DHMH POLICY

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

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

DHMH POLICY 01.03.06
Version Effective: May 23, 2016

HIPAA PRIVACY ADMINISTRATIVE REQUIREMENTS

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 (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 administrative and organizational requirements of Federal and State mandates regarding the privacy and security of protected health information (PHI).

The Secretary shall designate one individual as the DHMH Privacy Officer. The roles and responsibilities of the Privacy Officer and DHMH health care components (Covered Components) are explained. The DHMH Privacy Officer shall coordinate activities of the Privacy Office with the Corporate Compliance Office, the Office of the Attorney General (OAG), and DHMH Covered Components to implement, monitor, and enforce the requirements of this and related mandates.

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

The 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. This policy serves to meet the organizational requirement that such designation be officially documented and specifically identifies the DHMH Covered Components in the appendix.[1]

[1] The Covered Component Appendix currently only reflects DHMH components that meet the definition of a covered entity (health plan, health care provider, or health care clearinghouse); however, it is in the process of being revised to also include DHMH components that meet the definition of a business associate (creates, receives, maintain or transmits PHI).

II. BACKGROUND

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

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

This version dated May 23, 2016 replaces the versions dated April 14, 2003 and August 17, 2006. 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, 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. **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"** 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. **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; 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.

3. **"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.

4. **"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.

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. **"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.

7. **"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).

8. **"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.

9. **"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.

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

11. **"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.

1. Privacy Officer.

a. The Secretary of DHMH shall designate a Privacy Officer for DHMH within the Office of the Inspector General (OIG).

b. The DHMH Privacy Officer is responsible for:

i. Developing and assisting in the implementation of all policies, procedures, and guidelines that affect an individual's PHI.

ii. Assuring that practices are adopted by DHMH to protect PHI consistent with Federal and State law.

iii. Assisting Covered Components in limiting the incidental use of PHI.

c. The DHMH Privacy Officer shall work cooperatively with the Covered Components' Privacy Contacts to coordinate the duties related to the fulfillment of these responsibilities.

2. Covered Component Privacy Contact.

a. The senior manager of each DHMH Covered Component shall designate a Privacy Contact whom will act as liaison to the Privacy Officer, develop an understanding of the DHMH Individual Rights Policy (DHMH Policy 01.03.05) and related mandates, and perform designated required functions at the Covered Component level in coordination with the DHMH Privacy Officer.

b. Each Covered Component's Privacy Contact shall serve on a Department-wide Privacy Committee, if developed, under the direction of the DHMH Privacy Officer or designee.

c. Each Privacy Contact shall maintain information on the Covered Component's practices that ensure that individual rights are addressed in accordance with policy requirements.

d. Privacy Contacts serve as the primary contact to the DHMH Privacy Officer for release of information and receipt of information related to the Covered Component's privacy practices.

e. Privacy Contacts assists the DHMH Privacy Officer in performing HIPAA breach investigations, periodic information privacy risk assessments and related ongoing compliance monitoring tasks.

f. The Privacy Contacts serve as a resource for patients and clients concerning their rights under the Covered Components' Notice of Privacy Practices (NPP).

g. The Privacy Contacts serve as resources for the DHMH Privacy Officer for accessing information about the Covered Components' practices with regards to the implementation of DHMH policies and procedures on individual rights including, but not limited to:

i. Tracking an individual's request for access to PHI and the resulting action taken;

ii. Providing an accounting of disclosures for an individual's PHI;

iii. Providing an individual an opportunity to amend his/her PHI; and

iv. Restricting access to PHI in accordance with individual's request as agreed upon by the Covered Component and/or DHMH.

h. The Privacy Contact are liaisons to the DHMH Privacy Officer for acquiring information from within the Covered Component that is needed to resolve complaints that are based on the Covered Component's and/or the Department's privacy policies, in coordination and collaboration with the DHMH Privacy Officer, the Corporate Compliance Office, and the (OAG)..

3. Other DHMH Components.

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

b. The OAG will provide legal services to the Privacy Officer as required.

c. The DHMH Records Officer, or designee, will provide assistance regarding the records mandates, including the State and DHMH Records Management Programs, and related functions.

d. Other DHMH Covered Components will advise the DHMH Privacy Officer on their methods for undertaking matters such as the performance of privacy risk assessments, investigations of complaints, and the applicability of other mandates relevant to the functions of the Privacy Office.

D. ORGANIZATIONAL DESIGNATION.

1. Solely in its capacity as a healthcare provider and as a health plan, DHMH is a covered entity, subject to the provisions of HIPAA.

2. DHMH and its Covered Components' workforce are also subject to other Federal and State Laws and regulations concerning the confidentiality, privacy and security of PHI, including the **MCMRA.**

3. DHMH declares itself a "**hybrid entity**" as defined in the HIPAA regulations:

   a. DHMH is a single legal entity whose business activities include both covered and non-covered functions.

   b. The Department defines its Covered Components as those that meet the definition of a covered entity or business associate.

   c. All members of the DHMH workforce are required to complete the applicable HIPAA Training as defined in DHMH Policy 01.03.09 HIPAA Training Policy.

   d. Covered Components shall implement the practices required of the DHMH, which is the covered entity.

   e. With the designation of DHMH as a hybrid entity, DHMH Covered Components must have appropriate mechanisms to control the flow of data and information from one component of the organization to another, and must account for adequate protection of PHI when staff is shared between the components.

E. BUSINESS ASSOCIATE AGREEMENTS.

1. With assistance from the OAG, DHMH has developed a business associate agreement, which is to be used by all Covered Components where necessary.

2. DHMH and its Covered Components may disclose PHI to a business associate, or allow a business associate to create or receive PHI if DHMH or its Covered Components first obtains adequate assurance that the business associate will appropriately safeguard the PHI. This requirement **does not apply** to:

   a. Disclosure made to a provider concerning the individual's treatment;

   b. Use or disclosure made to another governmental agency for the purpose of public benefit eligibility or enrollment determinations where the agency is authorized by law to make these determinations; or,

   c. Use or disclosure otherwise authorized by law.

3. If the business associate is another governmental entity, whether internal or external to the DHMH, a Covered Component may execute a Memorandum of Understanding (MOU) or like document covering the required terms, or rely on other law that imposes upon the business associate the requirements otherwise authorized.

4. Oversight Responsibilities. If DHMH or a Covered Component becomes aware of a pattern or practice of a business associate that amounts to a material violation of the agreement, DHMH or a Covered Component must attempt to cure the breach or end the violation, and if such attempt is unsuccessful, terminate the agreement if feasible, and if not, report the problem to the Office of U.S. Secretary of Health and Human Services (HHS).

5. DHMH and its Covered Components shall report all breaches of a business associate agreement or MOU involving a violation of privacy practices to the DHMH Privacy Officer within one State business day of notice of the violation or potential violation.

F. STATE PRE-EMPTION.

1. HIPAA preempts State law if:

   a. The HIPAA provision is more stringent than the State law, and

   b. DHMH or its Covered Component could not possibly comply with both a provision of State law and HIPAA; or

   c. The State law creates an obstacle to the accomplishment of the goals and purposes of HIPAA.

2. Per a DHMH or a Covered Component's request, the OAG will provide guidance on the current analysis of pre-emption issues.

3. DHMH or a Covered Components may consult the OAG to determine whether a provision of State law is more stringent than HIPAA.

G. COMPLAINTS TO DHMH.

1. DHMH and its Covered Components shall provide a process for individuals to make complaints concerning requirements of this policy and the related privacy mandates, or the Department's compliance with these mandates.

2. The process for filing a complaint will be explained to patients and to clients in the Department's and Covered Components' NPPs.

3. DHMH and its Covered Components' workforce members must file complaints accordance with DHMH Policy 01.03.01 DHMH Corporate Compliance Program.

4. The DHMH Privacy Officer shall arrange to document all complaints received and their disposition.

H. CHANGES IN THE LAW.

1. DHMH, and Covered Components where necessary, will update or revise its policies and procedures on PHI as necessary to comply with changes in Federal or State laws or regulations dealing with privacy of PHI.

2. If a change in law materially affects the DHMH NPP, the DHMH Privacy Officer will promptly document, update, and distribute a revised NPP to comply with the applicable law.

3. DHMH will not implement a change to its privacy policies or procedures before distributing a revised NPP if applicable.

I. MITIGATION.

1. DHMH and a Covered Component shall attempt to mitigate, to the extent practical, any harmful effects known to DHMH or the Covered Component of a use or disclosure of PHI by an employee or business associate that is in violation of HIPAA or DHMH, or the Covered Component's policies and procedures.

2. If DHMH or a Covered Component's PHI has been misused by a business associate, DHMH or a Covered Component shall:

a. Investigate the misuse of the PHI.

b. Determine if the misuse was serious.

c. Determine if the misuse is repeated.

d. Counsel the business associate on the misuse of PHI.

e. Monitor the business associate's performance to ensure that the wrongful behavior has been remedied.

f. Reserve the right to terminate a business associate agreement in the event the misuse of PHI continues despite counseling.

g. Maintain a record, either written or electronically, of any communications, actions, or activities conducted to mitigate the harm.

J. APPLICATION OF SANCTIONS BY DHMH.

1. DHMH and its Covered Components will apply sanctions to members of their workforce that fail to comply with the policies and procedures on privacy of PHI, consistent with applicable personnel laws, State Personnel System law and the procedures of the DHMH Office of Human Resources (OHR).

2. DHMH and its Covered Components shall consult with the (OAG) prior to applying any sanctions, including consistency with the State Personnel System law.

3. The DHMH Privacy Officer, in coordination with other offices, shall develop an appropriate method for acquiring and maintaining reports on sanctions that is compatible with other applicable Federal or State laws or contractual agreements which limit access to confidential personnel information.

K. SAFEGUARDS.

DHMH and its Covered Components shall ensure that appropriate administrative, technical, and physical safeguards are in place to protect the privacy of PHI.

1. DHMH and its Covered Components will take reasonable steps to safeguard PHI from any intentional or unintentional use or disclosure that is in violation of privacy protection standards pursuant to DHMH or its Covered Components' policies and procedures.

2. Safeguards may include, but are not limited to, the following:

a. Shredding of documents that contain PHI prior to disposal from offices.

b. Implementing records management processes for protecting health information consistent with privacy policies. (See DHMH 01.03.05 Individual Rights Policy).

c. Requiring locking doors to medical records departments, or locking cabinets where medical records are kept, and limiting access to the keys or combinations to such locks.

d. Placing facsimile machines and other office equipment that are used for processing, sending or receiving PHI in areas with limited access, and limiting use of such equipment to those whose job functions include processing PHI.

e. Encrypting PHI and other non-public information when sent electronically to others outside of Maryland.gov or that is stored on Google Drive.

f. Encrypting mobile devices, such as laptops and flash drives that contain PHI.

g. Implementing policies to prohibit the sharing of personal log-in credentials.

3. DHMH and its Covered Components shall function under standard operating procedures that safeguard PHI.

4. DHMH and its Covered Components are to maintain awareness and adherence to other applicable DHMH policies and guidance related to technical and physical security, confidentiality, and privacy, including the following:

a. E-mail Security Tips

b. Data Eradication Procedures

c. DHMH Password Standards

d. Laptop, Portable, and Off-site Data Processing Equipment Protocol

e. DHMH 02.01.06, Information Assurance Policy and related Procedural Guidelines

f. DHMH 02.01.01, Employee Information Technology Security Policy: Protecting Non-public Information

g. DHMH 01.03.07, HIPAA Breach Response Policy

h. DHMH 01.03.08, Computerized Personal Information Breach Response Policy

i. DHMH 01.03.05, Individual Rights Policy

j. State of Maryland Information Security Policy

L. WHISTLEBLOWERS.

1. DHMH and its Covered Components shall investigate allegations of misconduct of a member of their workforce or a business associate when PHI is released.

2. DHMH and its Covered Components' workforce members who in good faith report a possible violation to appropriate officials may not be subject to retaliation.

M. DOCUMENTATION.

1. DHMH and its Covered Components shall maintain records, either written or electronic, of its privacy policies and procedures, communications required by privacy regulations, or any other actions, activities, or designations required by the privacy regulations.

2. Such documentation required under this policy will be retained by DHMH and its Covered Components for a period of at least 6 years.

IV. REFERENCES

- COMAR 14.18.02, Records Retention and Disposal Schedules
  http://www.dsd.state.md.us/comar/SubtitleSearch.aspx?search=14.18.02.*
- DHMH Information Security Website
  http://indhmh/secpolcy/html/infosys.htm.
- 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 Policy
  - DHMH 01.03.01, Corporate Compliance Program Policy
    http://dhmh.maryland.gov/policy/01.03.01%20Corporate%20Compliance%20Program%20and%20Addendum%201-12-12.pdf
  - DHMH 01.03.05, Individual Rights Policy▪▪
    http://www.dhmh.maryland.gov/docs/010305-IndividualRightsPolicy.pdf
  - DHMH 01.03.07, HIPAA Breach Response Policy
    http://dhmh.maryland.gov/docs/01.03.07%20HIPAA%20Breach%20Response%20Policy%207-22-14%20(1).pdf
  - DHMH 01.03.08, Computerized Personal Information Breach Response Policy.
    http://dhmh.maryland.gov/docs/01.03.08%20Computerized%20Personal%20Information%20Breach%20Response%20Policy%205-6-15.pdf
  - DHMH 01.05.06, Records Management Policy.
    http://dhmh.maryland.gov/docs/01.05.06%20DHMH%20Records%20Maagement%20Policy%205-5-15.pdf
  - DHMH 02.01.01, Information Technology Technical Security Policy, Standards & Requirements
    http://employeecentral.dhmh.maryland.gov/infosec/pdf/DHMH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf
  - DHMH 02.01.06, Information Assurance Procedural Guidelines
    http://dhmh.maryland.gov/Pages/iapguidelines.aspx
  - DHMH 01.03.09, HIPAA Training Policy
    http://www.dhmh.maryland.gov/docs/020911-HIPAA.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://marylandcode.org/ghg/
- State of Maryland Information Security Policy. http://doit.maryland.gov/publications/doitsecuritypolicy.pdf

V. APPENDIX

- DHMH Organization-HIPAA Covered Functions or Entities

APPROVED:

Van T. Mitchell, Secretary **May 23, 2016**
Effective Date

APPENDIX

DHMH 01.03.06-Appendix-DHMH HIPAA Covered Health Care Components as of January 12, 2012

DHMH Organization	HIPAA Covered Health Care Components	Designation
Chronic Hospital Facilities	Western Maryland Hospital Center	Provider
	Deer's Head Hospital Center	Provider
Community Health Administration – Local Health Department Programs	Allegany County	Provider
	Anne Arundel County	Provider
	Baltimore County	Provider
	Calvert County	Provider
	Caroline County	Provider
	Carroll County	Provider
	Cecil County	Provider
	Charles County	Provider
	Dorchester County	Provider
	Frederick County	Provider
	Garrett County	Provider
	Harford County	Provider
	Howard County	Provider
	Kent County	Provider
	Montgomery County	Provider
	Prince George's County	Provider
	Queen Anne's County	Provider
	St. Mary's County	Provider
	Somerset County	Provider
	Talbot County	Provider
	Washington County	Provider
	Wicomico County	Provider
	Worcester County	Provider
Lab Administration	All Services	Provider
Behavioral Health Administration	Thomas B. Finan Center	Provider
	RICA-Baltimore	Provider
	RICA-Rockville	Provider
	Eastern Shore Hospital Center	Provider
	Springfield Hospital Center	Provider
	Spring Grove Hospital Center	Provider
	Clifton T. Perkins Hospital Center	Provider
Prevention and Health Promotion Administration	Maryland AIDS Drug Assistance Program	Health Plan
	Md. AIDS Drug Assistance Program-Plus	Health Plan

Developmental Disabilities Administration	**Holly Center**	**Provider**
	Potomac Center	**Provider**
	Central Maryland Regional Office	**Provider**
	Eastern Shore Regional Office	**Provider**
	Southern Maryland Regional Office	**Provider**
	Western Maryland Regional Office	**Provider**
	SETT	**Provider**
Medicaid Programs	**All Programs and Functions**	**Health Plan**