

DHMH POLICY

<http://www.dhmh.state.md.us/policies/inpolm.htm>

OFFICE OF THE INSPECTOR GENERAL-DHMH POLICY 01.03.06
Effective Date: August 17, 2006

POLICY ON ADMINISTRATIVE & ORGANIZATIONAL REQUIREMENTS FOR PRIVACY OF HEALTH INFORMATION

Short Title: **Privacy Administrative Requirements Policy**

I. EXECUTIVE SUMMARY

The Department of Health and Mental Hygiene (DHMH) is committed to protecting the health information of Maryland citizens. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations require that DHMH adopt policies on specific issues. The purpose of this policy and related guidelines is to ensure department-wide consistency in fulfilling the administrative and organizational requirements of Federal and State mandates regarding protection of health information.

The Secretary shall designate one individual as the DHMH Privacy Officer. The roles and responsibilities of the Privacy Officer, the business units and other DHMH components are explained. The Privacy Officer shall coordinate activities of the Privacy Office with the Corporate Compliance Office, the Attorney General's Office, and the DHMH business unit offices to implement, monitor, and enforce the requirements of this and related mandates.

This policy explains the administrative and organizational requirements for privacy in the HIPAA standards including the Department's need to develop conforming relationships with business associates, a complaint process, sanctions against members of the workforce who violate privacy policies or practices, mitigation procedures should a violation occur, protection for whistleblowers, practices to safeguard health information, and retention of documentation otherwise required under the law.

The Office of the Attorney General has determined that DHMH is a single legal entity that performs a variety of healthcare and public health activities, thereby meeting the definition of a "hybrid entity" as defined in the HIPAA regulations. This policy serves to meet the organizational requirement that such designation be officially documented and specifically identifies the DHMH covered health care components in the appendix.

Department of Health & Mental Hygiene
Office of Regulation and Policy Coordination - Policy Administrator
201 West Preston Street - Suite 512 - Baltimore Maryland 21201-2301
Phone 410 767-5934 FAX 410 333-7304

II. BACKGROUND

In adopting this policy, DHMH is demonstrating due diligence toward compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations. This policy also incorporates requirements of the Maryland Confidentiality of Medical Records Act of 1990 and other applicable laws and regulations. These mandates protect and enhance the rights of consumers by ensuring them access to their health information and by providing restrictions over how their health information is used or disclosed. From a broader perspective, they also provide for improved efficiency and effectiveness in the healthcare system through a more uniform nationwide privacy framework.

Those Federal and State laws and regulations that are more stringent than the HIPAA requirements will generally remain in effect and will not be preempted by HIPAA. In addition, some state laws requiring disclosure of health information remain in effect. Certain exceptions from the HIPAA privacy requirements may be identified in the policy or subsequently published guidance.

This version of the Privacy Administrative Rights Policy replaces the version dated April 14, 2003. The major change in this version is the shift in the initiating and responsible agency to the Office of the Inspector General.

III. POLICY STATEMENTS

A. AUTHORITY

The Health Insurance Portability and Accountability Act (HIPAA); Public Law 104-191 authorizes and mandates DHMH to issue this policy.
<http://aspe.os.dhhs.gov/admsimp/pl104191.htm>

B. ROLES AND RESPONSIBILITIES

1. Privacy Officer

- a. The Secretary, DHMH shall designate a Privacy Officer for the Department in the Office of the Inspector General.
- b. The DHMH Privacy Officer is responsible for:
 - (1) developing and assisting in the implementation of all policies, procedures, and guidelines that affect an individual's health information.
 - (2) assuring that practices are adopted by DHMH to protect health information consistent with Federal and State law.
 - (3) assisting covered entities in limiting the incidental use of health information.
- c. The DHMH Privacy Officer shall work cooperatively with the business unit Privacy Contacts to coordinate the duties related to fulfillment of these responsibilities.

2. Business Unit Privacy Contact

- a. The senior manager of each DHMH covered healthcare component shall designate a Privacy Contact whom will act as liaison to the Privacy Office, develop an understanding of the DHMH Individual Rights Policy and related mandates, and perform designated required functions at the business unit level in coordination with the DHMH Privacy Officer.
- b. The Business Unit Privacy Contact shall serve on a department-wide Privacy Committee under the direction of the Privacy Officer.
- c. The Privacy Contact shall maintain information on the unit's business practices that ensure that individual rights are addressed in accordance with policy requirements.
- d. The Privacy Contact serves as the primary contact for the DHMH Privacy Office for release of information and receipt of information related to the business unit's privacy practices.
- e. The Privacy Contact assists the Privacy Office in performing periodic information privacy risk assessments and related ongoing compliance monitoring tasks.
- f. The Privacy Contact serves as a resource for patients and clients concerning their rights under the Notice of Privacy Practices.
- g. The Business Unit Privacy Contact serves as a resource for the Privacy Office for accessing information about the business unit's practices with regards to the implementation of DHMH policies and procedures on individual rights including, but not limited to:
 - (1) tracking an individual's request for access to health information and the resulting action taken;
 - (2) providing an accounting of disclosures for an individual's health information;
 - (3) providing an individual an opportunity to amend his/her health information; and
 - (4) restricting access to health information in accordance with an individual's request as agreed upon by the unit and/or DHMH.
- h. The Privacy Contact is the liaison to the Privacy Office for acquiring information from within the business unit that is needed to resolve complaints that are based on the DHMH privacy policies, in coordination and collaboration with the DHMH Privacy Office, the Corporate Compliance Office, and the Office of the Attorney General.

3. Other DHMH Components

- a. The DHMH Corporate Compliance Office and the DHMH Resident

Grievance System will work with the DHMH Privacy Office to establish a mechanism to log, to track, and to generate reports on complaints within the scope of their respective areas of responsibility.

- b. .The DHMH Office of the Attorney General will provide legal services to the Privacy Office as required.
- c. The DHMH Records Officer will provide assistance regarding the records mandates, including the State and DHMH Records Management Programs, and related functions.
- d. Other DHMH components will advise the Privacy Officer on methods for undertaking matters such as the performance of privacy risk assessments, investigations of complaints, and the applicability of other mandates relevant to the functions of the Privacy Office

C. ORGANIZATIONAL DESIGNATION

- 1. Solely in its capacity as a healthcare provider and as a health plan, DHMH is a covered entity, subject to the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and its implementing regulations.
- 2. DHMH and its employees are also subject to other Federal and State Laws and regulations concerning the confidentiality, privacy and security of health information including the Maryland Confidentiality of Medical Records Act of 1990, http://mlis.state.md.us/cgi-win/web_statutes.exe?ghg&4-301.
- 3. The Department of Health and Mental Hygiene declares itself a “**hybrid entity**” as defined in the HIPAA regulations:
 - a. DHMH is a single legal entity whose business activities include both covered and non-covered functions.
 - b. The Department defines its covered healthcare components as providers and health plans.
 - c. All members of the DHMH workforce are required to complete the applicable HIPAA Training program defined in Policy 02.09.11, HIPAA Training Policy <http://www.dhmh.state.md.us/policies/pdf/020911.pdf>.
 - d. Covered healthcare components of the Department shall implement the practices required of covered entities.
 - e. With the designation of the Department as a hybrid entity, DHMH business units must have appropriate mechanisms to control the flow of data and information from one component of the organization to another, and must account for adequate protection of health information when staff is shared between the components.

- f. Each covered healthcare component of DHMH, as stipulated in the Appendix, must attain compliance with all applicable HIPAA requirements by April 14, 2003.

D. BUSINESS ASSOCIATE AGREEMENTS

1. With assistance from the Office of the Attorney General, DHMH will adopt an appropriate governing document for the Department's business associate relations to include a written agreement template.
2. DHMH may disclose health information to a business associate, or allow a business associate to create or receive health information if DHMH first obtains adequate assurance that the business associate will appropriately safeguard the health information. This requirement **does not apply** to:
 - a. disclosure made to a provider concerning the individual's treatment;
 - b. use or disclosure made to another governmental agency for the purpose of public benefit eligibility or enrollment determinations where the agency is authorized by law to make these determinations; or,
 - c. use or disclosure otherwise authorized by law.
3. If the business associate is another governmental entity, whether internal or external to the Department, DHMH may execute a Memorandum of Understanding (MOU) or like document covering the required terms, or rely on other law that imposes upon the business associate the requirements otherwise authorized.
4. **Oversight Responsibilities:** If DHMH becomes aware of a pattern or practice of a business associate that amounts to a material violation of the agreement, the Department must attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement if feasible, and if not, report the problem to the Office of U.S. Secretary of Health and Human Services.
5. DHMH business units shall report all breaches of a business associate agreement or MOU involving a violation of privacy practices to the Privacy Office within 24 hours of notice of the violation or potential violation.

E. STATE PRE-EMPTION

1. The HIPAA Privacy Rule, as modified, preempts State law if:
 - a. that provision is more stringent than the State law, and
 - b. a covered entity could not possibly comply with both that provision of the State law and the final HIPAA Privacy Rule, as modified; or

- c. The State law creates an obstacle to accomplishment of the goals of the final HIPAA Privacy Rule, as modified.
2. The DHMH Office of the Attorney General's Office will provide guidance on the current analysis of pre-emption issues.
3. Business units must consult the Attorney General's Office to determine whether a provision of State law is more stringent than the HIPAA Privacy Rule.

F. COMPLAINTS TO DHMH

1. The Department shall provide a process for individuals to make complaints concerning requirements of this policy and the related privacy mandates, or the Department's compliance with these mandates.
2. The process for filing a complaint will be explained to patients and to clients in the Notice of Privacy Practices.
3. DHMH employees must file complaints according to the DHMH 01.03.01, Policy on DHMH Corporate Compliance Program, <http://www.dhmh.state.md.us/policies/010301.pdf>
4. The DHMH Privacy Office shall arrange to document all complaints received and their disposition.

G. CHANGES IN THE LAW

1. The Department will update or revise its policies and procedures on health information as necessary to comply with changes in Federal or State laws or regulations dealing with privacy of health information.
2. If a change in law materially affects the DHMH Notice of Privacy Practices, the Privacy Office will promptly document, update, and distribute a revised Notice of Privacy Practices to comply with the applicable law.
3. DHMH will not implement a change to its privacy policies or procedures before distributing a revised Notice of Privacy Practices.

H. MITIGATION

1. The Department shall attempt to mitigate, to the extent practical, any harmful effect known to DHMH of a use or disclosure of health information by an employee or business associate that is in violation of the privacy regulation or DHMH policies and procedures.
2. If DHMH health information has been misused by a business associate, the Department shall:
 - a. investigate the misuse of the health information.

- b. determine if the misuse was serious.
- c. determine if the misuse is repeated.
- d. counsel the business associate on the misuse of health information.
- e. monitor the business associate's performance to ensure that the wrongful behavior has been remedied.
- f. reserve the right to terminate a business associate agreement in the event the misuse of health information continues despite counseling.
- g. maintain a record, either written or electronically, of any communications, actions, or activities conducted to mitigate the harm.

H. APPLICATION OF SANCTIONS BY DHMH

- 1. The Department will apply sanctions to members of its workforce that fail to comply with the policies and procedures on privacy of health information, consistent with the State Personnel System law and the procedures of the DHMH Office of Human Resources.
- 2. DHMH employees shall consult the Attorney General's Office prior to applying any sanctions not consistent with the State Personnel System law.
- 3. The Privacy Officer, in coordination with other offices, shall develop an appropriate method for acquiring and maintaining reports on sanctions that is compatible with other applicable Federal or State laws or contractual agreements which limit access to confidential personnel information.

I. SAFEGUARDS

- 1. The Department shall ensure that appropriate administrative, technical, and physical safeguards are in place to protect the privacy of health information.
 - a. DHMH will take reasonable steps to safeguard health information from any intentional or unintentional use or disclosure that is in violation of privacy protection standards pursuant to DHMH policies and procedures.
 - b. Safeguards may include, but are not limited to the following:
 - (1) Shredding of documents that contain protected health information prior to disposal from offices.
 - (2) Implement records management processes for protecting health information consistent with privacy policies.
(See DHMH 01.03.05 Individual Rights Policy).

- (3) Requiring locking doors to medical records departments, or locking cabinets where medical records are kept, and limiting access to the keys or combinations to such locks.
 - (4) Placing facsimile machines and other office equipment that are used for processing, sending or receiving protected health information in an area with limited access, and limiting use of such equipment to those whose job functions include processing health information.
- c. DHMH business units shall function under standard operating procedures that safeguard health information.
- d. Business units are to maintain awareness and adherence to other applicable DHMH policies and guidance related to technical and physical security, confidentiality, and privacy.
See <http://indhmh/secpolicy/html/infosys.htm>.
- (1) E-mail Security Tips
 - (2) Data Eradication Procedures
 - (3) DHMH Password Standards
 - (4) Laptop, Portable, and Off-site Data Processing Equipment Protocol
 - (5) DHMH 02.01.06, Information Assurance Policy and related Procedural Guidelines

J. WHISTLEBLOWERS

1. The Department shall investigate allegations of misconduct of a member of the DHMH workforce or a business associate when health information is released.
2. Employees who in good faith report a possible violation to appropriate officials may not be subject to retaliation.

K. DOCUMENTATION

1. The Department shall maintain records, either written or electronic, of its privacy policies and procedures, communications required by privacy regulations, or any other actions, activities, or designations required by the privacy regulations.
2. Such documentation required under this policy will be retained for a period of at least six years.

IV. REFERENCES

- Health Insurance Portability and Accountability Act (HIPAA); Public Law 104-191, <http://aspe.os.dhhs.gov/admsimp/pl104191.htm>

The following sections of the final Privacy Rule, as modified, Federal Register on August 14, 2002 (67 Fed. Reg. 51,181 and the Privacy Rule, Federal Register on December 28, 2000 (65 Fed. Reg. 82,462):

§160.201 – Applicability,
§160.202 – Definitions

§160.203 – General rule and exceptions ,
§164.501 – Definitions,
§164.530 – Administrative requirements

- State Records Program, Annotated Code of Maryland, State Government Article, Title 10, §633 et seq., http://mlis.state.md.us/cgi-win/web_statutes.exe?qsg&10-633
- Maryland Confidentiality of Medical Records Act of 1990, Annotated Code of Maryland, Health General Article, §4-301 et seq. http://mlis.state.md.us/cgi-in/web_statutes.exe?ghg&4-301
- COMAR 14.18.02, Records Retention and Disposal Schedules <http://www.mdarchives.state.md.us/msa/intromsa/html/reg02.html>
- DHHM 01.03.05 Individual Rights Policy, <http://www.dhmm.state.md.us/policies/010305sof.pdf>
- DHHM 02.01.06, Information Assurance Policy, <http://www.dhmm.state.md.us/policies/summary.htm>.
- DHHM 02.09.11, HIPAA Training Policy, <http://www.dhmm.state.md.us/policies/pdf/020911.pdf>
- DHHM 02.10.02 Records Policy, <http://www.dhmm.state.md.us/policies/021002v5x.pdf>.
- DHHM HIPAA Intranet Website, <http://www.dhmm.state.md.us/hipaa>.

V. APPENDIX

- DHHM Organization-HIPAA Covered Functions or Entities <http://www.dhmm.state.md.us/policies/010306apdx.pdf>

APPROVED:

/s/ Signature on file

S. Anthony McCann, Secretary, DHHM

August 17, 2006
Effective Date