DHMH POLICY

http://dhmh.maryland.gov/pages/op02.aspx

OFFICE OF THE SECRETARY – Office of the Inspector General (OIG)

DHMH POLICY 01.03.05
Version Effective: May 23, 2016

HIPAA INDIVIDUAL RIGHTS

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), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the Omnibus Final Rule of 2013 (collectively, "HIPAA"), and their 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 individual rights requirements of Federal and State laws regarding protection of health information.

This policy explains the individual rights that are required under the HIPAA standards, including the requirements for adoption and distribution of the Notice of Privacy Practices, the rights of individuals to access and request amendment of their protected health information (PHI), restrictions on use and disclosure of PHI, confidential communications, and accounting of disclosures that have been made of individual's PHI. Individual rights under the Maryland Confidentiality of Medical Records Act of 1990 (MCMRA) and other applicable Federal and State laws and regulations on health information are also included.

II. BACKGROUND

In adopting this policy, DHMH is demonstrating due diligence toward compliance with HIPAA. This policy also incorporates requirements of the MCMRA and other applicable laws and regulations. These laws and regulations protect and enhance the rights of individuals by ensuring them access to their PHI and by providing restrictions over how their PHI is used or disclosed. From a broader perspective, these laws and regulations also provide for improved efficiency and effectiveness in the healthcare system through a more uniform nationwide privacy framework.

This version dated May 23, 2016 replaces earlier versions dated August 17, 2006 and November 16, 2011. This version includes routine edits and relevant changes to HIPAA pursuant to the Omnibus Final Rule.

III. POLICY STATEMENTS

A. AUTHORITY.

- The Health Insurance Portability and Accountability Act (HIPAA) of 1996; Public Law 104-191, and implementing regulations of 45 C.F.R. Parts 160 and 164, authorizes and mandates DHMH to issue this policy. http://aspe.hhs.gov/admnsimp/pl104191.htm
- The Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recoveries and Reinvestment Act of 2009; Public Law 111-5, http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf
- Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and GINA; Other Modifications to the HIPAA Rules (Omnibus Rule) of 2013; 78 Fed. Reg. 5566, https://www.federalregister.gov/articles/2013/01/25/2013-01073/modifications-to-the-hipaa-privacy-security-enforcement-and-breach-notification-rules-under-the
- The Genetic Information Non-discrimination Act of 2008; Public Law 110-233 http://www.eeoc.gov/laws/statutes/gina.cfm
- Maryland Confidentiality of Medical Records Act (MCMRA) of 1990, Annotated Code of Maryland, Health General § 4-301 et seq., http://www.dhmh.maryland.gov/psych/pdfs/Medicalreports.pdf

B. DEFINITIONS.

1. **"Access"** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

2. **Breach.**

   a. **"Breach"** means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule, which compromises the security or privacy of the PHI and is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

      i. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

ii. The unauthorized person who used the PHI or to whom the disclosure was made;

iii. Whether the PHI was actually acquired or viewed; and

iv. The extent to which the risk to the PHI has been mitigated.

b. **"Breach"** does not include:

i. Any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a Covered Entity (CE) or Business Associate (BA) if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Privacy Rule;

ii. Any inadvertent disclosure by a person who is authorized to access PHI at a CE or BA to another person authorized to access PHI at the same CE or BA, or organized health care arrangement in which the CE participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Privacy Rule; or

iii. A disclosure of PHI where a CE or BA has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

3. **Business Associate.**

a. **"Business associate"** means a person or entity that performs certain functions or activities (e.g., claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR §3.20, billing, benefit management, practice management, and re-pricing) that creates, receives, maintains or transmits PHI on behalf of, or provides services (e.g., legal, actuarial, accounting, consulting, data aggregation as defined in 45 CFR §164.501, management, administration, accreditation, or financial services) to the covered entity.

b. **"Business associate"** includes:

i. A health information organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to a covered entity and that requires access on a routine basis to such PHI;

ii. A person that offers a personal health record to one or more individuals on behalf of a covered entity; or

iii.. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate.

c. **"Business associate"** does not include:

i. A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual;

ii. A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR §164.504(f) are met;

iii. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law; or

iv. A covered entity participating in an organized health care arrangement that performs a function or activity as described under 45 CFR §160.103 for or on behalf of such organized health care arrangement, or that provides a service as described in 45 CFR §160.103 to or for such organized health care arrangement by virtue of such activities or services.

4. **"Covered entity"** means a health plan, health care clearinghouse, or health care provider that transmits health information in electronic form in connection with a covered transaction.

5. **"Covered health care component"** means a designated covered health care component of a hybrid entity that would meet the definition of a covered entity or business associate if it were a separate legal entity.

6. **"Disclosure"** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

7. **"Health information"** means any information, whether oral or recorded in any form or medium, that:

a. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

b. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

8. **"Hybrid entity"** means a single legal entity:

a. That is a covered entity;

b. Whose business activities include both covered and non-covered functions; and

c. That designates health care components in accordance with 45 CFR §164.105(a)(2)(iii)(C).

9. **"Individually identifiable health information"** means information that is a subset of health information, including demographic information collected from an individual, and:

a. Is created or received by a covered entity;

b. Relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and

c. Either identifies the individual or could reasonably be used to identify the individual.

10. **"Notice of privacy practices"** means a printed advisory that is generally given to a patient of a covered entity that explains the covered entity's uses and disclosures of the patient's PHI.

The HIPAA Privacy Rule requires that a NPP contain the following elements:

a. The NPP must describe the ways in which the covered entity may use and disclose PHI;

b. The NPP must state the covered entity's duties to protect privacy, provide a NPP, and abide by the terms of the NPP;

c. The NPP must describe individuals' rights, including the right to complain to the US Department of Health and Human Services (HHS) and to the covered entity if they believe that their privacy rights have been violated; and

d. The NPP must include a point of contact for further information and for making complaints to the covered entity.

11. **"Protected health information"** means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

12. **"Single legal entity"** means a legal entity that cannot be further differentiated into units with their own legal identities.

13. **"Workforce"** means employees, volunteers, trainees, and other persons performing work for a covered entity and is under the direct control of the covered entity whether paid or not.

C. ROLES AND RESPONSIBILITIES.

The roles and responsibilities of the DHMH Privacy Officer, the DHMH covered health care components (Covered Components), DHMH Covered Components' Privacy Contacts, and other DHMH components are included in DHMH Policy 01.03.06 HIPAA Privacy Administrative Requirements.

D. NOTICE OF PRIVACY PRACTICES.

1. The DHMH Privacy Office shall issue a Notice of Privacy Practices (NPP), written in plain language that states the individuals' rights with respect to the uses and disclosures of their PHI. The NPP is to be used by the DHMH Covered Components.[1]

2. DHMH and its Covered Components shall provide adequate notice to individuals of the uses and disclosures of their PHI that may be made by DHMH and of individuals' rights with respect to PHI or other confidential healthcare information. DHMH and its Covered Components will maintain documentation of compliance with this policy.

[1] Covered Components may make changes to the NPP where necessary, but it should be substantially similar and must contain the required elements setting forth specific rights assigned to the individual and the responsibility of the Covered Component in using, disclosing, and maintaining the PHI.

3. DHMH and its Covered Components will not limit its obligation to inform an individual of a use or disclosure of the individual's PHI that either Federal or State law requires or permits.

4. DHMH and its Covered Components will retain copies of the notices issued and if applicable, any written acknowledgments of the receipt of the NPP, or documentation of its good faith efforts to obtain such written acknowledgment.

5. DHMH and its Covered Components will provide a copy of the NPP to any individual upon request and will post the NPP on their websites.

6. A copy of the NPP will be posted at each entry points of service where individuals access DHMH or its Covered Components for treatment or services.

7. DHMH and its Covered Components shall provide each individual with a copy of their NPP upon revision of their applicable policies and procedures as identified in the NPP.

8. DHMH Covered Components administering covered functions will issue the NPP to individuals pursuant to this policy.

E. INDIVIDUAL RIGHTS.

1. An Individual's Right of Access to Inspect and Copy Health Information.

a. An individual has a right of access to inspect and obtain a copy of health information contained in a designated record set upon payment of reasonable copying expenses as established under COMAR 10.01.08.04 for DHMH programs or Health General Article, §4-304, Annotated Code of Maryland for other healthcare providers, for as long as the health information is maintained in the designated record set. When DHMH or its Covered Components maintain individuals' PHI using electronic health records (EHR), DHMH and its Covered Components will provide access in electronic format and transmit copies of the PHI to an entity or person designated by the individual, provided that any such choice is clear, conspicuous, and specific.

b. DHMH and its Covered Components must provide individuals with access to their PHI in the form or format requested, when reasonable.

c. DHMH and its Covered Components' workforce shall consult the Office of the Attorney General (OAG), if applicable regarding use of an exception, or for advice on any proposed denial of individuals' request to access their PHI.

d. DHMH and its Covered Components must disclose a record within a reasonable time but no more than 21 working days after the date an individual requests the disclosure.

2. An Individual's Right to Request Restrictions on Use or Disclosure of Health Information.

a. An individual may request that DHMH and its Covered Components restrict the use and disclosure of his or her PHI made for treatment, payment and health care operations (TPO) or disclosures to family or others involved in the individual's care; however, DHMH and its Covered Components are not required to agree to the restriction requested, except as required by law.

b. DHMH and its Covered Components are responsible for approving or denying a restriction. DHMH and its Covered Components workforce shall consult the OAG, as appropriate, for advice on denial of any request for restriction.

c. If DHMH or its Covered Components do agree to the restriction request, they must comply with the agreed restrictions except for purposes of treating the individual in a medical emergency.

d. DHMH and its Covered Components are required to agree to a restriction on disclosure of PHI to a health plan if the individual (or someone on the individual's behalf) pays DHMH or its Covered Components for the item or service in full and the disclosure is for payment or health care operations.

e. DHMH and its Covered Components may terminate their agreement to a restriction if the individual agrees in writing or orally agrees and such agreement is documented.

f. If DHMH or its Covered Components inform the individual that they are terminating the restriction agreement, any PHI that is created or received after the notice, other than PHI related to an item or service paid out of pocket as described in §E(2)(d), may be treated as unrestricted.

3. An Individual's Right to Request Confidential Communications.

a. DHMH and its Covered Components t will accommodate, when practicable, an individual's reasonable request to receive confidential communications of PHI by allowing the individual to request that such communications be made to the individual at an alternative location, or by an alternative means. This right does not generally apply to individuals in residential facilities.

b. DHMH and its Covered Components will not require individuals to explain why they want confidential communications.

c. An individual may request that confidential communication be sent to an alternative address that the individual feels is secure, so that PHI will not be placed in someone else's possession inadvertently.

d. If an individual indicates that the requested PHI will cause endangerment if the request is not approved, DHMH and its Covered Components ordinarily shall discontinue consideration of the reasonableness of the individual's request in determining whether it must accommodate the request.

e. DHMH and its Covered Components may refuse a request for confidential communication if the individual provides no alternative address or method of contact, or if the individual provides no information on how applicable payment will be made.

f. DHMH and its Covered Components are responsible for approving or denying a request for confidential communications. DHMH and its Covered Components shall consult the OAG, if applicable, for advice on denial of any request.

4. An Individual's Right to Request Amendment of Health Information.

a. DHMH and its Covered Components recognize an individual's right to request an amendment or correction of the individual's PHI if the individual makes a written request and believes that the information is incomplete or inaccurate.

b. When DHMH or its Covered Components are informed by another covered entity of an amendment to an individual's PHI, DHMH and its Covered Components must amend the PHI in written or electronic form.

c. If DHMH or its Covered Components accept an amendment request, it must make reasonable efforts to provide the amendment to persons that the individual has identified as needing it and to persons that DHMH or its Covered Components know might rely on the original information to the individual's detriment.

d. If DHMH or its Covered Components denies the individual's request, the individual must be provided with a written denial and allow the individual to submit a statement of disagreement for inclusion in the record.

e. DHMH and its Covered Components must take action on an individual's request within 60 days of its receipt (with one 30-day extension upon written notice to the individual setting forth the reason for the delay and a date on which DHMH or its Covered Components will take action).

f. DHMH and its Covered Components must retain copies of amendment requests and must document the titles of the persons or offices responsible for receiving and processing amendment requests and retain for documentation purposes.

5. An Individual's Right to an Accounting of Disclosures.

a. Upon an individual's request, DHMH and its Covered Components shall provide the person with an accounting of the disclosures of the individual's PHI over the previous 6 years, or a shorter period, if all data is included. A copy of the request and the written accounting that is provided to the individual must be retained for documentation purposes.

b. Exceptions – The types of disclosures that are not required to be provided an accounting of disclosure by DHMH and its Covered Components are disclosures:

i. For treatment, payment, or health care operations;

ii. To the individual or the individual's personal representative;

iii. That are incidental to a use or disclosure otherwise permitted or required by law;

iv. Pursuant to an authorization;

v. For facility directories, to people involved in an individual's care, disaster relief or other allowable notification purposes;

vi. For national security or intelligence purposes;

vii. To correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody;

viii. Of limited data sets; or

ix. That occurred prior to the April 14, 2003 compliance date.

c. DHMH and its Covered Components will provide an accounting for disclosures made through an EHR, including disclosures for treatment, payment, and health care operations. However, the accounting of disclosures made through an EHR is limited to the 3 years prior to the date on which the accounting is requested.

d. DHMH and its Covered Components shall temporarily exclude disclosures made to health oversight agencies or law enforcement from an

accounting if DHMH has written notice from the requesting agency or official that providing an accounting would impede the agency's or official's activities.

e. DHMH and its Covered Components must provide the individual with the first request for a list in any 12-month period at no charge. DHMH may charge the individual a reasonable, cost-based fee in accordance with COMAR 10.01.08.04 for each future request within the 12-month period provided that DHMH or its Covered Components inform the individual in advance of the fee and offers the individual the chance to withdraw or modify the request to avoid or reduce the fee.

f. DHMH and its Covered Components must provide the accounting to the individual within 60 days of receipt of the request (one 30-day extension is allowed with written notification to the requesting individual setting forth the reason for the delay and a date on which the DHMH or its Covered Components will take action).

IV. REFERENCES

- Code of Federal Regulations – Title 45
  The following sections of the Final Privacy Rule, as modified in 45 CFR Parts 160 and 164, revised as of October 1, 2010, discuss the individual's right to inspect and copy protected health information:

  §164.502 – Uses and disclosures of Protected Health Information: general rules
  §164.508 – Uses and disclosures for which an authorization is required
  §164.512 – Uses and disclosures for which an authorization or opportunity to agree or object is not required
  §164.520 – Notice of Privacy Practices for Protected Health Information
  §164.522(a)–Standard: Right of an individual to request restriction of uses and disclosures.
  §164.524 – Access of individuals to protected health information
  §164.526 – Amendment of Protected Health Information
  §164.522(b) – Rights to request privacy protection for protected health information
  Standard: Confidential communications requirements
  §164.528 – Accounting of disclosures of Protected Health Information
  §164.530 (j) – Standard: Documentation
  http://aspe.hhs.gov/admnsimp/final/PvcPre01.htm

- Code of Maryland Regulations (COMAR)
  - COMAR 14.18.02 Records Retention and Disposal Schedules
    http://www.dsd.state.md.us/comar/SubtitleSearch.aspx?search=14.18.02.*
  - COMAR 10.01.08.04 Fees
    http://www.dsd.state.md.us/comar/comarhtml/10/10.01.08.04.htm

- DHMH forms involving individual rights requests

http://indhmh/hipaa/html/guideandforms.html

- DHMH HIPAA Internet Website
  http://dhmh.maryland.gov/Pages/Index.aspx
  and
  http://dhmh.maryland.gov/oig/Pages/divisions.aspx#The_Corporate_Compliance%2c_Ethics_and_Privacy_Office
  or
  http://indhmh/hipaa/ (inside DHMH).

- DHMH Policies

  - DHMH Policy 01.05.06 Records Management Policy.
    http://dhmh.maryland.gov/docs/01.05.06%20DHMH%20Records%20Management%20Policy%205-5-15.pdf

  - DHMH 01.03.06 HIPAA Privacy Administrative Requirements
    http://dhmh.maryland.gov/policy/01.03.06%20Privacy%20Administrative%20Requirements%20and%20Appendix%20-%201-12-12.pdf

- Health Information Technology for Economic and Clinical Health (HITECH) as part of the American Recoveries and Reinvestment Act of 2009; Public Law 111-5
  http://www.gpo.gov/fdsys/pkg/PLAW-111publ5/pdf/PLAW-111publ5.pdf:

- Health Insurance Portability and Accountability Act (HIPAA); Public Law 104-191.
  http://aspe.hhs.gov/admnsimp/pl104191.htm

- HIPAA Omnibus Final Rule,
  http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

- Maryland Confidentiality of Medical Records Act of 1990, Annotated Code of Maryland, Health General Article, §4-301
  http://www.dhmh.maryland.gov/psych/pdfs/Medicalreports.pdf

- Maryland Public Information Act Manual (14th ed.), OAG, 2015
  http://www.oag.state.md.us/Opengov/PIA_manual_printable.pdf

APPROVED:

Van T. Mitchell, Secretary

May 23, 2016
Effective Date

This version DHMH 01.03.05, effective May 23, 2016 supersedes versions dated November 16, 2011 and August 17, 2006.