection with a transaction covered by HIPAA and therefore the SBC were not subject to HIPAA;

WHEREAS, Minnesota Statutes Section 62J.495-497 requires that all health care providers have an interoperable electronic health record system and the SBC implementation of such electronic health record system will result in the SBC transmitting health information in electronic form in connection with a transactions covered by HIPAA and therefore making the SBC covered by HIPAA;

WHEREAS, because the City has some components, the SBC, that are required to comply with HIPAA and other components that do not, the City may declare itself it a Hybrid Entity pursuant to Section 164.504(a) of the HIPAA privacy regulations (the "Privacy Rule");

WHEREAS, staff have determined that the City may more effectively and efficiently administer its HIPAA compliance program by declaring the City as a "hybrid entity" and formally designating the City's health care components;

WHEREAS, HIPAA regulations required the City to designate an individual as the privacy officer to be responsible for the development and implementation of required privacy policies and procedures for the City and the City's Minnesota Government Data Practices Responsible Authority ("Responsible Authority") has assumed those duties relative to HIPAA compliance by the City's Plans;

WHEREAS, the City must designate an individual as the security officer under the HIPAA regulations and the City's Chief Information Officer has assumed those duties relative to HIPAA security compliance by the City Plans;

WHEREAS, the City recently added an Information Security Officer and HIPAA security compliance duties have been transferred to the Information Security Officer;

WHEREAS, as a hybrid entity, the City has ongoing responsibilities to establish and maintain ongoing policies, procedures and business practices to maintain compliance with HIPAA requirements;

NOW, THEREFORE, BE IT RESOLVED, that the City Council hereby designates the City as a HIPAA Hybrid Entity;

FURTHER RESOLVED, that the SBC of the MDH&FS are hereby designated as the health care components of the City's HIPAA Hybrid Entity;

FURTHER RESOLVED that the City's Responsible Authority is hereby appointed as the HIPAA Privacy Officer responsible for the development an implementation of required HIPAA privacy policies and procedures for the City;

FURTHER RESOLVED that the City's Information Security Officer is hereby appointed as the HIPAA Security Officer responsible for the development an implementation of required HIPAA security policies and procedures for the City;

FURTHER RESOLVED that the City Plans shall designate a Privacy Coordinator and a Security Coordinator responsible for the development and implementation of required HIPAA privacy and security policies and procedures for the City Plans;

FURTHER RESOLVED that the SBC shall designate a Privacy Coordinator and a Security Coordinator responsible for the development and implementation of required HIPAA privacy and security policies and procedures for the SBC;

FURTHER RESOLVED, that a HIPAA Steering Committee is created and shall be consist of the following members: the City Clerk, the Chief Information Officer, the HIPAA Privacy Officer, the HIPAA Security Officer, the Privacy Coordinator for the City Plans, the Privacy Coordinator for the School Based Clinics, the Security Coordinator for the City Plans, the Security Coordinator for the School Based Clinics, a representative from the Minneapolis Fire Department, and a representative from Office of the City Attorney;

FURTHER RESOLVED, that the Privacy Officer is designated the Chair of the HIPAA Steering Committee;

FURTHER RESOLVED, that the City Council delegates to the HIPAA Steering Committee, the authority to approve changes in the designation of departments, divisions, units and/or programs as health care components in order to maintain compliance with the requirements of HIPAA; to develop policies and procedures, and outline other actions as necessary for implementation of HIPAA;

FURTHER RESOLVED, that the Chair of the HIPAA Steering Committee shall present an annual status report to the City Council through the appropriate committee.