POLICY A: HIPAA PRIVACY RULE

I. POLICY OVERVIEW

A. Purpose

The purpose of this policy is to provide guidance to all the School Based Clinics ("SBC") and designated Minneapolis Department of Health and Family Support ("MDHFS") employees by setting forth the basic requirements for protecting the confidentiality of medical information as required by the Privacy Rule.

B. Statement of Policy

It is the policy of the MDHFS SBC to comply with the Privacy Rule set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

C. Scope

This policy pertains to all individuals in the SBC who have access to, use, or disclose protected health information. The policies are approved by the City HIPAA Steering Committee and administered by the SBC Manager as the designated HIPAA Privacy and Security Coordinator for the SBC. See the attached SBC organizational chart.

D. Background

The federal Health Insurance Portability and Accountability Act of 1996 and its corresponding regulations are intended to protect privacy for individuals receiving health care services in the United States. The Privacy Rule, as it may also be called, establishes a national standard for the minimum level of protection for medical information. The intent of the statute and the regulatory rule is to expand consumer control over their medical information. All health care entities subject to the regulations must abide by the rules.

The Privacy Rule introduces the term "Protected Health Information", or "PHI". **PHI covers information relating to an individual's health, the care received and/or payment for services, including demographic data. It includes all information in any media related to the individual's health care that can be individually identified as belonging to a particular person.** The HIPAA privacy rule applies to "covered entities", which the SBC becomes upon implementation of Electronic Health Records in January, 2012. The privacy rule requires health care providers to have in place processes to safeguard protected Health Information.

In July 2011, the City of Minneapolis passed a resolution designating the City as a Hybrid Entity, the SBC as a health care component and the City's Responsible Authority as the Privacy Officer. The resolution also established a HIPAA Steering Committee with delegated authority related to HIPAA decisions.

There are many obligations imposed on a Covered Entity by privacy regulations. These include:

1. Developing and implementing policies and procedures to assure compliance;
2. Training SBC workforce on HIPAA requirements appropriate to their jobs;
3. Documenting SBC efforts to achieve compliance;
4. Developing safeguards to protect PHI; and
5. Designating a Privacy Official.

The basic tenet of the Privacy Rule is that providers may use and disclose PHI without the individual's authorization only for treatment, payment and health care operations, as well as certain public interest related purposes such as public health reporting. Other uses and disclosures of PHI generally require the written authorization of the individual.

The Privacy Rule also introduces the concept of "minimum necessary". This requirement mandates that when using or disclosing PHI, or when requesting PHI from external providers or entities, providers will make reasonable efforts to limit PHI to the minimum necessary to accomplish the intended purpose. The Privacy Rule does recognize that providers may need to use all of an individual's health information in the provision of patient care. However, access to PHI by the workforce must be limited based on job scope and the need for the information.

The Privacy Rule also includes a set of rights for consumers of health care services. These include the right to obtain a written notice explaining how the SBC will use and disclose their information, to access their health information (including requesting copies, requesting amendments, and receiving an accounting of specified disclosures), to request that certain information be restricted from use or disclosure for purposes of treatment, payment and health care operations (this request need not be granted if it is unreasonable or overly burdensome), to request that information be communicated in particular ways to ensure confidentiality, and to refuse to authorize the release of information for most purposes not related to treatment, payment or health care operations.

This policy provides an overview of the requirements of the Privacy Rule. There are more detailed policies on certain issues discussed herein such as authorization for the use and disclosure of PHI, notice of SBC privacy practices, and patient rights. There is also a separate policy addressing the requirements the Privacy Rule places on research.

Another section of HIPAA contains a "Security Rule". This Security Rule focuses on ensuring that electronic health information that pertains to an individual remains secure. Separate policies address the requirements of the Security Rule. These policies address, among other issues, the maintenance and/or exchange of medical information via e-mail, fax, hand-held devices, and non-SBC personal computers and networks.

In 2009 the HITECH Act strengthened the privacy and security rules. HITECH includes the Breach Notification Rule which requires Covered Entities and their business associates to provide various notifications to individuals regarding unauthorized disclosures of PHI. Separate policies address the requirements of the Breach Notification Rule.

E. Comparison with Existing State Laws

HIPAA regulations do not supersede MN State law where the state law is more stringent. The overarching statute related to government data practices is known as the Minnesota Government Data Practices Act, Minnesota Statutes Chapter 13, ("MGDPA"). The MGDPA regulates the collection, creation, storage, maintenance, dissemination and access to government data including data of the SBC. Additionally, the Minnesota Health Records Act governs the release or disclosure of health records and the Minnesota Consent of Minors for Health Services law establishes the situations in which a minor may give consent for health services and the consent of no other person is required. Further, other federal and state statutes provide additional protection for certain medical, mental health, and substance abuse information. SBC must comply with both the federal Privacy Rule and existing state laws. In situations where laws conflict or overlap, SBC must comply with the law that provides the patient with the greater protection or that restricts SBC procedures more. Determining which law applies can be complex; any questions should be referred to the SBC Privacy Coordinator.

II. USE & DISCLOSURE OF PROTECTED HEALTH INFORMATION

A. Statement of Policy

Protected Health Information (PHI) may be used and disclosed by SBC personnel for treatment, payment and health care operation (as defined by HIPAA) to carry out their duties. SBC personnel may also need to disclose PHI on clients to persons outside the SBC or to request PHI from these persons. SBC staff must limit their uses, disclosures, and requests for PHI to the minimum amount of information necessary to accomplish the purpose of the use or disclosure.

B. Definitions

Protected Health Information (PHI): Individually identifiable health information. Health Information means any information whether oral or recorded in any form or medium that is created or received by the SBC and relates to the past, present, or future physical or mental health or condition, provision of health care or payment for provision of health care to an individual.

Use: The sharing, employment, application, utilization, examination, or analysis of protected health information within the SBC or its contract providers.

Disclosure: The release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the SBC or its contract providers.

Treatment: The provision, coordination or management of health care and related services by the SBC, including the coordination of health care with a third party; consultation between SBC and another health care provider(s) relating to a SBC client; or the referral of a SBC client to another health care provider.

Payment: Activities undertaken by the SBC to obtain reimbursement for the provision of health care. Activities include determinations of insurance coverage, billing, claims management, medical data processing and utilization review activities.

Health Care Operations: The following activities related to the SBC function as a health care provider: Quality assessment & improvement activities, protocol development, care coordination, business management activities and evaluating provision of care.

Authorization: The formal consent document releasing PHI from the records of an entity covered by the privacy provisions of HIPAA.

C. Special Requirements for Mental Health and Health Information of Minors

1. Mental Health Information

   a. Although the federal privacy rule largely does not make a distinction between medical and mental health information, Minnesota state law does provide special protections for mental health information. Mental health information, except psychotherapy notes, may be shared among SBC providers and SBC contract providers for the purposes of treatment. All other uses and disclosures require the specific authorization of the client to disclose mental health information.

   b. Mental health information (*excluding psychotherapy notes*) includes medication prescription(s) and monitoring, counseling session start and stop times, modalities/frequencies of treatment, results of clinical tests, or summaries of diagnosis, functional status, treatment plans, symptoms, prognosis, or progress recorded by mental health professionals.

   c. Psychotherapy notes receive special protection under HIPAA Privacy Rule. Psychotherapy notes means notes recorded (in any medium) by a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint, or family therapy session and that are separated from the rest of the individual's medical record. A clinic provider may not use or disclose psychotherapy notes for any purpose, including most treatment, payment or health care operations, without a separate written authorization signed by a parent (or the client under circumstances where the minor can give effective consent). Psychotherapy notes may be released without client authorization for the SBC to defend itself in legal action brought on by the client, Secretary of HHS wants to review them or law requires the use or disclose or to advert a serious threat to health and safety with SBC Privacy Coordinator approval.

   d. Psychotherapy notes in a SBC medical record are only accessible to mental health provider.

   e. Questions regarding the use or disclosure of mental health information should be referred to the SBC Privacy Coordinator.

2. Minors and Their Records

   a. Use and disclosure of protected health information associated with the care of minors should be administered using the same principles as consent for treatment. However, if the minor can consent for services per federal or state statute, then the minor controls his or her privacy rights. Generally, a parent or assigned guardian controls a minor's privacy rights. There are a number of exceptions that apply in which a minor holds the right to consent and therefore controls all consequent privacy rights. These exceptions include the following:

      i. Emancipated minors may give effective consent for medical, mental and other health services. Emancipated minors are those persons who (a) have reached the age of 18, (b) have lawfully married, or (c) have been declared emancipated by court order. Emancipated minors hold the right to consent and control all consequent privacy rights.

      ii. A minor who has borne a child has the right to give effective consent to personal medical, mental, dental and other health services, or to services for the minor's child, and the consent of no other person is required. The minor holds the right to control all consequent privacy rights.

      iii. A minor may give effective consent for medical, mental and other health services to determine the presence of or to treat pregnancy and conditions associated therewith, venereal disease, alcohol and other drug abuse, and the consent of no other person is required. The minor holds the right to control all consequent privacy rights. A minor who is living separate and apart from parents or legal guardian, whether with or without the consent of a parent or guardian and regardless of the duration of such separate residence, and who is managing personal financial affairs, regardless of the source or extent of the minor's income, may give effective consent to personal medical, dental, mental and other health services, and the consent of no other person is required. The minor holds the right to control all consequent privacy rights.

   b. In situations where the minor may not give effective consent, the parent controls the consequent privacy rights.

   c. A child abuse report which is required to be filed under Child Abuse Reporting Act is not "health record," and cannot be released as such.

   d. SBC staff may not release health records to parents of a client who is age 18 or older without the authorization of the client.

D. Permitted Disclosures for Public Interest Related Purposes

1. SBC providers and staff may disclose PHI without authorization for a variety of public interest related purposes including the following:

   a. Public health activities that involve safety or communicable disease;

   b. To report victims of abuse, neglect, or domestic violence;

   c. Judicial and administrative proceedings;

   d. Law enforcement purposes;

   e. Organ and tissue donations;

   f. National security and intelligence activities;

   g. Workers' compensation; and

   h. Requests related to decedents.

2. Limitations regarding minimum necessary use, mental health and substance abuse information may apply to these public interest related disclosures.

E. De-Identified Information

1. De-identified information may be used or disclosed as long as no means of re-identification is disclosed.
2. In order to meet the definition of "de-identified" under the federal HIPAA Privacy Rule, all of the following specified identifiers must be removed: names, geographic designations smaller than a state (except for the initial three digits of zip codes if the first three digits cover an area having more than 20,000 people), dates (other than years), ages over 89 (although all persons over 89 may be aggregated into a single category), telephone and fax numbers, e-mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate and license numbers, vehicle identification numbers, device identifiers and serial numbers, URLs and IP addresses, biometric identifiers, identifiable photographs and any other unique identifiers.
3. SBC providers and staff may disclose PHI to a business associate for the purpose of de-identifying such information. Business associate relationship exists when an individual or non-SBC entity, acting on behalf of the SBC, assists in the performance of a SBC function or activity involving the use or disclosure of PHI. In order to have access to PHI, however, the business associate must have been formally recognized by SBC administration as such and entered in to a business associate agreement.
4. If all of the required identifiers are not removed, information can still be treated as de-identified if a qualified statistician determines that the risk of re-identification is very small. This analysis must be documented.

III. CLIENT RIGHTS REGARDING PROTECTED HEALTH INFORMATION

A. Statement of Policy

It is the policy of the SBC to comply with client rights regarding Protected Health Information (PHI) as set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

B. Background

Expanded consumer control and privacy protections were important concerns for the drafters of the HIPAA Privacy Rule. To this end, individuals have certain rights set forth in the HIPAA Privacy Rule as follows:

1. The right to obtain a written notice explaining how PHI will be used and disclosed.
2. The right to access and obtain a copy of their medical records.
3. The right to request an amendment of their PHI.
4. The right to obtain an accounting of disclosures of their PHI (with limited exceptions).
5. The right to request that certain information be restricted from use or disclosure for purposes of treatment, payment or health care operations (although HIPAA allows the SBC to use its discretion in agreeing to such requests).
6. The right to request restrictions on the manner and method of confidential communications.

C. Providing Rights

SBC shall provide clients with certain rights pertaining to their PHI. These rights are as follows:

1. The right to obtain a written notice explaining how SBC will use and disclose their information.
2. The right to access their medical information (this includes seeing their records, requesting copies, requesting amendments to their records, and getting an accounting of specified disclosures).

3. The right to request that certain information is restricted from use or disclosure for purposes of treatment, payment, and health care operations. (SBC may not grant this request if it is deemed unreasonable or overly burdensome. Also in some situations the parent will have the right to the information even though the client has requested nondisclosure.)
4. The right to request that information be communicated in particular ways to ensure confidentiality.
5. The right to refuse to authorize the release of PHI for purposes not related to treatment, payment or health care operations or those required by law. (In some situations the parent will have the right to authorize release of the information even though the patient has refused to authorize the release.)

IV. ADMINISTRATIVE & OPERATIONAL REQUIREMENTS

A. Statement of Policy

It is the policy of the School Based Clinic (SBC) to adopt administrative policies and implement procedures that fulfill the administrative requirements set forth in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

B. Implementation

SBC shall implement administrative and operational measures to ensure compliance with the Privacy Rule as follows:

1. Develop policies, procedures and systems to protect patient privacy;
2. Train staff on these procedures;
3. Appoint a Privacy Coordinator to make sure privacy procedures are developed, adopted, and followed;
4. Secure records that contain PHI and implement reasonable safeguards to limit access to PHI to those SBC employees whose jobs require such access.
5. Account for specified disclosures of PHI;
6. Establish a complaint mechanism for privacy concerns; and
7. Establish and enforce a system of sanctions for employees who violate privacy policies and procedures.

V. ADMINISTRATIVE, TECHNICAL & PHYSICAL SAFEGUARDS

A. Statement of Policy

The SBC HIPAA Coordinator has established appropriate procedures for administrative, technical and physical safeguards to insure the security of PHI and prohibit access to PHI by anyone other than those individuals specifically authorized to work with PHI as part of the SBC operations. While conducting work the SBC receives confidential and sensitive information in a variety of forms. The variety of communication methods creates concern about how to protect the privacy of this information while providing quality of care and service. In order to assist staff in maintaining the privacy of individual's health information and in order to meet the SBC obligations as outlined in the HIPAA regulations the following set of safeguard guidelines have been developed.

B. Administrative Safeguards

1. The SBC privacy coordinator shall work collaboratively with the Chair of the City of Minneapolis HIPAA steering committee to ensure proper safeguards are in place to insure the use, access, and disclosure of PHI is consistent with HIPAA, Federal, State, and local regulations.
2. These safeguards include but are not limited to effective review and audit protocols to monitor individual use, access, and disclosure of PHI maintained in any form across the SBC.
3. The privacy coordinator shall be responsible for recommending procedures to the HIPAA Steering Committee to routinely test for inappropriate use, access or disclosure of PHI.
4. The SBC Privacy Coordinator shall report annually to the HIPAA steering committee chair on the results of the application of these procedures.

VI. BUSINESS ASSOCIATES

A. Statement of Policy

The purpose of this Policy is to provide a process for establishing a written agreement with each of the SBC's Business Associates as required by the HIPAA Privacy Rule. The SBC contracts with various outside entities and organizations to perform functions or provide services on behalf of the SBC that may involve the disclosure of Protected Health Information ("PHI") to the outside entity. These outside entities are the SBC's Business Associates. Business Associates ("BA") also include other components of the City of Minneapolis which are not designated health care components under the City's HIPAA Hybrid Entity. The policy of the SBC is to obtain written assurances from BAs that they will appropriately safeguard any PHI they create or receive on the SBC's behalf. Such written assurances will be in place before the SBC discloses PHI to the Business Associate.

VII. ENFORCEMENT

A. Each SBC employee is responsible for understanding and complying with this policy and the Privacy Rule. It is the responsibility of SBC Manager and supervisors to provide appropriate privacy training to all employees on an ongoing basis and that employees reporting to them are complying with SBC privacy policies.

B. Any SBC employee who knows of, suspects, or has a question regarding a possible violation of the Privacy Rule may contact the SBC Privacy Coordinator. No employee shall be retaliated against for reporting a possible violation.

C. SBC employees who violate the Privacy Rule shall be disciplined through the civil service process and in accordance with the applicable Collective Bargaining Agreement. Discipline may involve actions up to and including termination of employment.

D. The federal Office for Civil Rights ("OCR") of the Department of Health and Human Services will enforce the Privacy Rule on behalf of the federal government. SBC employees, patients, and clients may file a complaint with the OCR and are not required to use the MDHFS complaint process.

E. There are both civil monetary penalties and criminal sanctions for violations of the Privacy Rule.

F. If a SBC provider or other employee is found to have violated any of the privacy standards, the OCR may impose a civil penalty of no less than $100 and no more than $50,000 for each violation. If a MDHFS provider or other employee is found to have repeatedly violated the exact same requirement or prohibition, the OCR may impose a civil penalty of up to $1,500,000 in a single year. Additional fines may be imposed pursuant to state law.

G. Criminal sanctions, including larger fines and imprisonment, may be imposed for knowingly disclosing or obtaining PHI in violation of the Privacy Rule.

Procedures

A-1: Use & Disclosure of Protected Health Information
A-2: Client Rights Regarding Protected Health Information
A-3: Administrative Requirements
A-4: Business Associates

Applicable Attachments

1. Privacy Authorization Matrix
2. Required Elements for Authorization to Release PHI
3. Authorization of Request/Release of PHI: Edison Form
4. SBC Organization Chart: Privacy Rule Roles
5. Minneapolis HIPAA Hybrid Entity Structure
6. Notice of Privacy Practices
7. Data Privacy Acknowledgement Form
8. Minor Consent Form

Approved

Craig Steiner — 12/07/11
Chair, City of Minneapolis HIPAA Committee — Date

Barbara Kyle — 12/05/11
Program Manager, Minneapolis School Based Clinics — Date