DHMH POLICY

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

OFFICE OF THE INSPECTOR GENERAL (OIG) **DHMH POLICY 01.03.08**
Effective Date: May 6, 2015

COMPUTERIZED PERSONAL INFORMATION BREACH RESPONSE POLICY

I. EXECUTIVE SUMMARY

The Department of Health and Mental Hygiene (DHMH) is committed to protecting the personal information of Maryland citizens. State Government Article, §10-1301 et seq., Annotated Code of Maryland, Governmental Procedures-Security and Protection of Information, (SB 676) of 2013, requires that DHMH adopt a policy to comply with its mandates. The purpose of this policy and related guidelines is to ensure Department-wide consistency in fulfilling SB 676 requirements in responding to a breach of a security of a system (personal information breach).

The Secretary of DHMH has designated a Privacy Officer for DHMH within the Office of the Inspector General (OIG), whose duties will include working cooperatively with all units within DHMH (e.g., boards, commissions, facilities, administrations, local health departments) to coordinate the duties related to the fulfillment of these responsibilities. This policy explains the computerized personal information breach response procedures that are required under SB676 standards, including the requirements for notifying the Maryland Department of Information Technology (DoIT), the OIG, the Office of the Attorney General (OAG), and the affected individuals in the event of a personal information breach. Thus, this policy applies to individual's computerized personal information, which is defined and outlined in Part III, Section B of this policy.

II. BACKGROUND

The 2013 Session of the Maryland General Assembly passed SB 676 that established for units of local and State government (not including the Judiciary and Legislative branches) specified requirements with regard to the protection of an individual's personal information from unauthorized access. **Effective July 1, 2014**, SB 676 requires the Executive branch, DHMH, and other governmental units (e.g., public institutions of higher education and local agencies) to notify individuals of a breach of their unencrypted personal information. The law defines a breach as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of the personal information.

In order to protect personal information from unauthorized access, use, modification, or disclosure, a unit of local or State government that collects an individual's personal information must implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected and the nature of the unit and its operations. Similarly, a unit that uses a nonaffiliated third party as a service provider (and discloses personal information about an individual) must require that the third party implement and maintain reasonable security procedures and practices as specified by SB 676.

In adopting this policy, DHMH is demonstrating its due diligence towards compliance with SB 676's mandates regarding a government agency's response to a personal information breach. This

Computerized Personal Information Breach Response Policy is documented to provide a well-defined, organized approach for handling such a response. This policy outlines steps that units within DHMH will take upon the discovery or notification of a personal information breach. Consequently, this policy will assist DHMH staff in determining: (1) Whether a computer incident is a SB 676 breach; (2) Whether the computer incident has to be reported to DoIT; and (3) Whether the computer incident involves protected health information (PHI), which would also require a Health Insurance Portability and Accountability Act (HIPAA) breach analysis pursuant to the DHMH HIPAA Breach Response Policy.[1]

III. POLICY STATEMENTS

A. Authority:

State Government Article, §10-1301et seq., Annotated Code of Maryland, Governmental Procedures-Security and Protection of Information (SB 676) of 2013.
http://mgaleg.maryland.gov/2013RS/chapters_noln/Ch_304_sb0676T.pdf

B. Definitions:

1. **Breach.**

   a. **"Breach of the security of a system"** means the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity, of the personal information maintained by a unit.

   b. **"Breach of the security of a system"** does not include the good faith acquisition of personal information by an employee or agent of a unit for the purpose of the unit provided that the personal information is not used or subject to further unauthorized disclosure.

2. **"Computer Incident"** means a violation of computer security policies, acceptable use policies, or standard computer security practices.[2]

3. **"Encryption"** means the protection of data in electronic or optical form, in storage or in transit, using a technology that:

   a. Is certified to meet or exceed the level that has been adopted by the Federal Information Processing Standards (FIPS), FIPS 140-2, issued by the National Institute of Standards and Technology (NIST);[3] and

   b. Renders such data indecipherable without an associated cryptographic key necessary to enable decryption of such data.

[1] HIPAA Breach Response Policy
http://dhmh.maryland.gov/docs/01.03.07%20HIPAA%20Breach%20Response%20Policy%207-22-14%20%281%29.pdf

[2] Refer to NIST SP 800-61 Revision 2 *Computer Security Incident Handling Guide* for guidance in creating an incident management policy and developing plans and procedures to support it.
[3] FIPS 140-2; http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

4. **"Exfiltration"** means the unauthorized transfer of information from an information system.[4]

5. **"Nonaffiliated Third-Party"** means any person or entity other than a unit or its workforce members.

6. **Personal Information.**

   a. **"Personal Information"** means an individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:

      i. A Social Security number;
      ii. A driver's license number, state identification card number, or other individual identification number issued by a unit;
      iii. A passport number or other identification number issued by the United States government;
      iv. An individual Taxpayer Identification Number; or
      v. A financial or other account number, a credit card number, or debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

   b. **"Personal Information"** does not include information that:

      i. Is publicly available information that is lawfully made available to the general public from federal, State, or local government records;
      ii. An individual has consented to have publicly disseminated or listed;
      iii. Except for a medical record that a person is prohibited from re-disclosing under §4-302(d)[5] of the Health-General Article, is disclosed in accordance with the federal Health Insurance Portability and Accountability Act (HIPAA); or
      iv. Is disclosed in accordance with the Federal Educational Rights and Privacy Act (FERPA).

7. **"Personally Identifiable Information"** means any information about an individual maintained by an agency, including:[6]

   a. Any information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, date and place of birth, mother's maiden name, or biometric records; and

   b. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[4]NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, for the definition of exfiltration.
[5]The Maryland Confidentiality of Medical Records Act (MCMRA).
[6]Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). National Institute of Standards and Technology, page 2-1 for the definition of personally identifiable information.

8. **"Reasonable Security Procedures and Practices"** means data security procedures and practices developed, in good faith, and set forth in a written security policy.

9. **"Records"** means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

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

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

C. Security Measures:

1. In general, to protect personal information from unauthorized access, use, modification, or disclosure, a unit that collects personal information of an individual shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information collected and the nature of the unit and its operations.

2. Requirements for third-party service providers:

   a. This subsection shall apply to a written contract or agreement that is in effect or entered into **on or after July 1, 2014**.

   b. A unit that uses a nonaffiliated third-party as a service provider to perform services for the unit and discloses personal information about an individual under a written contract or agreement with the third-party shall require by written contract or agreement that the third-party implement and maintain reasonable security procedures and practices that:

      i. Are appropriate to the nature of the personal information disclosed to the nonaffiliated third-party; and
      ii. Are reasonably designed to help protect the personal information from unauthorized access, use, modification, disclosure, or destruction.

D. Notifying the OIG and the Office of Information Technology of a Breach:

1. Any workforce member of DHMH who knows, believes, or suspects that a personal information breach has occurred, shall report the alleged personal information breach to the workforce member's supervisor, unit's Executive Director, Health Officer, or designee immediately.

2. The workforce member's supervisor, unit's Executive Director, Health Officer, or designee, within 1 business day of the discovery or notification of the personal information breach, or by exercising reasonable diligence should have known about the personal information breach, shall provide a brief written and

telephonic notice of alleged breach to the DHMH Privacy Officer[7] located within the DHMH OIG and to the Security Division located within the DHMH Office of Information Technology(DHMH OIT). Notice shall include at minimum:

a. Description of alleged personal information breach.

b. Date of alleged personal information breach.

c. Date supervisor, unit's Executive Director, Health Officer, or designee learned of the alleged personal information breach.

d. Names and titles of individuals within the unit with the best knowledge to ascertain if a personal information breach has occurred and the steps taken to mitigate.

E. Investigation Following Notice of a Breach or to Determine if incident is a Breach:

1. If a unit that collects computerized data that includes personal information of an individual discovers or is notified of a personal information breach the unit, in cooperation with the DHMH Privacy Officer, DHMH OIT Security Division, and other DHMH staff where appropriate, shall conduct in good faith a reasonable and prompt investigation to determine whether the unauthorized acquisition of personal information of the individual has resulted in the misuse of the information. All documentation related to the personal information breach investigation, including the risk assessment and notifications made shall be kept on file with the unit and the DHMH Privacy Officer and retained for a minimum of 3 years as further indicated under paragraph (4) of this section.

2. Except as provided in subparagraph (b) of this paragraph:

   a. If after the investigation is concluded, the unit determines that the misuse of the individual's personal information has occurred or is likely to occur, the unit or nonaffiliated third party, if authorized under a written contract or agreement with the unit, shall notify the individual of the personal information breach.

   b. Unless the unit or nonaffiliated third-party knows that the encryption key has been broken, a unit or the nonaffiliated third-party is not required to notify an individual under subparagraph (a) of this paragraph if:
      i. The personal information of the individual was secured by encryption or redacted; and
      ii. The encryption key has not been compromised or disclosed.

3. Except as provided in Section H of this policy, the notification required under paragraph (2) of this section shall be given as soon as reasonably practicable after the unit conducts the investigation required under paragraph (1) of this section.

[7] DHMH Privacy Officer, 410-767-5411.

4. If, after the investigation required under paragraph (1) of this section is concluded, the unit determines that notification under paragraph (2) of this section is not required, the unit shall maintain records that reflect its determination for 3 years after the determination is made.

F. Notice of Breach by Nonaffiliated Third-Party:

1. A nonaffiliated third-party that maintains computerized data that includes personal information provided by a unit of the Department shall notify the unit of a personal information breach without unreasonable delay and in no case later than 15 calendar days after the discovery of a personal information breach, if the unauthorized acquisition of the individual's personal information has occurred or is likely to occur.

2. Except as provided in Section H of this policy, the notification required under paragraph (1) of this section shall be given as soon as reasonably practicable after the nonaffiliated third-party discovers or is notified of the personal information breach.

3. A nonaffiliated third-party that is required to notify a unit of a personal information breach under paragraph (1) of this section shall share with the unit information relating to the personal information breach.

G. Risk Assessment of Computer Incident:

1. In order to determine whether a computer incident is deemed to be a personal information breach, which compromises the security, confidentiality, or integrity of the personal information, a unit under the guidance of DHMHOIT and OIG must conduct a risk assessment of at least the following factors:[8]

   a. The type of personal information involved in the computer incident;

   b. The unauthorized person that acquired the personal information;

   c. The cause of the computer incident;

   d. The extent of the computer incident;

   e. Whether the computer incident can be contained;

   f. Whether the personal information was encrypted; and if so, whether the encryption key was broken;

   g. The harm to the affected individuals that could potentially be caused by the computer incident; and

[8] NIST 800-61, Computer Security Incident Handling Guide

h. Whether the unauthorized acquisition of the personal information of the individual has resulted in or is likely to result in the misuse of the information.

2. The unit, in cooperation with DHMH OIT and DHMH Privacy Officer or designee, shall:

a. Document the risk assessment as part of the investigation into the computer incident using the Personal Information Breach Notification Form,[9]or in substantially the same form as the Personal Information Breach Notification Form (see **Attachment**),including the outcome of the risk assessment process;

b. Determine whether the computer incident is deemed to be a personal information breach, resulting in or likely to result in the misuse of the information;

c. Determine the need to move forward with personal information breach notification based on the outcome of the risk assessment.

H. Permissible Delay of Notification of Breach:

1. The notification required under Section E may be delayed:

a. If a law enforcement agency determines that the notification will impede a criminal investigation or jeopardize homeland or national security; or

b. To determine the scope of the personal information breach identify the individuals affected, or restore the integrity of the system.

2. If notification is delayed under paragraph (1)(a) of this section, notification shall be given as soon as reasonably practicable after the law enforcement agency determines that the notification will not impede a criminal investigation and will not jeopardize homeland or national security.

I. Methods for Notification:

The notification required under Section E may be given:

1. By written notice sent to the most recent address of the individual as reflected in the records of the unit;

2. By electronic mail to the most recent electronic mail address of the individual as reflected in the records of the unit if:

a. The individual has expressly consented to receive electronic notice; or

b. The unit conducts its duties primarily through Internet account transactions or the Internet.

[9] Personal Information Breach Notification form can be found on the DHMH website

3. By telephonic notice to the most recent telephone number of the individual as reflected in the records of the unit; or

4. By substitute notice as provided in Section J of this policy if:

   a. The unit demonstrates that the cost of providing notice would exceed $100,000 or that the affected class of individuals to be notified exceeds 175,000; or

   b. The unit does not have sufficient contact information to give notice in accordance with item (1), (2), or (3) of this section.

J. Substitute Notice:

Substitute notice under Section I (4) of this policy shall consist of:

1. Electronically mailing the notice to an individual entitled to notification under Section E if the unit has an electronic mail address for the individual to be notified;

   a. In the event the email gets bounced-back as either no such email or mailbox full, give written notice to the individual as provided in Section I (1).

   b. The written notice to the individual should include that substitute notice to the individual by email was attempted but was unsuccessful.

2. Conspicuous posting of the notice on the Web site of the unit if the unit maintains a Web site; and

3. Notification to appropriate media.

4. Other means that are reasonably calculated to reach the individual.

K. Contents of Notification:

1. The notification required under Section E shall include:

   a. To the extent possible, a description of the categories of information that were, or are reasonably believed to have been, acquired by an unauthorized person, including which of the elements of personal information were, or are reasonably believed to have been, acquired;

   b. Contact information for the unit making the notification, including the unit's address, telephone number, and toll-free telephone number if one is maintained;

   c. The toll-free telephone numbers and addresses for the major consumer reporting agencies; and

d. The toll-free telephone numbers, addresses, and Web site addresses for:

i. The Federal Trade Commission; and
ii. The Office of the Attorney General

A statement that an individual can obtain information from these sources about steps the individual can take to avoid identity theft.

2. The notification under Section E shall not include:

a. Protected health information (PHI), such as clinical information, HIV/AIDS status, test results, etc.

b. Any other information that if obtained by an unauthorized person, could result in significant harm to the individual.

L. Requirements for Notice to 1,000 or More Individuals:

1. In general, if a unit is required to give notice of breach of the security of a system to 1,000 or more individuals, the unit also shall notify, without unreasonable delay, each consumer reporting agency[10] that compiles and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. §1681a(p),[11] of the timing, distribution, and content of the notices.

2. Names and other information not required. This section does not require the inclusion of the names or other personal identifying information of recipients of notices of the personal information breach.

M. Prior Notice of Breach to be Provided to the Office of the Attorney General and the Department of Information Technology:

1. Before giving the notification required under Section E, a unit shall provide notice of a personal information breach.to the OAG's Consumer Protection/Identity Theft Unit.[12] A unit shall also notify the Assistant Attorney General assigned to provide legal advice to the affected unit.

2. In addition to the notice required under paragraph (1) of this section, a unit shall provide notice of a personal information breach.to DoIT, DHMH OIT, and the OIG as described in Sections D and N.

[10] List of Consumer Reporting Agencies; http://files.consumerfinance.gov/f/201207_cfpb_list_consumer-reporting-agencies.pdf
[11] 15 U.S.C. § 1681a(p); http://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf

[12] Contact the OAG Identity Theft Unit at 410-576-6491; E-mail: idtheft@oag.state.md.us

N. Reporting of a Computer Incident to the Department of Information Technology:

1. Pursuant to the DHMH Information Security Policy, 02.01.01, and the State of Maryland's Information Security Policy, DHMH must report computer incidents and events (any observable occurrence in a network or system) to the DHMH OIT Security Division, who will notify DoIT. This reporting requirement applies to all LHDs, including those LHDs that are not on the "DoIT Infrastructure." [13]

2. With respect to the notice to DoIT, pursuant to a personal information breach, which is required under Section M, units must coordinate all reports of computer incidents to DoIT through DHMH OIT by sending *a* summary of the incident to DHMH OIT's security incident email address,[14]after verifying that an incident has occurred. Units are asked to provide as much information about the incident as possible, including:

    a. The computer incident category;[15]

    b. How the computer incident was discovered;

    c. Affected IP addresses;

    d. Port numbers;

    e. Information about the affected unit's system;

    f. Impact to the unit; and

    g. Final resolution.

3. DHMH OIT and OIG will assess the information provided by a unit, which will be obtained from DHMH OIT's security incident email address, in order to determine whether the computer incident must be reported to DoIT. If the information provided is insufficient to make such a determination, DHMH OIT and/or the OIG will contact the unit that provided the information in order to obtain additional information as needed.

O. Reportable Incidents-Additional Agency Guidance:

DoIT has outlined the specific incident reporting categories as delineated below. In order to help agencies in determining whether a computer incident meets the threshold of a reportable event, note below the following listed categories[16] that will help to define when computer incidents should be reported to DoIT through DHMH OIT. If any of the listed yield a yes (Y) response, the incident must be reported to DoIT through DHMH OIT as described in Section N.

[13] DoIT Infrastructure pertains to State of Maryland systems where information is processed, stored or transmitted. LHDs on County systems must also adhere to the reporting requirement.
[14] DHMH.securityincident@maryland.gov
[15] State of Maryland Information Security Policy, Page 19.
[16] NIST 800-61, Computer Security Incident Handling Guide

Agency Incident Categories

Category	Name	Description
CAT 1	Unauthorized Access	In this category, an individual gains logical or physical access, without permission, to a state agency's network, system, application, data, or other resource.
CAT 2	Denial of Service (DoS)	An attack that *successfully* prevents or impairs the normal functionality of networks, systems or application by exhausting resources. This activity includes being the victim or participating in the DoS.
CAT 3	Malicious Code	*Successful* installation of malicious software (e.g., virus, worm, Trojan Horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus (AV) software.
CAT 4	Improper Usage	A person violates acceptable computing use policies in Section 11 of the State of Maryland Information Security Policy or Sections 10 & 11 of the DHMH Information Security Policy.

Functional Impact Categories

Category	Definition	Reportable to DoIT
None	No effect to the organization's ability to provide all services to all users	N
Low	Minimal effect; the organization can still provide all critical services to all users but has lost efficiency	N
Medium	Organization has lost the ability to provide a critical service to a subset of system users	Y
High	Organization is no longer able to provide some critical services to any users	Y

Information Impact Categories

Category	Definition	Reportable to DoIT
None	No information was exfiltrated, changed, deleted or otherwise compromised	N
Privacy Breach	Sensitive personally identifiable information (PII) of taxpayers, employees, beneficiaries, etc. was accessed or exfiltrated	Y
Proprietary Breach	Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated	Y
Integrity Loss	Sensitive or proprietary information was changed or deleted	Y

Recoverability Impact Categories

Category	Definition	Reportable to DoIT
Regular	Time to recovery is predictable with existing resources	N
Supplemented	Time to recovery is predictable with additional resources	Y
Extended	Time to recovery is unpredictable; additional resources and outside help are needed	Y
Not Recoverable	Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation	Y

P. Computer Incidents Involving Protected Health Information (PHI):

Computer Incidents involving PHI [17] may also have to be reported to DoIT through DHMH OIT using DHMHOIT's security incident email address. Consequently, a personal information breach analysis may have to be conducted as well as a HIPAA breach analysis, pursuant to the HIPAA Breach Response Policy, if the personal information that was improperly accessed, used, modified, or disclosed includes health information and any one of the eighteen PHI identifiers (e.g., name, social security number, Medicaid number). [18]Thus, a computer incident could eventually be deemed to be both a personal information breach and a HIPAA breach, neither, or a combination of the two.

Q. Destruction of Records:

When a unit is destroying [computerized] records of an individual that contain personal information of the individual, the unit shall take reasonable steps to protect against unauthorized access to or use of the personal information, taking into account:

1. The sensitivity of the records;

2. The nature of the unit and its operations;

3. The costs and benefits of different destruction methods; and

4. Available technology.

If a personal information breach occurs during the destruction of records, then a unit must follow the reporting instructions in this policy.

R. Maintenance of Breach Information/Log:

As described above and in addition to the reports created for each computer incident, the DHMH Privacy Officer shall maintain a process to record or log all personal information breaches that are reported to the OIG regardless of the number of

[17] 45 CFR § 160.103 for the definition of PHI
[18] *Id*. at § 164.514 for listing of 18 PHI identifiers

individuals affected. The following information shall be collected and logged for each personal information breach:

1. A description of what happened, including the date of the personal information breach, the date of the discovery of the personal information breach, and the number of individuals affected, if known.

2. A description of the types of personal information that were involved in the personal information breach (e.g., full name, social security number, account number).

3. A description of the action taken with regard to notification of affected individuals and/or other parties regarding the personal information breach.

4. The results of the risk assessment.

5. Resolution steps taken to mitigate the personal information breach and prevent future occurrences.

S. Preemption:

The provisions of this policy are exclusive and shall preempt any contrary provision of a policy or regulations of the unit.

T. Workforce Training:

It is the responsibility of DHMH to protect and preserve the confidentiality of personal information of Maryland Citizens. To avoid possible personal information breaches and inform the DHMH workforce members of the importance of promptly reporting computer incidents and the consequences for failing to do so, the DHMH Privacy Officer and DHMHOIT will coordinate with other DHMH officials and units to assist in the training of their workforce members on their respective responsibilities and obligations under SB 676.

U. Sanctions:

Any workforce member in violation of this policy may be subjected to the appropriate disciplinary action up to and including termination of employment.

V. Waiver Deemed Void and Unenforceable:

A waiver of any provision of this policy is deemed contrary to agency policy and is void and unenforceable.

W. Compliance:

A unit or nonaffiliated third-party that complies with § 501(b) of the federal Gramm-Leach-Bliley Act (GLBA); 15 U.S.C. § 6801, § 216 of the federal Fair and Accurate Credit Transactions Act (FACTA); 15 U.S.C. § 1681W Disposal of Records; the federal Interagency Guidelines Establishing Information Security Standards; and the federal Interagency Guidance on Response Programs for Unauthorized Access to Customer

Information and Customer Notice; and any revisions, additions, or substitutions of those enactments, shall be deemed to be in compliance with this policy. Compliance with this policy does not relieve a unit from a duty to comply with any other requirements of federal law relating to the protection and privacy of personal information.

IV. REFERENCES

- State Government Article, §10-1301 et seq., Annotated Code of Maryland, Governmental Procedures- Security and Protection of Information, (SB 676) of 2013.
  http://mgaleg.maryland.gov/2013RS/chapters_noln/Ch_304_sb0676T.pdf

- 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.aspxand
  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, Health General Article, §4-301 et seq.,Annotated Code of Maryland
  http://dhmh.maryland.gov/psych/pdf/Medicalreports.pdf

- DHMH Information Technology Technical Security Policy, Standards & Requirements (DHMH Policy 02.01.01)
  http://employeecentral.dhmh.maryland.gov/infosec/pdf/DHMH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf

- State of Maryland Information Security Policy.
  http://doit.maryland.gov/publications/doitsecuritypolicy.pdf

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

- DHMH HIPAA Breach Response Policy (DHMH Policy 01.03.07)
  http://dhmh.maryland.gov/docs/01.03.07%20HIPAA%20Breach%20Response%20Policy%207-22-14%20(1).pdf

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

- DHMH Information Assurance Policy (DHMH Policy 02.01.06)
  http://www.dhmh.maryland.gov/SitePages/summary.aspx

- DHMH Employee Information Technology Security: Protecting Non-Public Information Policy (DHMH Policy 02.01.01)
  http://dhmh.maryland.gov/docs/02.01.01%20EITS%2010-16-13.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

- Federal Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; 12 CFR Part 570, Appendix B to part 570.
  http://www.fdic.gov/news/news/financial/2005/fil2705a.pdf

- Federal Interagency Guidelines Establishing Information Security Standards; 12 CFR Appendix F to Part 225.
  http://www.gpo.gov/fdsys/pkg/CFR-2012-title12-vol3/pdf/CFR-2012-title12-vol3-part225-appF.pdf

- 15 U.S.C. 1681W-Disposal of Records.
  http://www.gpo.gov/fdsys/pkg/USCODE-2010-title15/pdf/USCODE-2010-title15-chap41-subchapIII-sec1681w.pdf

- Federal Fair and Accurate Credit Transactions Act (FACTA) of 2003; (Public Law 108-159).
  http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf

- Federal Gramm-Leach-Bliley Act (GLBA); also known as the Financial Services Modernization Act of 1999 (Public Law 106-102).
  http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf

- Federal Family Educational Rights and Privacy Act (FERPA) of 1974; codified at 20 U.S.C. §1232g; 34 CFR Part 99.
  http://www2.ed.gov/policy/gen/guid/fpco/pdf/2012-final-regs.pdf

- NIST SP 800-61 Revision 2 *Computer Security Handling Guide*
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

V. ATTACHMENT

- Personal Information Breach Notification Form
  http://indhmh/hipaa/pdf/2015/Personal-Information-BREACH-NOTIFICATION-FORM.pdf

APPROVED:

Van T. Mitchell, Secretary, DHMH

May 6, 2015
Effective Date

SB 676 PERSONAL INFORMATION BREACH/NOTIFICATION FORM

Department of Health and Mental Hygiene
Investigation and Risk Assessment

DETERMINING A PERSONAL INFORMATION BREACH:

Was there an unauthorized acquisition of Personal Information (PI) as the result of a computer incident?
_____

If yes, explain: _____
_____
_____

Does the computer incident also involve an impermissible acquisition, access, use or disclosure of Protected Health Information (PHI)? (Y or N)
If yes, complete this form and also adhere to the DHMH HIPAA Breach Response Policy.

Does the computer incident involve any of the following exceptions to the definition of Personal Information? _____
If yes, which one? _____
_____

1) Is publicly available information that is lawfully made available to the general public from federal, State, or local government records;

2) An individual has consented to have disseminated or listed;

3) Except for a medical record that a person is prohibited from re-disclosing under § 4-302(d) of the Health-General Article, is disclosed in accordance with the Health Insurance Portability and Accountability Act (HIPAA); or

4) Is disclosed in accordance with the Federal Educational Rights and Privacy Act (FERPA).

What type of Personal Information is involved in the computer incident? _____
_____

Who was the unauthorized person that acquired the Personal Information? _____
_____

What was the cause of the computer incident? _____
_____

What was the extent of the computer incident? _____
_____

Can the computer incident be contained? _____
_____

Was the Personal Information encrypted? _____
And if so, was the encryption key broken? _____

What type of harm could potentially be caused by the computer incident? _____
_____
_____

Will the unauthorized acquisition of the Personal Information of the individual(s) result in or is likely to result in the misuse of the information? _____
_____

DO YOU THINK THIS CONSTITUTES A SB 676 BREACH OF PERSONAL INFORMATION UNDER THE DHMH PERSONAL INFORMATION BREACH RESPONSE POLICY? WHY OR WHY NOT? (Explain your logic)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Notes: (anything else not covered)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

COMPLETE THE FOLLOWING WHERE APPLICABLE:

***Information about the Unit:**

Name: _____
Address: _____
_____
Investigator:_____ Phone:_____
Email:_____

***Information about the Nonaffiliated Third-Party:** (if applicable)

Name: _____
Address: _____
_____
Investigator: _____ Phone: _____
Email:_____

***Information regarding the Breach:**

Date of Breach: _____ Date of discovery: _____
Approximate # of individuals affected? _____ 1000 or more? _____
Type of Breach: (e.g., unauthorized access, denial of service, malicious code, improper usage, improper destruction):_____
_____
Location of Breached Information: (e.g., laptop, desktop, email, network, data base)
_____
_____

Type of Personal Information involved: (e.g., demographic, financial, ID number)
_____
_____

Brief description of the Breach:
_____
_____
_____
_____

Types of safeguards that were in place prior to the Breach: (e.g., firewalls, encryptions, locks)
_____
_____

***Notice of Breach and Actions Taken:**

Date(s) Notice was given to individual(s): _____
Was substitute notice required? (Y or N) _____
Was Media Notice required? (Y or N)_____
Actions taken in response to the Breach: (e.g., mitigation, sanctions, safeguards, policies)
_____
_____

Describe the actions taken: _____
_____
_____

*** Required fields:** These fields will be a part of the log that is maintained by the DHMH Privacy Officer. Please make sure they are filled out as thoroughly and as accurately as possible.

_____ _____
Name Date

_____
Signature