Maternal Infant Health Program (MIHP)
Field Confidentiality Guidelines

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is the federal Health Insurance Portability and Accountability Act of 1996. The overall intent of this law is to make it easier for the consumer to obtain seamless care, irrespective of the number of different providers they see, while still protecting the confidentiality and privacy of the patient.

The law is designed to make it easier for people to keep their health insurance when they change jobs. It sets standards for the electronic exchange of patient information, protecting the privacy and security of consumer health data. The U.S. Department of Health and Human Services issued the Privacy Rule to implement that aspect of the law, and its Office of Civil Rights is in charge of enforcing it.

HIPAA assures privacy and security of Protected Health Information (PHI) and Electronic Protected Health Information (ePHI), as defined below:

Protected Health Information (PHI) is health information combined with any identifier that is created, received, transmitted and/or maintained by a HIPAA-covered entity. Health information includes any information relating directly or indirectly to:

- An individual’s past, present or future physical or mental health
- Provision of care to the individual
- Past, present or future health care bills and payments for provision of health care to the individual

Identifiers include:

- Name
- Address (all geographic subdivisions smaller than state, including street address, city, county, ZIP code, and equivalent geocodes {demographic characterization of a neighborhood/locality})
- Names of relatives
- Names of employers
- All elements (except years) of dates related to an individual, including birth date, admission date, date of service, discharge date, date of death, and exact age if over 89
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social security number
- Medical record number
- Medicaid ID number
- Health plan beneficiary number
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers or serial numbers
- Web Universal Resource locater (URL)
- Internet Protocol (IP) address number
- Biometric identifiers, including finger or voice prints
- Photographic images
- Any other unique number, characteristic, or code that may identify an individual

Electronic Protected Health Information (ePHI) is individually identifiable health information that is:

- Transmitted by electronic media
- Maintained in electronic media

HIPAA applies to PHI which is recorded or transmitted in <u>any</u> form or medium. This includes verbal, written and electronic information.

Covered Entities

HIPAA covered entities are health plans (including health insurance companies and employer-sponsored health plans), health care clearinghouses, and health care providers that engage in defined electronic standard transactions, which generally relate to insurance reimbursement. Examples include hospitals, ambulances/EMTs, private physicians and social workers. MIHP providers are considered covered entities.

MIHP providers, as covered entities, are required to comply with HIPAA. Agency contracts must include language requiring contractors to meet HIPAA standards, including record retention requirements for contractors who store the agency's paper or electronic records.

If an agency violates HIPAA, the agency, not MDHHS, is responsible for securing legal counsel should it become necessary. MDHHS attorneys do not represent MIHP agencies that breach confidentiality or in any other legal matters.

MIHP Staff Required to Comply with HIPAA

All MIHP staff must be familiar with HIPAA requirements. Each staff should have a copy of the *MIHP Field Confidentiality Guidelines* for their own reference.

MIHP staff are responsible for maintaining the privacy and security of all confidential information that they transport, store or access at the office or off site. This includes, but is not limited to the following:

- PHI and ePHI
- Computers that contain or access confidential information
- Any device capable of storing PHI, such as flash or thumb drives

Staff who are assigned to work from home on a part-time or full-time basis in an official capacity are responsible for maintaining the privacy and security of all confidential information in the home environment.

More specifics are provided below.

1. Confidentiality Agreements

a. All staff with access to PHI must sign confidentiality agreements with the MIHP agency before having contact with beneficiaries, handling PHI, or transporting PHI, physically or electronically. This includes the coordinator, professional staff, administrative staff, data entry staff, State of Michigan MILogin System users, and anyone else who has access to PHI.
b. The agency must keep these signed confidentiality agreements on file.

2. IT/Network Security

a. Confidential information or PHI sent from a laptop, Personal Digital Assistant (PDA) and other electronic or mobile devices in the field must be either encrypted or transmission must occur on a password-protected secure network/website.
b. Using the beneficiary's name, even though no other identifying information is provided, is not acceptable in communications sent to her medical care provider or MHP. MIHP providers that wish to send communications electronically must use encryption software.
c. There is one exception to "a." and "b." above. You are not required to encrypt information on your smart phone if the beneficiary indicates that calling or texting her is the best way to reach her. The beneficiary is asked this question during the administration of the *Risk Identifier.*
d. All electronic records containing PHI must be stored in an encrypted or password-protected file.
e. Data entry can take place at the MIHP agency's office, at the beneficiary's home, or at another location but only where confidentiality is assured.

3. Mobile Device Safeguards and HIPAA Security Protection from Malicious Software

a. Anti-virus software must be installed on all home computers and mobile devices used for MIHP business.
b. Employees are required to maintain updates to current operating systems (ex. Microsoft updates/patches).

4. Safeguarding PHI in Transport

a. While it is recommended that PHI not be stored in vehicles due to the inability to maintain triple-locking security, it is sometimes necessary due to practical considerations. In such cases, the following guidelines must be followed:
   - A double-locking system must be used to transport MIHP records to assure there is no inadvertent access to PHI by unauthorized persons.
   - All PHI (hard copies and data stored on laptops) must be transported in a locked box, preferably in the trunk of a locked car.
   - If the vehicle used for transport does not have a trunk, the locked box containing PHI must be secured in an inconspicuous location and the vehicle remains locked at all times.
b. MIHP staff are responsible to ensure that transported PHI be delivered only to the appropriate individuals authorized to receive the information. The agency must have a protocol in place for record delivery.
c. If PHI is transported in service delivery, MIHP staff must assure that they carry the minimum identifiable information necessary to provide service in the field. An agency protocol for maintaining security during service delivery must be in place.
d. PHI related to any beneficiary other than the beneficiary being served at the current visit may not be accessed at that visit.

5. Safeguarding PHI in the Agency Office

a. A triple-locking system must be used in the agency office to secure MIHP records (workable, locking filing cabinet inside an office or room with a locking door, within a building with locking exterior doors and windows).

b. Documents that contain PHI may be visible only to the beneficiary or to agency staff who have signed confidentiality agreements. Records must be shielded from other agency staff, office visitors, etc.
c. The agency office must use a private space for **all** discussions with the beneficiary.
d. The office must use a private space for case conferencing and discussing beneficiary information with other staff, referral sources, etc.

6. Safeguarding PHI in the Staff Home

a. A triple-locking system must be used to store MIHP records in staff homes to assure there is no inadvertent access to PHI by unauthorized persons.
b. Materials must be put away in a locked container or filing cabinet when not being used, and kept in a secure room with a locking door that is not accessible to others, including children, spouses, relatives, other home occupants, and visitors.
c. Documents being worked on that contain PHI must not be visible to anyone other than the MIHP staff. Children, spouses, relatives, other home occupants and visitors must not have access to these documents.
d. The printing of confidential information from home computers should be kept to a minimum and only as needed.
e. Passwords must not be shared or accessible to family members or others.
f. Do not talk on the phone with a beneficiary or about a beneficiary unless other persons in the home are not able to hear.

7. Safeguarding PHI in the Community

a. Any method used to transmit PHI must be secure, including verbal transmission. Do not discuss a beneficiary with another individual in a public setting of any kind, on the phone or face-to-face.
b. Do not talk to any unauthorized person (family, friends, etc.) about a beneficiary at any time or any place, even if you do not state the beneficiary’s name or any other identifying information.

8. Record Retention

a. All records, including hard copy, computer records and e-records, , must be maintained for a minimum of seven (7) years after the last date of service per Medicaid policy, unless a longer retention period is otherwise required under federal or state laws or regulations. <u>Agencies that no longer operate an MIHP remain bound by this requirement.</u>
b. Closed beneficiary records must be maintained in a HIPAA-compliant secure location using a triple-locking system. All accounting records relating to health records must be identified and kept with health records.
c. MDHHS must have access to closed charts for seven (7) years after the date that the MIHP agency closes.

9. Disposal of PHI

a. All media containing PHI or ePHI must be destroyed appropriately (shredded and not identifiable/legible) and must never be placed in regular trash. This includes printed information, documents that have been scanned into the computer, faxes, hard drives, diskettes and CDs. Hard drives must be erased in accordance with industry standards.

Confidentiality Breaches

Report confidentiality breaches to the Office of Civil Rights, US Department of Health and Human Services: http://www.hhs.gov/ocr/privacy/.

Breaches may also be reported to the Michigan Department of Health and Human Services, MIHP office: mihp@michigan.gov.

The Michigan Department of Health and Human Services expects all MIHP providers to comply with all federal confidentiality laws. The field confidentiality guidelines are offered as a minimum requirement. You may read more at the following web site: http://www.hhs.gov/ocr/privacy/index.html