DHMH POLICY

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

OFFICE OF THE INSPECTOR GENERAL (OIG) **DHMH POLICY 01.03.07**
Effective Date: July 22, 2014

HIPAA BREACH RESPONSE 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), the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), the Omnibus Rule of 2013, together known as 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 HIPAA breach response requirements.

The Secretary of DHMH has designated a Privacy Officer for DHMH within the Office of the Inspector General (OIG), whose duties include working cooperatively with the DHMH covered components' HIPAA privacy contacts to coordinate the duties related to the fulfillment of these responsibilities. This policy explains the breach response procedures that are required under HIPAA standards, including the requirements for notifying affected individuals in the event of a breach of their unsecured Protected Health Information (PHI).

II. BACKGROUND

The American Recovery and Reinvestment Act of 2009 (ARRA) was signed into law on February 17, 2009. Title XIII of ARRA is the Health Information Technology for Economic and Clinical Health Act (HITECH). HITECH significantly impacted the HIPAA Privacy and Security Rules. While HIPAA did not require notification when patient PHI was inappropriately disclosed, covered entities may have chosen to include notification as part of the mitigation process. HITECH required notification of certain breaches of unsecured PHI to the following: individuals, Secretary of the U.S. Department of Health and Human Services (HHS), and the media. The effective implementation date for these provisions was September 23, 2009.

In January of 2013, HHS released the "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and the Genetic Information Nondiscrimination Act (GINA); Other Modifications to the HIPAA Rules" (Omnibus Rule), which made changes to the HIPAA regulations to improve their workability and effectiveness, increase flexibility, and to decrease burdens on the regulated entities. The Omnibus Rule modified the HITECH definition of a breach to eliminate the previous harm standard. **Effective September 23, 2013**, it states that an "acquisition, access, use, or disclosure in a manner not permitted 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:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.[1]

In adopting this policy, DHMH, as a hybrid entity, is demonstrating due diligence towards its compliance with HIPAA and HIPAA's mandates regarding a covered entity's response to a breach of unsecured PHI. This Breach Response Policy is documented to provide a well-defined, organized approach for handling such a response. This policy outlines steps DHMH will take upon the discovery of the unauthorized acquisition, access, use, or disclosure of PHI, which compromises the security or privacy of the PHI of an individual(s).

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

B. Definitions:

For the purposes of this policy, the following terms have the meanings indicated:

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,

[1] 45 CFR § 164.402.

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"** excludes:

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.
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.[2]

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 C.F.R. 3.20, billing, benefit management, practice management, and re-pricing) that creates, receives, maintains or transmits protected health information on behalf of, or provides services (e.g., legal, actuarial, accounting, consulting, data aggregation as defined in § 164.501, management, administration, accreditation, or financial services) to the covered entity.[3]

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

[2] ARRA/HITECH Title XIII Section 13400; § 164.402.
[3] 45 CFR § 160.103

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 § 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 § 160.103 for or on behalf of such organized health care arrangement, or that provides a service as described in § 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. **"Disclosure"** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

6. **"Encryption"** means the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key.

7. **"Health care component"** means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(C).

8. **"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.

9. **"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 § 164.105(a)(2)(iii)(C).

10. **"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.

11. **"Law enforcement official"** means any officer or employee of an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to investigate or conduct an official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

12. **"Limited data set"** means PHI that excludes the following direct identifiers of the individual or of relative, employers, or household members of the individual:

a. Names;
b. Postal address information, other than town or city, State, and zip code;
c. Latitude, longitude, and census block;
d. Telephone numbers;
e. Fax numbers;
f. Electronic mail addresses;
g. Social security numbers;
h. Medical record numbers;
i. Health plan beneficiary numbers;
j. Account numbers;
k. Certificate/license numbers;

l. Vehicle identifiers and serial numbers, including license plate numbers;
m. Device identifiers and serial numbers;
n. Web Universal Resource Locators (URLs);
o. Internet Protocol (IP) address numbers;
p. Biometric identifiers, including finger and voice prints; and
q. Full face photographic images and any comparable images.

13. **"Organization"** for the purposes of this policy, means the covered entity to which the policy and breach notification apply.

14. **"Personal representative of a deceased individual"** means a person who has authority to act on behalf of the decedent or decedent's estate.

15. **"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.

16. **"Reasonable diligence"** means the business care and prudence expected from a person seeking to satisfy a legal requirement under similar circumstances.

17. **"Unsecured protected health information"** means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5 on the HHS website. Electronic PHI that is password protected but not encrypted is still deemed to be "unsecured."

a. Electronic PHI is not deemed to be "unsecured" if it has been encrypted as specified in the HIPAA Security Rule by the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key and such confidential process or key that might enable decryption has not been breached. To avoid such a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. The following encryption processes meet this standard:

i. Valid encryption process for data at rest (e.g., data that resides in databases, file systems, and other structured storage systems) are consistent with National Institute of Standards and Technology (NIST) Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.
ii. Valid encryption processes for data in motion (i.e., data that is moving through a network, including wireless transmission) are those that comply , as appropriate, with NIST Special Publication 800-52, Guidelines for the

Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to Internet Protocol Security (IPsec) Virtual Private Networks (VPN); or 800-113, Guide to Secure Sockets Layer (SSL) VPNs, and may include others which are Federal Information Processing Standards (FIPS) 140-2 validated.

b. PHI is not deemed to be "unsecured" if the media on which the PHI is stored or recorded has been destroyed in the following ways:

i. Paper, film, or other hard copy media have been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

ii. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.[4]

18. **"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. Discovery of a Breach:

A breach of PHI shall be treated as "discovered" as of the first day on which an incident that may have resulted in a breach is known to DHMH, or by exercising reasonable diligence would have been known to DHMH (includes breaches by DHMH's business associates).[5] DHMH shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent (e.g., business associate acting as an agent of DHMH) of DHMH. Following the discovery of a potential breach, DHMH, in cooperation with its business associate where applicable, shall begin an investigation, conduct a risk assessment, and if warranted based on the investigation and risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed by DHMH to have been accessed, acquired, used, or disclosed as a result of the breach. DHMH shall also begin the process of determining what external notifications are required or should be made (e.g., Secretary of HHS, media outlets, and law enforcement officials).

D. Notification of a Breach:

[4] HHS issued guidance on protecting personally identifiable health care information; document was the work of a joint effort by HHS, its Office of the National Coordinator for Health Information Technology and Office for Civil Rights, and the CMC (Issued 4/17/09).
[5] 45 CFR § 164.404

1. Any member of DHMH who knows, believes, or suspects that a breach of PHI has occurred, shall report the alleged breach to the workforce member's supervisor, covered component's HIPAA privacy contact or Administration's Executive Director immediately.

2. The workforce member's supervisor, covered component's HIPAA privacy contact or Administration's Executive Director, within 5 calendar days, shall provide written and telephonic notice of alleged breach to the DHMH Privacy Officer located within the DHMH Office of the Inspector General. Notice shall include at minimum:

   a. Description of alleged breach.
   b. Date of alleged breach.
   c. Date supervisor, covered component's HIPAA privacy contact, or Administration's Executive Director learned of the breach.
   d. Names and titles of individuals within DHMH with best knowledge to ascertain if a breach has occurred and the steps taken to mitigate.

3. It is the responsibility of DHMH to protect and preserve the confidentiality of PHI of Maryland Citizens. To avoid possible breaches of PHI and inform the DHMH workforce members of the importance of promptly reporting privacy and security incidents and the consequences for failing to do so, the DHMH Privacy Officer will coordinate with other DHMH officials and departments to assist in the training of their workforce members on their respective responsibilities and obligations under HIPAA, which will include a review of the DHMH covered components' annual HIPAA compliance checklists
   (See: http://indhmh/hipaa/pdf/2010/HIPAA_Checklist_Revised_0315010.pdf).

E. Breach Investigation:

After a potential breach is reported, the DHMH Privacy Officer or designee will work with the covered component's HIPAA privacy contact, Administration's Executive Director or designees in order to conduct an investigation, which includes an analysis to determine whether a breach of unsecured PHI has occurred, and if so, what notifications are required. The DHMH covered component's HIPAA privacy contact or designee shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with the DHMH Privacy Officer and others in DHMH as appropriate (e.g., administrations, workforce members, Office of Information and Technology), including the Office of the Attorney General (OAG), if necessary. The DHMH Privacy Officer or designee shall be the key facilitator for all breach notification processes to the appropriate entities (e.g., HHS, media, and law enforcement officials). Within 20 days of the initiation of the breach investigation (more or less time may be necessary depending on the circumstances), the covered component's HIPAA privacy contact, Administration's Executive Director or designees shall provide to the DHMH Privacy Officer, OIG, and OAG a copy of the Breach/Notification report form. (See: http://indhmh/hipaa/pdf/2013/BREACH-DISCOVERY-FORM.pdf). All documentation related to the breach investigation,

including the risk assessment and notifications made, shall be kept on file with the DHMH Privacy Officer and retained for a minimum of 6 years.

F. Risk Assessment:

1. The HIPAA Privacy Rule provides individuals with certain rights regarding their PHI and establishes certain limitations on the use and disclosure of such PHI by covered entities and their business associates. For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the HIPAA Privacy Rule. A use or disclosure of PHI that is incidental to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the HIPAA Privacy Rule and would not qualify as a potential breach. An "acquisition, access, use, or disclosure in a manner not permitted 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:

    a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
    b. The unauthorized person who used the PHI or to whom the disclosure was made;
    c. Whether the PHI was actually acquired or viewed; and
    d. The extent to which the risk to the PHI has been mitigated.

2. The DHMH covered component's HIPAA privacy contact, Privacy Officer, or designee:

    a. Shall document the risk assessment as part of the investigation in the Breach/Notification report form noting the outcome of the risk assessment process;
    b. Has the burden of proof for demonstrating that all notifications were made as required or that the acquisition, access, use or disclosure did not constitute a breach;
    c. Based on the outcome of the risk assessment, determine the need to move forward with breach notification; and
    d. May make breach notifications without completing a risk assessment.

G. Timeliness of Notification:

Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by DHMH or the business associate involved. It is the responsibility of DHMH to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.

H. Delay of Notification Authorized for Law Enforcement Purposes:

If a law enforcement official states to the organization that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, DHMH shall:

1. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the time period specified by the official; or
2. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.[6]

I. Content of the Notice:

The notice shall be written in plain language and must contain the following information:

1. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
2. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
3. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
4. A brief description of what the organization is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
5. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, web site, or postal address.

J. Methods of Notification:

The method of notification will depend on the individuals/entities to be notified. The following methods must be utilized accordingly:

1. Notice to Individual(s): Notice shall be provided promptly and in the following form: [7]

    a. Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If DHMH knows that the

[6] 45 CFR § 164.412
[7] 45 CFR § 164.404

individual is deceased and has the address of the next kin or personal representative of the individual, written notification by first-class mail to the next of kin or personal representative shall be carried out. Some limited examples include:

i DHMH may send one breach notice addressed to both a plan participant and the participant's spouse or other dependents under the plan that are affected by a breach, if they all reside at a single address and all individuals to which the notice applies are clearly identified on the notice. When a plan participant (and/or spouse) is not the personal representative of a dependent under the plan, however, DHMH will address a breach notice to the dependent himself or herself.

ii. In the limited circumstances that an individual affirmatively chooses not to receive communications from DHMH at any written address or email address and has agreed only to receive communications orally or by telephone, DHMH may telephone the individual to request and have the individual pick up their written breach notice from DHMH directly. In cases in which the individual does not agree or wish to travel to DHMH to pick up the breach notice, DHMH shall provide all of the information in the breach notice over the phone to the individual and document that it has done so.

b. Substitute Notice: In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, DHMH will provide a substitute form of notice reasonably calculated to reach the individual. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.

i. In a case in which there is insufficient or out-of-date contact information for fewer than 10 individuals, then the substitute notice may be provided by an alternative form of written notice, telephone, or other means.

ii. In the case in which there is insufficient or out-of-date contact information for ten or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of DHMH's website, or a conspicuous notice in a major print or broadcast media in DHMH's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

c. If DHMH determines that notification requires urgency because of the possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

2. Notice to Media: Notice shall be given to prominent media outlets serving the State and regional area (of the breached individuals) when the breach of unsecured PHI affects 500 or more individuals of the State or jurisdiction.

a. The notice shall be provided in the form of a press release.
b. What constitutes a prominent media outlet differs depending upon the state or jurisdiction where an organization's affected individuals may reside. For a breach affecting more than 500 individuals across a particular state, a prominent media outlet may be a major, general-interest newspaper with a daily circulation throughout the entire state. In contrast, a newspaper serving only one town and distributed on a monthly basis, or a daily newspaper of specialized interest (such as sports or politics) would not be viewed as a prominent media outlet. Where a breach affects more than 500 individuals in a limited jurisdiction, such as a city, then a prominent media outlet may be a major, general-interest newspaper with daily circulation throughout the city, even though the newspaper does not serve the whole state.[8]

3. Notification to HHS Secretary: The DHMH Privacy Officer must provide notice to the HHS secretary concurrently with the notification to the affected individuals (for any breach involving 500 or more individuals) or within 60 days after the end of each calendar year (for breaches involving less than 500 individuals).[9] The DHMH Privacy Officer will notify the HHS Secretary by visiting the HHS website and filling out and electronically submitting a breach report form at: http://www.hhs.gov/ocr/privacy/hipaa/complaints/hipcomplaintform.pdf In the latter case, the DHMH Privacy Officer will maintain a log and other documentation of each breach to ensure that the scope and extent of the information provided to the HHS Secretary is in compliance with HIPAA. The content of the notice will be the same as described above.

K. Maintenance of Breach Information/Log:

As described above and in addition to the reports created for each incident, DHMH shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of individuals affected.[10] The following information shall be collected/logged for each breach:

[8] (HHS Federal register comments, p. 5653, 1/25/13).
[9] Note: If the breach involves "secured" PHI, no notification needs to be made to HHS.
[10] The organization shall delegate this responsibility to one individual (e.g., Privacy Officer).

1. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
2. A description of the types of unsecured PHI that were involved in the breach (e.g., full name, social security number, date of birth, home address, account number).
3. A description of the action taken with regard to notification of affected individuals, the media, and the Secretary regarding the breach.
4. The results of the risk assessment.
5. Resolution steps taken to mitigate the breach and prevent future occurrences.

L. Business Associate Responsibilities:

In 2013, the Omnibus Rule extended liability for compliance to the HIPAA Privacy and Security Rules to business associates and their subcontractors. With these modifications, business associates are now directly liable for impermissible uses and disclosures, provision of breach notification to the covered entity, completing breach risk assessments, breach documentation requirements, and civil and criminal penalties for violations.[11] All business associates of DHMH that access, create, maintain, retain, modify, record, store, transmit, destroy, or otherwise hold, use, or disclose unsecured PHI shall, without unreasonable delay and in no case later than 15 calendar days after discovery of a breach, notify DHMH of such breach even if the business associate has not conclusively determined within that timeframe that the incident constitutes a breach as defined by HIPAA. Such notice shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed by the business associate to have been accessed, acquired, or disclosed during such breach.[12] The business associate shall provide DHMH with any other available information that DHMH is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the business associate of the discovery of the breach, DHMH will be responsible for notifying affected individuals, unless otherwise agreed upon by the business associate to notify the affected individuals. It is the responsibility of DHMH to document this notification.

M. Workforce Training:

DHMH shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the workforce members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and promptly report breaches within the organization, as well as return or destroy PHI, as appropriate for the incident. Workforce members (i.e., HIPAA privacy contacts) that assist in investigating, documenting and resolving breaches are trained on how to complete these activities.

[11] 45 CFR § 164.410
[12] Business Associate responsibility under ARRA/HITECH, and the Omnibus Rule for breach notification should be included in the organization's business associate agreement.

N. Complaints:

DHMH has included contact information in its Notice of Privacy Practices for individuals to make complaints concerning its privacy policies and procedures or its compliance with such policies and procedures. DHMH will take no retaliatory action against individuals if they make such complaints. Individuals have a right to receive notification whenever a breach of their unsecured PHI occurs.

O. Sanctions:

DHMH shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with its privacy policies and procedures.

P. Retaliation/Waiver:

DHMH may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. DHMH may not require individuals to waive their privacy right as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

IV. REFERENCES

- Federal Health Insurance Portability and Accountability Act (HIPAA) of 1996; Public Law 104-191 (1996), and implementing regulations at 45 C.F.R. Parts 160 and 164, codified at 42 U.S.C § 1320d et seq.
  http://aspe.hhs.gov/admnsimp/pl104191.htm

- Federal 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 (2009), codified at 42 U.S.C. § 17931 et seq.
  http://www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf

- DHMH HIPAA Websites
  http://dhmh.maryland.gov/hipaa/SitePages/Home.aspx and
  http://mhcc.dhmh.maryland.gov/hit/HIPAA/Pages?hipaa_main.aspx or http://indhmh/hipaa/ (inside DHMH)

- Maryland Confidentiality of Medical Records Act (MCMRA) of 1990, Annotated Code of Maryland, Health General §4-301, et seq.
  http://dhmh.maryland.gov/psych/pdf/Medicalreports.pdf

- Annotated Code of Maryland, State Government Article, Title 10, § 633
  http://mgaleg.maryland.gov/webmga/frmStatutesText.aspx?article=gsg&section=10-633&ext=html&session=2013RS&tab=subject5

- COMAR 14.18.02, Records Retention and Disposal Schedules
  http://www.dsd.state.md.us/comar/SubtitleSearch.aspx?search=14.18.02.*

- DHMH 02.10.02 Records Policy
  http://dhmh.maryland.gov/policy/02.10.02%20Records%20Retention%20Policy%205-16-02.pdf

- Maryland Public Information Act
  http://www.oag.state.md.us/Opengov/Appendix_C.pdf
- HIPAA Omnibus Final Rule,
  http://www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf
- The Genetic Information Non-discrimination Act
  http://www.eeoc.gov/laws/statutes/gina.cfm

APPROVED:

_____ July 22, 2014
Joshua M. Sharfstein, M.D., Secretary, DHMH **Effective Date**