BACKGROUND OF HIPAA

The Health Insurance Portability and Accountability Act of 1996, better known as HIPAA, was one of the most sweeping pieces of federal legislation to impact the healthcare industry. Its initial intent was to reduce the rising costs of healthcare by providing portability of healthcare coverage for consumers and creating efficiencies in healthcare administration through standardization in electronic transactions. During debate over this legislation, Congress recognized that the advances in technology that were proposed could erode the privacy of health information. Therefore, as part of the Act, Congress mandated the development of Federal privacy protections for Individually Identifiable Health Information.

A portion of the American Recovery and Reinvestment Act of 2009 is the Health Information Technology for Economic and Clinical Health Act (the "HITECH Act"), which contains a series of amendments to HIPAA that expand and fortify the privacy and security requirements of HIPAA.

HOW HIPAA APPLIES TO MADISON COUNTY PUBLIC HEALTH (MCPH)

Prior to the HITECH Act, HIPAA applied only to "Covered Entities," which are Health Care Providers, Health Plans and Health Care Clearinghouses (see Glossary definitions at Policy No. HIP002). As of February 17, 2010, "Business Associates" became directly subject to large parts of the HIPAA Privacy Rule and Security Rule. A "Business Associate" is an entity that performs services for a "Covered Entity" that involves the use or disclosure of Protected Health Information ("PHI"). PHI is defined as individually identifiable information that relates to an Individual's health status, the provision of healthcare or payment for healthcare. Business Associate services include, but are not limited to, those of a legal, actuarial, accounting, consulting, data aggregation, managerial, administrative, accreditation, and financial nature. MCPH is a "Business Associate" in relation to its "Covered Entity" clients with whom PHI is used or exchanged during the course of MCPH's engagement with that client.

THE PRIVACY AND SECURITY RULES

The HIPAA Privacy and Security Rules set forth standards to protect the privacy and security of PHI in all forms – verbal, written, and electronic. Covered Entities and Business Associates must develop, implement, and maintain Privacy and Security Policies and Procedures that meet the numerous standards under the Privacy and Security Rules, with a primary focus on prohibiting unauthorized or inappropriate use and disclosure of PHI. The Privacy and Security Rules also require that each Covered Entity and Business Associate educate its employees with respect to its HIPAA Privacy and Security Policies.

ENFORCEMENT / PENALTIES

The Office of Civil Rights in the Department of Health and Human Services is the regulatory agency responsible for enforcing civil penalties under HIPAA. The Department of Justice is the agency that enforces criminal penalties under HIPAA. Furthermore, the HITECH Act gives State Attorneys General the authority to file suit in federal court against any entity accused of violating HIPAA in a manner that the Attorney General has reason to believe adversely affects any resident of that Attorney General's state.

The civil monetary penalties for non-compliance with HIPAA are significant. The HITECH Act increased the amount of civil penalties that can be applied to violators of HIPAA. The civil monetary penalties now range from $100 to $50,000 per HIPAA violation.

PRIVACY PROGRAM OVERSIGHT

MCPH has designated a Privacy Officer; which position is currently filled by the Director of Nursing. The Privacy Officer is responsible for overseeing the implementation of, and compliance with, MCPH's Privacy Policies and Procedures.

REPORTING VIOLATIONS

Several options are available for reporting privacy violations or concerns, including contacting the Privacy Officer. Reporting of alleged or known violations is expected, encouraged and, under certain circumstances, required.

RESPONDING TO REPORTED CONCERNS / VIOLATIONS

All reports of suspected or known violations of MCPH's Privacy Policies and Procedures will be investigated by the Privacy Officer. The identity of reporting individuals is kept confidential to the extent permitted by law, unless doing so would prevent a full and effective investigation. Disciplinary action commensurate with the proven violations will be enforced.

Glossary of HIPAA Terms

1. **Accounting for Disclosures.** Information that describes a Covered Entity's or Business Associate's disclosures of PHI, other than disclosures of hard copy or electronic copy PHI (other than electronic health records as described below) for Treatment, Payment, and Health Care Operations, disclosures made with patient authorization, and certain other limited disclosures, provided that disclosures of PHI through electronic health records for purposes of Treatment, Payment and Health Care Operations must be listed on an Accounting of Disclosures. For those categories of disclosures that need to be in the accounting, the accounting must include disclosures that have occurred during the 6 years prior to the date of the request for an accounting (or a shorter time period at the request of the individual), with 2 important exceptions: (1) an accounting of disclosures for Treatment, Payment and Health Care Operations made through an Electronic Health Record need only include disclosures that occurred within the 3 years prior to the date of the request for an accounting, and (2) disclosures made before the compliance date for a Covered Entity are not part of the accounting requirement.

2. **Authorization (HIPAA Authorization).** A specific type of written permission given by the individual to use and/or disclose protected health information about the individual. The requirements of a valid authorization are defined in the HIPAA regulations and MCPH's policies/procedures.

3. **Breach.** The unauthorized acquisition, access, use, or disclosure of PHI which compromises the security or privacy of such information, except where an unauthorized person to whom the information is disclosed would not reasonably have been able to retain such information.

4. **Business Associate.** Generally, an entity or person who performs a function or service on behalf of a Covered Entity, and in performing the function or service, receives PHI from or on behalf of a Covered Entity. Examples of such functions or services include claims processing, case management, utilization review, quality assurance, billing, and legal, actuarial, accounting, and accreditation. A Business Associate can also be a Covered Entity in its own right.

5. **Confidential Information.** Confidential information is information related to MCPH or its clients that is proprietary or otherwise nonpublic information. Confidential Information includes, but is not limited to any of the following information in any form: proprietary information of MCPH or of a MCPH client; PHI; PII; minutes for Board of Health and other committee meetings; grievances and appeals; business records; marketing and business development goals, strategies and plans; private correspondence; trade secrets; fees, or other charge information; compensation

and benefits information; financial information, and non-public information obtained from MCPH's affiliated hospitals and other business partners.

6. **Covered Entity.** A health plan, a health care clearinghouse, or a health care provider who transmits health information in electronic form in connection with financial or administrative activities related to health care.

7. **De-identified Data**. Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is de-identified. Health information is considered de-identified (1) if stripped of all of the 18 direct identifiers defined under HIPAA, or (2) if an expert in statistical and scientific method determines that there is a very small risk that the information could be used alone or in combination with other information to identify an individual. The HIPAA standards do not apply to De-identified Data.

8. **Designated Record Set.** A group of records maintained by or for a Covered Entity that includes (1) medical and billing records about individuals maintained by or for a covered health care provider; (2) enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; and (3) used, in whole or in part, by or for the Covered Entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for a Covered Entity.

9. **Disclosure.** The release, transfer, provision of access to, or divulging in any other manner of protected health information outside of the entity holding the information.

10. **Health Insurance Portability and Accountability Act of 1996 (HIPAA).** A federal law (Public Law 104-191), which, in part, governs the standards for the electronic exchange, privacy and security of health information. The definition of "HIPAA", as used herein, includes the regulations promulgated thereunder (45 CFR Parts 160 and 164).

11. **Individual.** The person who is the subject of PHI.

12. **Individually Identifiable Health Information.** A subset of Health Information, including demographic information, (1) that is created or received by a Health Care Provider, Health Plan, employer, or Health Care Clearinghouse; 2) that relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and (3) that identifies the individual, or might reasonably be used to identify the individual.

13. **Institutional Review Board (IRB).** An IRB can be used to review and approve a

researcher's request to waive or alter the Privacy Rule's requirements for an Authorization. The Privacy Rule does not alter the membership, functions and operations, and review and approval procedures of an IRB regarding the protection of human subjects established by other Federal requirements.

14. **Marketing.** Marketing means, (1) to communicate about a product or service that encourages recipients of the communication to purchase or use the product or service.

15. **Minimum Necessary**. The least information reasonably necessary to accomplish the intended purpose of the use, disclosure, or request. Unless an exception applies, this standard applies to a Covered Entity when using or disclosing PHI or when requesting PHI from another Covered Entity. A Covered Entity that is using or disclosing PHI for research without Authorization must make reasonable efforts to limit PHI to the minimum necessary. A Covered Entity may rely, if reasonable under the circumstances, on documentation of IRB or Privacy Board approval or other appropriate representations and documentation establishing that the request for PHI for the research meets the Minimum Necessary requirements.

16. **OCR.** Office of Civil Rights, the branch of the HHS that is responsible for federal oversight of the privacy and security regulations.

17. **Personally Identifiable Information (PII).** Information related to an individual that is sensitive information such as credit card numbers, social security numbers, drivers' license numbers or other information that could be used to facilitate identify theft of the individual.

18. **Privacy Rule**. The regulations at 45 CFR 160 and 164, which detail the requirements for complying with the standards for privacy under the administrative simplification provisions of HIPAA.

19. **Protected Health Information** (**PHI**). Any information, whether oral or recorded in any form or medium that is created or received by a Covered Entity that identifies an Individual or might reasonably be used to identify an Individual and relates to:

    - The individual's past, present or future physical or mental health; OR
    - The provision of health care to the individual; OR
    - The past, present or future payment for health care.

    Information is deemed to identify an Individual if it includes either the patient's name or any other information that taken together or used with other information could enable someone to determine an Individual's identity. (For example: date of birth, medical record number, health plan beneficiary number, address, zip code, phone number, email address, fax number, IP address, license number, full face

photographic images or Social Security Number.)

PHI excludes individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act (FERPA) (records described in 20 USC 1232g(a) (4)(B)(iv)) and employment records held by a Covered Entity in its role as employer. (See also definitions of "health information" and "individually identifiable health information")

20. **Use.** With respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

ROLE OF THE PRIVACY OFFICER

Purpose

MCPH has designated a Privacy Officer as the Director of Nursing who is responsible for:

1. Oversight of Privacy related policies and procedures,
2. Receiving and responding to requests, complaints and reports of alleged violations, and
3. Providing guidance and information about Privacy related matters.

Policy

A. Designated Privacy Officer

The Privacy Officer at MCPH will be an individual with knowledge of the HIPAA Privacy and Security regulations.

B. Responsibilities of Privacy Officer

1. Oversee the development and maintenance of MCPH Privacy policies and procedures.
2. Oversee the development and any revisions to MCPH's Business Associate Agreements (BAA) for use with clients and vendors and provide guidance to MCPH on their use and on BAA procedures generally.
3. Ensure the review of all non-MCPH BAAs tendered to ensure that they meet the HIPAA requirements.
4. Oversee the preparation of training materials for MCPH and ensure that training of all personnel is conducted and documented.
5. Respond to employee questions regarding MCPH's privacy obligations and procedures.
6. Be point of initial contact within MCPH in the event MCPH experiences a Breach, or possible Breach, of PHI or PII; assess whether Breach occurred and recommend any mitigating steps and coordinate any required client notice.
7. Maintain records relating to remediation.

8. Coordinate response in the event MCPH is the subject of an audit of its Privacy Laws compliance by the Office of Civil Rights or other authorities, including MCPH's preparations for audit.

9. Monitor new or revised laws or regulations pertaining to privacy and security to determine if new steps or modification of existing compliance steps are necessary or advisable.

10. Make recommendations for compliance with revisions and provide any necessary training.

11. Ensure adequate documentation and record retention and maintenance in accordance with laws, and as necessary to demonstrate compliance.

Administrative Requirements

As required by the HIPAA Privacy Rule, MCPH has developed HIPAA Privacy policies and procedures that provide guidance for the safeguarding of Protected Health Information (PHI) and electronic Protected Health Information (ePHI) received from, or created for or on behalf of, Covered Entity clients.

1. Administrative policies have been developed, and will be maintained and revised as necessary in accordance with the HIPAA Privacy Regulations. This function will be carried out by the Privacy Officer who will have oversight for the MCPH Privacy Program. Privacy policies define the processes and procedures to follow to prevent inappropriate use and/or Disclosure of PHI and PII.

2. All HIPAA policies will be presented to the Health Commissioner by the Privacy Officer. Upon approval, the policies will be implemented.

3. HIPAA policies and procedures will be reviewed annually by the Privacy Officer. Revisions will be made, as warranted, and will be fully documented.

4. All policies and procedures will be documented, in either written or electronic form, and will be maintained for a period of at least six years from the date of creation or the date when last in effect, whichever is later. The Privacy Officer will have responsibility for this task.

5. Privacy policies and procedures will be maintained at all times on the MCPH Sharepoint (for access by workforce members).

Acceptable Uses of PHI by MCPH

Purpose

This privacy policy is adopted to ensure that MCPH staff members only use PHI as necessary to perform services for MCPH. **This applies to all forms of PHI whether it is oral, written, or electronic.**

Procedure

A. Permitted Uses

1. As appropriate to their respective job functions, MCPH staff may use PHI to perform the following services:
   a. To provide remote monitoring services to enrollees
   b. For MCPH's proper management and administration
   c. For Data Aggregation Purposes
   d. For De-identification Purposes

2. In all cases, a use or disclosure must be allowed under the services and business associate agreement with the client. If a MCPH staff member needs to utilize PHI in a manner that is not allowed under the applicable client arrangement, the staff member will consult MCPH's Privacy Officer.

3. If a MCPH staff member needs to use or disclose PHI for any other purpose, the staff member will contact the MCPH Privacy Officer before undertaking the task. The MCPH Privacy Officer will confirm that such uses or disclosure is appropriate. MCPH will make reasonable efforts to limit the access as established; however, exceptions may apply, based on varying job responsibilities.

B. Uses and Disclosures of PHI which are not Allowed

1. MCPH staff members will not use or disclose PHI for any of the purposes listed below without the explicit and written approval of the Privacy Officer
   a. MCPH staff members will not use or disclose PHI for any marketing purposes
   b. MCPH staff members will not use or disclose PHI for any fundraising efforts
   c. MCPH will not receive any remuneration for the use or disclosure of PHI

Minimum Necessary Policy

Purpose

This privacy policy is adopted to ensure that MCPH staff members make reasonable efforts to limit access to, and Disclosure of, PHI/ePHI and PII to the minimum amount necessary to carry out the task at hand. **This applies to all forms of PHI and PII, whether it is oral, written, or electronic.**

Procedure

A. Access to PHI and PII

1. MCPH will make reasonable efforts to limit the access as established; however, exceptions may apply, based on varying job responsibilities.

2. Employees and other workforce members will not access, use or disclose PHI or PII unless necessary for them to perform the job responsibilities.

B. Requesting, Using or Disclosing PHI

1. MCPH staff will make reasonable efforts to request, use, or disclose only *the minimum amount* of PHI or PII necessary to accomplish the specific purpose of the task.

2. MCPH staff will follow established criteria and work with the Covered Entity client to limit the PHI or PII requested or disclosed, and review requests or Disclosures on an individual basis in accordance with such criteria.

Access, Amendment and Accounting of Disclosures

Purpose

MCPH's Covered Entity Clients are required to provide individuals with access to PHI, an accounting of certain Disclosures of PHI and to amend PHI under certain circumstances. Therefore, MCPH's Covered Entity Clients may require that MCPH keep track of certain Disclosures of PHI, and be able to provide an accounting of such Disclosures to the Client or directly to the Individual. This policy sets forth MCPH's policy with regard to Access, Amendment of PHI and for Accounting for Disclosures of PHI.

Procedure

A. Responding to Requests for PHI

1. If a MCPH staff member receives a request for access to PHI from a client or an individual, the staff member should notify the MCPH Privacy Officer within 24 hours of that request. The MCPH Privacy Officer will evaluate the request to determine whether the request is an acceptable request and how to respond to the request.

B. Responding to Requests to Amend PHI

1. If a MCPH staff member receives a request to amend PHI from a client or an individual, the staff member should notify the MCPH Privacy Officer within 24 hours of that request. The MCPH Privacy Officer will evaluate the request to determine whether the request is an acceptable request and how to respond.

C. Accounting of Certain Disclosures

1. The following is a list of types of Disclosures for which a Covered Entity may require MCPH to provide an Accounting of Disclosures, and therefore, MCPH should keep a record of such Disclosures:

    a. Disclosures required by the Secretary of the U.S. Department of Health and Human Services to investigate or determine compliance with the Privacy Rules;

    b. Disclosures made for public health purposes;

    c. Disclosures regarding abuse, neglect or domestic violence to a government authority authorized to receive such reports;

d. Disclosures to a health oversight agency for purposes of oversight activities authorized by law. For example, Disclosures of PHI to government entities for purposes of audits, investigations, inspections, licensure or disciplinary actions are all subject to the accounting requirement;

e. Disclosures made in the course of judicial or administrative proceeding. For example, Disclosures made in response to a court or administrative tribunal order, subpoena, or discovery request must be accounted for;

f. Disclosures of PHI for law enforcement purposes when not pertaining to a Patient in legal custody. For example, Disclosures made to law enforcement officials for purposes of identifying or locating a suspect, fugitive, witness or missing person.

g. Disclosures to coroners, medical examiners, and funeral directors to fulfill their respective duties;

h. Disclosures to organ procurement organizations for purposes of facilitating cadaveric organ, eye or tissue donation or transplantation;

i. Disclosures for research purposes made pursuant to an institutional review board or privacy board approval of a waiver of Authorization and Disclosures made for purposes of research preparation;

j. Disclosures made to prevent or lessen a serious threat or harm to the health or safety of a person or the public;

k. Disclosures related to Armed Services personnel made for activities deemed necessary by military command authorities to assure the proper execution of a military mission;

l. Disclosures authorized by and to the extent necessary to comply with laws relating to workers' compensation programs;

m. Disclosures that are required by law (e.g. Disclosures of PHI in response to a subpoena.)

D. Recordkeeping of Disclosures

1. For each Disclosure, MCPH shall document:
    a. Date of the Disclosure;
    b. Type of PHI disclosed;
    c. Name and address (if known) of each person or entity to whom the Disclosure was made; and
    d. Purpose of Disclosure.
2. MCPH shall document, and maintain a record of, all Disclosures for a period of 6 years.

De-Identification of PHI

Purpose

MCPH is committed to ensuring the privacy and confidentiality of the PHI and ePHI received from, or created for or on behalf of, Covered Entity clients. The HIPAA Privacy Regulation permits the Disclosure of "de-identified" PHI without an Individual's Authorization, and therefore a Covered Entity client may request that MCPH "de- identify" PHI prior to using or disclosing it under certain circumstances. This policy provides guidance on how to prepare "de-identified" PHI.

Procedure

A. De-identification of PHI

1. The HIPAA Privacy Regulation permits the creation of de-identified information; that is, information that has been stripped of any elements that may identify the Individual, such as name, birth date, or social security number.

2. PHI that has been appropriately de-identified is not subject to the protection requirements of the Privacy Regulation, and is no longer considered PHI.

3. PHI may be de-identified by one of the two following methods:
   a. The PHI can be de-identified in a manner that a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
      i. Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an Individual who is a subject of the information; and
      ii. Documents the methods and results of the analysis that justify such determination;

   Or

   b. PHI may be de-identified according to the *safe harbor method* outlined in the Privacy Regulation, but only if MCPH staff have first confirmed that MCPH has no actual knowledge that the de-identified PHI could be used to re-identify the Individual. In addition, the information must be stripped of all

of the following identifiers of the Individual/patient or of relatives, employers, or household members:

i. Names
ii. All geographic subdivisions smaller than a state (including street address, city, county, precinct, zip code and their equivalent geocodes except for the initial three digits of a zip code if according to the current publicly available data from the Bureau of the Census)
iii. All elements of dates (except year) for dates directly related to an Individual, including birth date, admission date, discharge date, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
iv. Telephone numbers
v. Fax numbers
vi. Electronic mail addresses
vii. Social security numbers
viii. Medical record numbers
ix. Health plan beneficiary numbers
x. Account numbers
xi. Certificate/license numbers
xii. Vehicle identifiers and serial numbers, including license plate numbers
xiii. Device identifiers and serial numbers
xiv. Web Universal Resource Locators (URLs)
xv. Internet Protocol (IP) address numbers
xvi. Biometric identifiers, including finger and voice prints
xvii. Full face photographic images and any comparable images, and
xviii. Any other unique identifying number, characteristic or code

4. MCPH may assign a code or other means of identification to allow de-identified information to be re-identified by MCPH provided that:
   a. The code or other means of record identification is not derived from or related to information about the Individual/patient, and is not otherwise capable of being translated so as to identify the Individual; and
   b. MCPH does not use or disclose the code or other means of record identification for any purpose, and the mechanism for re-identification is not disclosed.

5. MCPH follows the Ohio Department of Health's (ODH) Data Methodology Standards for Public Health Practice as it pertains to deidentification of epidemiological data. These standards are included in this policy for reference but may also be found on the ODH website.

Business Associate Agreements

Purpose

1. This privacy policy is adopted to ensure that MCPH executes a business associate agreement with its Covered Entity clients when MCPH will use, disclose, create and/or receive PHI from those clients.

2. As a Business Associate, MCPH will also enter into written business associate agreements with its vendors, contractors, etc. to which MCPH discloses PHI that it receives from Covered Entity clients.

Procedure:

A. Form Business Associate Agreements

1. The Privacy Officer will develop and revise, as necessary, a form Business Associate Agreement to be entered into with each Covered Entity Client from which MCPH receives, or on behalf of which MCPH creates, PHI. The form Business Associate Agreement shall contain the required provisions under the HIPAA Privacy and Security Regulations, as well as other protections considered to be prudent.

B. Procedure for Entering Into Business Associate Agreements

1. MCPH staff responsible for entering into an engagement with a Covered Entity client which will involve the use or disclosure of PHI will be responsible for sending the form Business Associate Agreement to the Covered Entity Client for signature.

2. MCPH may be asked to sign a Covered Entity Client's form Business Associate Agreement. This is acceptable (although, it is preferable to have the Covered Entity Client execute MCPH's form Business Associate Agreement).

3. Business Associate Agreements other than the form developed by MCPH should not be signed without prior review and approval by the Privacy Officer.

4. Copies of all executed Business Associate Agreements should be kept with the underlying services agreement.

5. Copies of all executed Business Associate Agreements must be forwarded to the Privacy Officer.

C. Agreements With Vendors to Protect the Privacy and Security of HIPAA-Protected Information

1. MCPH must also enter into a Business Associate Agreement with its vendors and subcontractors that will have access to PHI.

2. The person responsible for entering into the vendor arrangement is responsible for ensuring that a business associate agreement is executed.

3. MCPH strongly prefers that its form business associate agreement for vendors is used. However, should a vendor insist on utilizing its own form of agreement, that form must be reviewed and approved by the Privacy Officer.

4. Copies of all executed Business Associate agreements with vendors should be kept with a copy of the underlying services agreement. In addition, a copy of the business associate agreement should be sent to the Privacy Officer.

Handling of Confidential Information

Purpose

MCPH requires that all members of its workforce treat all Confidential Information in a manner that maintains the confidentiality of the information.

Procedures

1. All Confidential Information must be handled and maintained in a confidential manner.

2. If a MCPH staff member is directed to destroy Confidential Information, the staff member must ensure that:

    1) Original documents are not destroyed but placed in storage;
    2) Copies of the above are destroyed in the following manner;
       a. All paper documents must be shredded.
       b. Electronic files must be destroyed.

3. In the event the original documents contain PHI or PII, the staff member should consult with MCPH's Privacy Officer for the proper storage of that information.

4. Questions regarding disposal of other Confidential Information must be directed to the Health Commissioner.

Training

Purpose

MCPH is committed to ensuring that workforce members are aware of all established administrative policies and procedures, particularly those that have been developed to meet regulatory requirements. MCPH will provide training to all workforce members, as appropriate and necessary

A. Development/Content

1. The Privacy Officer will be responsible for the development of Privacy training, and will work collaboratively with the Health Commissioner for development of specific needs in the training.

2. When indicated and warranted and to address concerns that arise, specialized training will be developed collaboratively by the Privacy Officer and the applicable operational or departmental manager.

B. Delivery of Training

a. Initial Training. All new hires will receive Privacy training as part of their orientation to MCPH. This introductory training will be provided via live sessions and/or the Intranet. Introductory Privacy training is mandatory for all workforce members prior to being given access to restricted systems.

b. Specific Training. Operational and departmental managers will be responsible for the provision of Privacy training, specific to their operations, as applicable. Managers will also be responsible for identifying Privacy-related risks in their areas, and addressing those risks with appropriate training. The Privacy Officer will be available, upon request, to assist with development and delivery of such training.

c. On-going Training. Education and awareness of MCPH's Privacy Policies and Procedures will be incorporated into overall compliance education and will provided on an on-going basis. This may include information and articles posted to the Intranet, or other ways of communicating Privacy standards. The Privacy Officer will oversee these activities. On-going training will include, but not be limited to:

- Privacy reminders on topics such as faxing and emailing PHI, incidental Disclosures, entering into Business Associate Agreements, etc.;

- Notification of new threats or risks that may arise; and
- Information on how to report Privacy concerns or risks.

d. Annual Refresher Training. Privacy refresher training will be provided to all workforce members annually.

e. Targeted Specialized Training. Additional specialized training for targeted high-risk areas, or in response to concerns that have arisen will be provided by the Privacy Officer and/or in collaboration with the applicable operational or departmental manager; the time and frequency will be determined by the involved parties.

C. Training Evaluation and Documentation

1. The Privacy Officer will periodically review training content and methodology to evaluate its effectiveness, as well as to establish on-going training goals. Training content and/or mechanisms will be revised as appropriate.

2. The Privacy Officer will be responsible for maintaining documentation of the various training modules/materials provided to workforce members. This includes documentation of targeted specialized training, changes in any training programs, reasons for the training and/or changes, etc.

3. Documentation of completion of Privacy training for MCPH employees will be performed by the Privacy Officer. The Privacy Officer may, in his or her discretion, document web-based Privacy training in an electronic format and in-person training in paper format.

Complaint Policy

Purpose

This policy sets forth MCPH's policy regarding the making of complaints by individuals with respect to MCPH's privacy policies and procedures, compliance with such policies and procedures, or MCPH's compliance with federal or state law applicable to the confidential nature of PHI or PII.

POLICY:

A. The Privacy Officer is responsible for developing and implementing a process whereby individuals may register complaints concerning MCPH's Privacy policies and procedures and MCPH's compliance with those policies and procedures.

B. The Privacy Officer is responsible for documenting all complaints received related to MCPH's compliance with the Privacy policies and procedures and/or applicable state or federal law compliance.

C. Upon receipt of credible complaints of suspected violations or irregularities, the Privacy Officer shall conduct an investigation, as appropriate, into the facts and circumstances surrounding the alleged violation, and take corrective action where appropriate.

D. MCPH will take all reports of wrongdoing seriously. The Privacy Officer shall, upon completion of the appropriate investigation, determine whether the alleged wrongdoing is a violation of state or federal law, a violation of MCPH's Privacy Policies or otherwise poses an economic or reputational risk to the company. The Privacy Officer shall make recommendations for resolution to be reviewed and approved by the Health Commissioner.

E. If the Private Officer believes that the allegation, if true, would constitute a violation of law, he shall, in his discretion, consult with the appropriate legal counsel, and as he deems appropriate, report any allegations of wrongdoing, including the results of any investigation and any subsequent punishments or remedial actions taken, to the Health Commissioner.

F. The Privacy Officer shall document the results of any investigation.

G. No adverse action or retribution of any kind will be taken against an individual because he or she reports in good faith a suspected violation of MCPH's Privacy Policies or other irregularity. MCPH will attempt to treat such reports confidentially and to protect the identity of the individual who has made a report to the maximum extent consistent with fair and rigorous enforcement of this Policy.

Breach Reporting Requirements

Purpose.

The Breach Notification Rules related to the Privacy and Security Rules require MCPH to notify its clients when there has been a breach of unsecured PHI. MCPH also may have contractual obligations to notify if there has been a breach of unsecured PHI.

Policy

A. If PHI or PII has been inappropriately used or disclosed, such use or disclosure must be reported to MCPH's Privacy Officer immediately.

B. The following are examples of the types of occurrences that MCPH staff members should report to the Privacy Officer as potential breaches.

- Emails including identifying information or being sent to or intercepted by a non-intended party
- Failure to lock up PHI or PII outside of business hours
- Sharing systems logon pass codes or leaving them in plain sight
- Removing PHI or PII off premises
- Suspected systems infiltration by non-authorized party
- Individual reported complaint
- Faxing identifying information to the wrong fax number

C. The Privacy Officer will investigate the incident to determine whether it is a breach of PHI or PII and MCPH's reporting obligations.

D. When investigating the incident, the Privacy Officer will determine whether MCPH has reporting obligations to the client or to any other entity. In determining whether the incident is or is not a breach of unsecured PHI, the Privacy Officer will determine whether there is a low probability that the PHI has been compromised. In making his/her determination, the Privacy Officer will take into consideration:

1. The type of information inappropriately used or disclosed
2. The characteristics of the recipient of the information
3. Whether the PHI was actually acquired or viewed
4. The ability to mitigate the inappropriate disclosure

E. If the incident involves PII, the Privacy Officer will review the applicable state reporting requirements and the relevant client arrangement.

Sanctions

Purpose

MCPH has adopted this Sanction Policy to comply with the Health Insurance Portability and Accountability Act of 1996 and the regulations requirement for such a policy, as well as fulfill our duty to protect the confidentiality and integrity of confidential medical information as required by law.

MCPH has adopted Privacy Policies requiring employees or other agents (e.g. interns and contracted staff) to protect the integrity and confidentiality of PHI and PII. MCPH will not tolerate violations of these policies and standards; any such violation constitutes grounds for disciplinary action up to and including termination, and/or professional discipline.

Any employee who believes that that a violation has occurred as a result of his/her own actions or through the actions of another staff member should immediately report the incident to the Privacy Officer. The Privacy Officer will conduct a thorough and confidential investigation. Violations include, but not limited to, the following:

- Breach of client protected health information and confidentiality
- Destruction of data or computer equipment
- Tampering or destruction of physical security
- Violation of HIPAA or other federal or state laws that protect an individual's privacy of protected health information
- Violations of Administrative Policies on PHI

In the discretion of management, MCPH may terminate an employee for the first breach of the privacy and security policy or individual policies, if the seriousness of the offence warrants such action. An employee could expect to lose her or his job for any willful or gross negligence. For less serious breaches, management may respond with a verbal or written warning or reprimand or may recommend suspension without pay, demotion, or other sanctions.

MCPH
Administrative Policy on
Handling PHI in the Office Environment

PURPOSE

To ensure the confidential and appropriate handling of protected health information (PHI) in public and non-public areas of the office environment where potential unauthorized persons are found.

GENERAL POLICY

MCPH and its employees shall utilize reasonable effort to protect privacy and limit disclosure of such information. Generally, if the information identifies the individual and relates to his or her health status, the information is considered protected health information (PHI).. Reasonable effort may include restructuring and/or reorganizing information flow in areas where information is collected; improving personnel practices and habits in day to day activities to better prevent random disclosure of PHI; initiating stricter practices to safeguard client records stored or utilized in public/non-public areas and relocating record storage to more secure locations, including secure electronic storage. The following procedures address these areas and are to be followed to assure PHI confidentiality is maintained.

PROCEDURES – PUBLIC AREAS AND PRIVATE OFFICES

Public Areas

At no time should protected health information be discussed or in any way revealed in public areas of the facility:.

- Whenever practical, keep doorway(s) closed to the front office area to prevent access by unauthorized persons or utilize signs to prevent entry by unauthorized persons.
- Keep all client PHI away from front desk area and public areas and always out of reach.
- Position computer monitors away from public areas at all times to prevent anyone from viewing information on computer screens, or utilize privacy filters on monitor screen.
- Computers must be locked when employees step away from computers.

- When client record folders must be used, records must be placed in folders with identifying information facing away from public areas.
- Avoid conversation in public areas regarding PHI.
- Place shredder or secure disposal containers in public areas for immediate destruction of protected health information that is no longer necessary to be maintained in the client record.
- At the close of the business day, place all client records, and any other materials containing PHI in a preferably locked room/file cabinet out of view and access of unauthorized persons, i.e. cleaning services, maintenance.
- Lock door(s) to records room before leaving.

Private Office

- During office hours when records are in use, records must be safeguarded at all times to prevent accidental disclosure of PHI. A file cabinet, desk drawer, or shielded area behind the desk may be used to store records between clients when records require additional documentation, data entry into computer, quality assurance review, etc.
- Position computer monitor away from public areas to prevent viewing information on computer screen.
- Computers must be locked when employees step away from computers.
- Private office room doors should be closed when discussing client PHI to reduce the risk of conversation flowing into public areas.
- Staff are discouraged from using break and personal areas of the building for discussing or sharing information regarding the care and/or condition of clients. Such discussions or consultations should be done in secure locations in private offices where the potential for disclosure through verbal communications is minimized.
- Family members, friends, sales representatives, maintenance workers, cleaning service, other visitors must not be in work areas where PHI is present during office hours without good reason and authorization of the Privacy Officer. Visitors in the office must be accompanied at all times.
- If emergency repairs or cleanup are necessary in the office during business hours, the Privacy Officer will establish accommodations for these while making a good faith effort to abide by privacy policies to protect PHI.
- When private offices are not in use they must be maintained in orderly fashion with no protected health information in view at any time.

- On a periodic basis the Privacy Officer should walk through the office environment (private offices, storage rooms, etc.) at the close of the business day and check to see that no PHI is inadvertently left out in view of cleaning service, maintenance workers, etc. who may have valid and authorized reason to be in office areas after hours.

MCPH
Administrative Policy on Removal of Protected Information from the Main Office Environment or Facility

PURPOSE

To provide guidelines for the removal of Protected Health Information (PHI) from the office in a way that protects the client's confidentiality in accordance with the Health Insurance Portability and Accountability Act of 1996.

Definitions:

PHI:	Individually identifiable health information that is: 1) transmitted by electronic means, 2) maintained in any medium described in the definition of electronic media (Sec. 162.103), and 3) transmitted or maintained in any other form or medium.
Electronic Media:	The mode of electronic transmission. It includes the Internet (wide-open), Extranet (using Internet technology to link a business with information only accessible to collaborating parties), leased lines, dial-up lines, private networks, and those transmissions that are physically moved from one location to another using magnetic tape, disk, or compact disk media. (Sec. 162.103)
Mobile Media:	Any type of storage media that is easily transported from one place to another (e.g. laptops, tablets)

GENERAL POLICY

All reasonable efforts must be taken to protect and ensure clients' PHI remains secure and confidential when removed, stored or transported away from the facility.

Where electronic media is concerned, it is recommended that all files containing PHI be stored on secure file servers rather than hard drives of desktop computers, laptop computers, and other mobile media. This greatly simplifies the protection of PHI, as well as improves the ability to provide backup and recovery of the PHI. It is recognized, however, that there are situations that require PHI to be stored on media other than file servers. In such situations, adherence to the following procedures is required. It is required that a file system encryption technology be used to encrypt files containing PHI.

PROCEDURES

Removing/Transporting PHI from the Facility

- Prior approval must be obtained from the Privacy Officer before any PHI can be removed from the facility.
    - The Privacy Officer may grant standing approval for employees who regularly remove PHI from the facility in the performance of their jobs. It is recommended that the Privacy Officer maintain a log of these approvals.
- Secure the records for transport.
- You will be held personally responsible for the security of PHI in your possession and if a breach of confidentiality occurs you are liable.
- Upon returning the PHI to the facility store in appropriate location.

Mobile Media

- Electronic computers or devices containing PHI must be password protected so that a password is required to login to the tablet.
- Laptop computers and electronic tablets containing PHI must be physically secured when not in use, or when left unattended. This may be accomplished by placing the laptop in a locked cabinet/closet, leaving the laptop in a locked office, or use of a cable and lock type security system that allows the laptop to be secured to furniture.
- As an additional means of protection, it is required that a file system encryption technology be used to encrypt files containing PHI. This technology would require the use of a key, PIN, or both to gain access to the information in the file.
- Disks, CD's, Magnetic Tape, USB drives and similar storage media will not be used to store or transport PHI.

MCPH
Administrative Policy on Faxing PHI

PURPOSE

To provide guidelines for receipt, use and dissemination of protected health information by analog line facsimile

GENERAL POLICY

Adherence to the company's Policy of Confidentiality is expected with the use of facsimile when transmitting client health information. Fax users must be instructed on the proper procedures for handling of confidential information. It is recommended that specific client healthcare information be faxed only when the data are to be used for client care coordination. HIPAA provisions allow facsimile of data for treatment, payment and healthcare operations without an authorization. Use of the fax for these reasons should only occur when the original document will not serve the purpose. Fax machines must be located in a secure area that is protected from public view and available only to those employees legitimately entitled to access protected health data.

PROCEDURES

<u>For Transmitting PHI</u>

- Use a cover letter for each fax transmission and retain it in correspondence.
- Verify by telephone number when possible the availability of the receiver and log the fax transaction.
- Notify recipients of any misdirected or returned fax and file an incident report.
- When the faxed information is to be included in a medical record, it must be clearly legible, complete, accurate and dated with appropriate signatures as indicated.

- Faxed data must include:

  Date and time of fax transmission
  Sending facility's name and address
  Sending facility's telephone and fax number
  Sender's name
  Receiving facility's name and address
  Receiving facility's telephone and fax number
  Authorized receiver's name
  Number of copies sent
  Statement regarding
  disclosure
  Statement regarding confidentiality

If a fax transmission fails to reach the recipient, check the internal logging system of the fax machine to obtain the recipient's fax number

For Receiving and Handling of Fax

- Remove any incoming material
- Count the number of pages received
- Follow any instructions on the cover letter
- Ensure that the information is routed to the intended receiver in a prompt and secure manner.
- If the recipient is not available to receive the information, seal the faxed documents in an envelope and set aside for pickup, or deliver to the recipient's private mail or pick up basket.
- If the Privacy Officer deems necessary, following receipt of a misdirected fax, send a request using the incorrect fax number, explain the misdirected information and ask for destruction of all documents received
  from the said facility. Complete an incident report and forward to Company Privacy Officer.

Examples of Confidentiality Statements

"The information contained in this facsimile message is privileged and confidential information intended for the use of the addressee listed above. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this Tele-copied information is strictly prohibited. If you have received this facsimile in error, please destroy it and immediately notify us by telephone by calling us at the number above."

"The information contained in this facsimile message is privileged and confidential information intended for the use of the addressee listed above. If you are neither the intended recipient nor the employee or agent responsible for delivering this message to the intended recipient, you are hereby notified that any disclosure, copying, distribution or the taking of any action in reliance on the contents of this facsimile is strictly prohibited. If you have received this facsimile in error, please destroy it and immediately notify us by telephone by calling us at the number above."

"This facsimile may contain confidential or privileged information and is intended only for the recipient named above. Receipt of this transmission by any person other than the intended recipient does not constitute permission to examine, copy or distribute the accompanying material. If you receive this facsimile in error, please notify us by telephone and return the original facsimile to us by mail."

"This message is intended only for the use of the individual or entity to which it is addressed and may contain information that is privileged, confidential and exempt from disclosure under applicable law. If the reader of this message is not the intended recipient or the employee or agent responsible for delivering the dissemination, distribution or copying of this communication is strictly prohibited. If you received this communication in error, please notify us immediately by telephone and return the original message to us at the above address. Thank you."

OHIO DEPARTMENT OF HEALTH
DATA METHODOLOGY STANDARDS FOR PUBLIC HEALTH PRACTICE

Disclosure Limitation Standard:
Tabulations of confidential Ohio Department of Health data shall be suppressed when the table denominator value minus the table numerator value is less than 10.

A. Overview / Summary of Standard

The standard is adopted to limit disclosure of confidential personal information when tabulating confidential information for the public. A table generally includes the following components: a numerator, a denominator and a rate calculated from these two quantities. The numerator is usually a count of persons with some trait or condition. The denominator represents the population of persons from which the numerator was drawn and may or may not be shown in the table. The table rate allows for comparison across denominator populations. The key feature of the standard that allows public release of tables is the existence of a critical minimum number of persons (10) without the trait or condition among the population of interest. If the denominator minus numerator is at least 10, then we judge the likelihood of identity disclosure to be sufficiently small so as to allow for publication of the table. Non-confidential information need not hold to the standard. The standard is not a test of statistical reliability.

B. Rationale / Description of Problem

This standard has been developed to protect the confidentiality of personal health information released by ODH. As public health workers we have an ethical and legal obligation to provide such protection. This protection will help to ensure that providers of these data continue to participate in these data collection activities.

The disclosure limitation issue is one of numerators and denominators, or of cells in a table. Numerators are typically the cases in a public health statistic and denominators are the population from which the cases arise. In tabular data, one can think of a specific cell as the numerator and the row total as the denominator. The characteristic defining the frequency cells or defining the case is often confidential. The risk of disclosure is greatest when the denominator is small and the ratio of numerator to denominator is high. Small denominators are common in tabulations for smaller geographic areas and for subpopulations (e.g., narrow age ranges, race groups, ethnic groups, small geographic areas). In situations with many cases drawn from a large pool of potential cases the risk of disclosure is small.

We usually report data for fairly large populations (e.g., County). Sometimes we need to report data for smaller areas such as census tracts or neighborhoods or for subpopulations (e.g., race groups). These data for small populations are often exactly what data users need to do their public health work of preventing disease and injury. With this standard, ODH has balanced disclosure limitation objectives against a responsibility to disseminate public health information to a wide variety of users and at a geographic and subpopulation level that supports public health work. In developing a disclosure limitation strategy, ODH has balanced the benefits and risks of cautious vs. liberal approaches to data release. On one hand, a cautious approach would suppress more tables based on small numbers and prevent misuse of the data. On the other hand, a liberal approach would disseminate more tables for the widest possible use at greater risk. The standard ODH has chosen for disclosure limitation is a result of how it weighs the relative benefits of (i) preventing misuse of data and (ii) disseminating data to users.

Local health departments, as the principal public health practitioners in the field, have greater access to detailed confidential information than other users. Tabulations compiled for Local Health Departments and for other program-approved users need not abide by the data suppression methodology outlined in this standard. Those approved users must, however, abide by the ODH standard when they re-release

ODH tabulations to the public. Granting greater access to these users presents an added concern of preserving disclosure limitation at a level removed from ODH, and over which ODH has limited control.

The standard has been extensively discussed in the Data and Research Policy Committee of ODH. The standard applies to all tabulations of departmental confidential data, including those produced automatically over the internet in the Information Warehouse. The standard does not apply to the release of observation-level datasets to approved users, except that those users may be expected to adhere to the tabulation standard when producing public reports.

C. Guidelines for Implementation of the Standard

Understand what is confidential A complete and up-to-date listing of confidential datasets and data elements is an important component of this disclosure limitation standard. Research staff must understand which data elements in each dataset are protected by this standard. The standard does not apply to non-confidential datasets, although ODH may at times wish to prevent disclosure of sensitive information from the non-confidential datasets.

Define the numerator(s) and denominator(s) Clear understanding and definition of the numerators and denominators in a table is critical for correct application of this standard. Program research staff must determine in advance which elements of a table represent numerators and which represent denominators. For example, a county low birth weight rates table is a series of 88 low birth weight numerators and total birth denominators (one set for each county). A table of pre-term babies by age is a series of age-specific counts of pre-term birth numerators and age-specific total birth denominators (one set for each county). Some indicator tables don't have clear single numerators. For example, in a county table of mother's marital status one must specify whether the married count or the unmarried count or both counts represent numerators. A different sort of numerator/denominator pair occurs when the very existence of a person in a database is confidential. An example of this is the induced terminations registry. A table of abortion rates by county would have abortion counts as the numerator and the population of women as the denominator.

Assess the impact of applying the standard to a table Once the numerator and denominator are defined, researchers should determine which rows in a table will be suppressed based on the standard. If no suppression is dictated then a single table will meet all needs for the table. If suppression is required the researcher may need to maintain a public version of the table as well as a confidential version for approved users. Researchers should also assess whether suppressed numbers in a table can be calculated from unsuppressed numbers in the same table. Also, researchers need to be aware of other tables already published that may be used to determine suppressed values by subtraction.

Consider changes to tables to increase dissemination of public information There are several strategies available to reduce data suppression in tables. Since disclosure risk is highest when tables include small denominators, researchers should consider aggregating smaller denominators into fewer and larger denominators. For example, researchers might combine multiple years of data together to increase the counts in table cells. A similar strategy would be to group geographic areas together. For example, if a census tract table is overly suppressed perhaps a zip code table would be adequate to represent the geographic variation in a health indicator. Another example in an age-specific table would be to re-define age into broader categories.

Release data in multiple customized formats when necessary Some population groups are important to public health but inherently small in size. For example, teen mothers or Hispanic mothers as denominator groups often lack sufficient observations to pass the standard for County level or City level tables. Researchers should consider special reports to allow for release of important public health statistics for smaller groups that are overly suppressed in automated tabulation systems.

Reference: The "denominator – numerator at least 10" rule was originated by Garland Land, Missouri Dept. Health. He presented the rule at the NAPHSIS/CDC Assessment Initiative Conference in January, 2002 at Minneapolis.