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

DHMH POLICY 01.03.09
Version Effective: May 23, 2016

HIPAA TRAINING POLICY

I. EXECUTIVE SUMMARY

This policy establishes a HIPAA Training Program for the Department of Health and Mental Hygiene (DHMH) that are mandated by the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the Omnibus Final Rule of 2013, and their implementing regulations (collectively, "HIPAA"). All new workforce members of DHMH must receive Level 1 Training, which is a basic overview of the HIPAA Standards. In addition, all workforce members of DHMH's covered health care components (Covered Components) must receive Level 2 Training on an annual basis, which covers HIPAA more in depth. The policy also requires that all DHMH units document and maintain all of their HIPAA-related training.

.

II. BACKGROUND

The HIPAA Standards mandated that the U.S. Department of Health and Human Services (HHS) develop standards for the maintenance and transmission of protected health information (PHI). The primary objectives of HIPAA are to enhance the privacy and security of PHI and to standardize the reporting and billing processes for all health and medical-related information. PHI that is maintained or transmitted in any medium or form by a DHMH unit is subject to the HIPAA Standards. In addition, the HIPAA Privacy and Security Rules affect the PHI maintenance and transmission of electronic, written, and oral forms of PHI. A DHMH unit's failure to comply with the HIPAA Standards could result in significant penalties to the unit or DHMH.

The HIPAA Standards require that covered entities must provide HIPAA training to its workforce as necessary and appropriate for the members of the workforce to carry out their functions within the covered entity. Such training must occur within a reasonable period after the person joins the workforce. In order to ensure DHMH's compliance with the HIPAA Standards, a Privacy Officer was designated for DHMH in the Office of the Inspector General (OIG).

The Office of the Attorney General (OAG) has determined that DHMH is a single legal entity that performs a variety of health care and public health activities, thereby meeting the definition of a "hybrid entity" as defined in the HIPAA regulations. Consequently, DHMH is divided into Covered

Components and non-covered health care components. A Covered Component is any DHMH unit that would meet the definition of a covered entity or business associate if it were a separate legal entity.

This policy outlines the basic training requirements to meet the goal of ensuring that all DHMH workforce members are presented with an overview of the HIPAA guidelines (level 1 training) and more in depth annual HIPAA training (level 2 training) for workforce members of a DHMH Covered Component.[1]

This version, DHMH 01.03.09 dated May 23, 2016 recodifies and supersedes DHMH Policy 02.09.11 dated November 16, 2011, and the previous versions dated August 17, 2006 and. September 28, 2003. This version contains: 1) Relevant regulatory changes pursuant to the Omnibus Final Rule; 2) Editorial and formatting changes; and 3) Updates to links.

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, http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- 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 Article, §4-301 et seq., http://marylandcode.org/ghg/

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.

[1] List of current DHMH Covered Components can be found in DHMH Policy 01.03.06 HIPAA Privacy Administrative Requirements (See Appendix)

2. **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.

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.

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.

3. **"Code sets"** means under HIPAA, any set of codes used to encode data elements, such as tables of terms, medical concepts, medical diagnostic codes, or medical procedure codes. Code sets include both the codes and their descriptions.

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. **"Due diligence"** means the demonstration of good faith efforts on the part of DHMH to be compliant with all of the HIPAA rules.

8. **"External customer"** means an individual or agency who receives direct services from DHMH.

9. **"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.

10. **"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).

11. **"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;

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

12. **"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.

13. **"Privacy and security"** means the maintenance of PHI in a manner which ensures that access is available only to individuals and/or agencies that have a right to the information.

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

15. "**Transaction"** means the exchange of information between two or more parties to carry out financial or administrative activities related to health care.

16. **"Unit"** means any business unit, department, administration, board, commission, local health department (LHD) or entity within DHMH.

17. **"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. HIPAA TRAINING REQUIREMENTS.

1. New Workforce Members (LEVEL 1 TRAINING).

a. : Every new workforce member in a DHMH unit must receive Level 1 HIPAA training, consisting of an overview of HIPAA, at DHMH headquarters, at their DHMH units or via computer-based training through the DHMH Training Services Division (TSD) via the HUB, and should include, but not be limited to, the following topics:

i. What HIPAA is and how it came to be;

ii. Major components and implementation timeframes of HIPAA (privacy, security, code sets, due diligence, and transactions);

iii. Instances when patient authorization is or is not required before disclosing the patient's PHI;

iv. Treatment, payment, and health care operations;

v. Current departmental policies and State laws regarding HIPAA, including the Maryland Confidentiality of Medical Records Act;

vi. What is considered PHI;

vii. General HIPAA terminology;

viii. Penalties associated with violations of HIPAA rules;

ix. Reporting suspected violations of HIPAA rules;

x. How to obtain additional assistance or information regarding HIPAA within DHMH; and

xi. How HIPAA could affect workforce members and their work unit.

b. Upon completion of Level 1 training, workforce members will sign a form acknowledging receipt of this training. One copy of the acknowledgement form will be given to the workforce member and another will be placed in their official DHMH personnel file.

2. Annual (LEVEL 2 TRAINING).

a. All workforce members of a DHMH Covered Component must receive Level 2 HIPAA training annually, which is more in depth and is job-specific, at their DHMH units or via computer-based training through DHMH TSD via the HUB. This training shall include, but is not limited to, the following topics:

i. Minimum necessary standard;

ii. Business associate agreements;

iii. Permitted use and disclosures;

iv. Notice of privacy practices;

v. Breach Notification Rule;

vi. Privacy Rule;

vii. Security Rule;

viii. Patient's rights;

ix. Penalties (organizational and individual);

x. Physical and workstation security;

xi. De-identification;

xii. Encryption; and

xiii. Electronic transmissions of PHI.

b. Upon completion of Level 2 training, workforce members will sign a form acknowledging receipt of this training. One copy of the acknowledgement form will be given to the workforce member and another will be placed in their personnel file.

c. Each DHMH covered component will provide ongoing Level 2 training for new workforce members where applicable.

D. DOCUMENTATION.

1. The HIPAA Standards require that a covered entity must document that HIPAA training has been provided to its workforce members.

2. It is recommended that the documentation include, but is not limited to, the following:

a. Content;

b. Training dates: and

c. Attendee's name

3. Methods of documenting HIPAA training include, but are not limited to, the following:

a. Training program sign-in sheets;

b. Signed confidentiality statements acknowledging receipt and understanding of any training attended;

c. Electronic access trails to record computer-based training completion or test results;

d. Documenting and retaining meeting handouts, aids, and minutes; and

e. Retention of appropriate email messages.

4. Each DHMH unit must document that it has provided HIPAA training to its workforce, and each unit must retain such documentation for a period of at least 6 years.

E. THE ASSIGNMENT OF RESPONSIBILITIES FOR THE HIPAA TRAINING PROGRAM.

1. The DHMH OIG has the responsibility to periodically audit the Level 2 training records of each DHMH Covered Component to insure compliance with HIPAA training requirements.

2. The Corporate Compliance Officer/Privacy Officer has the responsibility to:

   a. Coordinate the development, scheduling and delivery of computer-based Level 1 and Level 2 Training modules with the DHMH TSD;

   b. Assist DHMH units in conducting Level 1 and Level 2 HIPAA training if requested; and

   c. Incorporate Level 1 training into DHMH headquarters new employee orientation program;

F. CONSEQUENCES FOR INADEQUATE HIPAA TRAINING.

1. HHS can issue a penalty of up to $1.5 million per violation of an identical HIPAA provision in a calendar year. The Office for Civil Rights (OCR) is the enforcement arm of HHS, and it can follow up on any HIPAA breach that is reported to HHS. Training, risk analysis, and documentation are base-line criteria to OCR because they are considered reasonable measures to identify whenever there is a HIPAA breach. In many cases, some aspect of a HIPAA breach involved human error, and if there was inadequate training in a covered entity, it is easy for OCR to state that better training might have prevented the breach.

2. Because most privacy and security breaches involve human mistakes, training can reduce the risk of having such incidents. Breaches are very costly in terms of time, money and reputation to a covered entity. Each member of a workforce is a risk, and the better trained the workforce is regarding “breach pitfalls,” the lower the overall risk will be.

3. Inadequate training will be flagged in a HIPAA audit if an organization is audited.

4. Certain HIPAA violations can lead to civil or criminal penalties for the workforce members of a covered entity. Workforce members may receive discipline at the covered entity, including termination.

5. The OAG can also enforce HIPAA regulations.

IV. REFERENCES

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

- 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 Article, §4-301 et Seq.,
  http://marylandcode.org/ghg/

- 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 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

APPROVED:

Van T. Mitchell, Secretary

May 23, 2016
Effective Date

This version effective May 23, 2016 supersedes and recodifies DHMH 02.09.11 dated November 16, 2011, and previous versions dated August 17, 2006 and September 28, 2003.