# HIPAA Privacy Procedures
# For Human Resource Staff Administering Group Health Plans

**General Policy:** All protected health information of state group health plan enrollees shall be disclosed only as authorized under this procedure.

## I. Definitions

***HR staff*** means personnel in the human resources office of an appointing authority with access to enrollment and eligibility data of individual enrollees in the state group health plans.

***Privacy Official*** means the person designated by the Department of Civil Service to enforce and administer HIPAA compliance efforts for the Employee Benefits Division in administering the state group health plans. The Privacy Official may designate employees of the Employee Benefits Division to act on the Privacy Official's behalf. The Privacy Official can be contacted by e-mail at MDCS-HIPAA@michigan.gov; by phone at (517) 373-7977 or (800) 505-5011; by fax at (517) 373-3174; or by mail at Privacy Official, Michigan Department of Civil Service, 400 South Pine Street, P.O. Box 30002, Lansing, MI 48909.

***Protected health information*** means all information connected to enrollment and eligibility for enrollees in the state group health plans and all information about these enrollees contained in the HRMN System and the files and documents of state human resources offices.

## II. Access by HR Staff

All human resources staff shall receive a copy of these procedures and training on their implementation. Beginning April 14, 2003, HR staff cannot have direct access to protected health information until completing training on these procedures. An appointing authority must ensure that any new hires receive HIPAA training, which the Employee Benefits Division will make available. Documentation of HR staff's attendance at training must be retained for six years after the employee separates.

Employees who provide limited assistance in completing payroll operations and who otherwise have no direct access to protected health information are authorized by the Privacy Official to access PHI for those limited purposes after signing an acknowledgment form created by the Employee Benefits Division. The Privacy Official must grant written approval for any other personnel outside of the human resources office to have direct access to protected health information.

## III. Protected Health Information Retention

A HIPAA Folder must be kept inside or with the medical personnel file of each employee that contains all documents related to enrollment and eligibility in state health plans created or received after April 14, 2003. Copies of files or documents must be retained for at least six years after separation of the employee. HRMN transactions are archived electronically, so receipts of HRMN transactions do not need to be included in the file. The file contents may include:

- Enrollment forms, including supporting documents such as birth certificates.
- Enrollee use and disclosure authorizations forms
- Employee requests to exercise HIPAA rights
- Documents supporting disclosures to personal representatives and governmental officials
- Documentation of HIPAA training for staff, including acknowledgments for those with limited access to protected health information.
- Documentation of Privacy Official authorization to use or disclose protected health information
- Other documents related to health plans that the Privacy Official requests be included

## IV. Rights of Enrolled Employees

HIPAA creates new rights or modifies existing ones of enrollees related to their protected health information. Requests to exercise these rights shall be handled as follows:

**A. Notice of Privacy Practices.** The Employee Benefits Division has provided a copy of the plans' HIPAA Notice of Privacy Practices to all current employee enrollees. HR staff shall provide all new hires after March 30, 2003 with a copy of the HIPAA Notice of Privacy Practices. HR staff shall also provide a copy of the HIPAA Notice of Privacy Practices when requested by an employee. The notice can be viewed at the Employee Benefits section of the Michigan Department of Civil Service's homepage at www.michigan.gov/mdcs.

**B. Enrollee Information Requests.** Human resources staff shall, upon request, provide an enrolled employee with copies of the contents of the employee's HIPAA Folder and screen prints of HRMN benefit information summarizing the employee's protected health information. If an employee seeks protected health information beyond that available in these sources, instruct the employee to make the request to the Privacy Official in writing. If an employee does not request protected health information in person, HR staff shall reasonably confirm the identity of the employee before disclosure.

HR staff shall also release information to a personal representative (legal guardian, medical power of attorney, etc.) who demonstrates legal authority to make health-related decisions or access protected health information for the employee. Any questions on the authority of the personal representative must be directed to the Privacy Official. HR staff shall include copies of any documentation provided by a personal representative in the enrollee's HIPAA Folder. HR staff must respond to requests within 7 days.

**C. Enrollee Amendment Requests.** An enrolled employee may request that the employee's protected health information be amended. HR staff shall respond to any amendment requests within 14 days. HR staff may respond to and make permissible changes to protected health information in HRMN. This includes address changes, enrollment of new dependents, etc. Acknowledgment of any amendments must be presented to the enrollee. A screen print of the benefit change can satisfy this requirement.

If HR staff is unsure of its authority to process a change, it shall contact the Employee Benefits Division for guidance. If HR staff cannot (for example, the employee is ineligible for a plan or outside the proper enrollment periods) make a requested change, HR staff shall issue a written denial of the request that briefly explains why the amendment cannot be made and includes the following notice:

> If you believe this decision is incorrect, you may file a written appeal to the Employee Benefits Division that explains why the decision is incorrect and includes all necessary documentation. Appeals must be mailed to Employee Benefits Division, Department of Civil Service, P.O. Box 30002, Lansing, MI 48909. If you believe your HIPAA rights have been violated by this decision, you may file a HIPAA Privacy Complaint Form (CS-1782) with the EBD Privacy Official at the same address.

**D. Enrollee Restriction and Accommodation Requests.** An enrolled employee may request (1) additional restrictions on the use and disclosure of the employee's protected health information or (2) confidential communications about protected health information in a different manner than currently done. HR staff shall instruct employees trying to make such requests that they must be made in writing to the EBD Privacy Official.

**E. Information Disclosure Reports.** An enrolled employee may request an accounting of disclosures of the employee's protected health information. HR staff shall instruct employees seeking an accounting that they must make such a request in writing to the EBD Privacy Official.

**F. Privacy Complaints.** If an employee wants to file a privacy complaint, instruct the employee that a written complaint can be filed with the EBD Privacy Official or with the Director of the Department of Health and Human Services. Complaints to the EBD Privacy Official must use the HIPAA Privacy Complaint Form (CS-1782), available at the Employee Benefits section of www.michigan.gov/mdcs.

**V. Authorized Use and Disclosures.** Human resources staff may internally use or externally disclose protected health information in the following circumstances:

- To enter, update, or use enrollment, eligibility, and payroll deduction information in HRMN.
- To coordinate plan administration activities with the Employee Benefits Division.
- Pursuant to requests by an enrolled employee or an employee's personal representative.
- Pursuant to a valid court order, subpoena or warrant, if the Privacy Official is notified of the disclosure as provided below.
- When authorized by the relevant enrollee using the HIPAA Disclosure Authorization Form.
- When authorized by the Privacy Official.

The Employee Benefits Division has created a standard disclosure authorization form that complies with HIPAA requirements. If a completed and signed standard disclosure authorization form is submitted, the disclosure must be made as authorized in the form. If a different form is

used, you must contact the Employee Benefits Division to determine whether the authorization form complies with HIPAA requirements. An employee may present a written revocation of a prior authorization, which prevents any further disclosures in reliance on the previous authorization. Copies of all authorization and any revocations must be maintained in an enrollee's HIPAA Folder.

Any use or disclosure of protected health information must entail the minimum use or disclosure necessary. Any documentation supporting the authority to disclose protected health information to parties other than HR staff and the Employee Benefits Division must be retained in the enrollee's HIPAA Folder until six years after separation.

When disclosing pursuant to a court order, subpoena, or warrant, HR staff must send an e-mail or letter to the Privacy Official detailing the name and employee number of the enrollee whose PHI is disclosed, the disclosure date, the name and address of the recipient, a brief description of the PHI disclosed and the reason for the disclosure. The court document and any other documents related to the disclosure must also be placed in the enrollee's HIPAA folder.

Any doubts regarding the appropriateness of a use or disclosure must be directed to the Privacy Official for clarification.

**VI. Security Measures.** HR staff shall undertake reasonable security measures to avoid the misuse or inappropriate disclosure of protected health information. Such measures include:

- Not remaining logged in to HRMN at an unattended computer
- Not leaving cabinets containing protected health information unsecured and unattended
- Not leaving documents containing protected health information out and unsecured
- Discussing protected health information so as to minimize risks of unintended listeners

**VII. Compliance.** HR staff shall promptly report any unauthorized uses or disclosures of protected health information to the Privacy Official. Violations of this procedure are grounds for discipline and may lead to civil and criminal penalties.