State of Maryland
Department of Health & Mental Hygiene
Parris N. Glendening, Governor Georges C. Benjamin, M.D., Secretary

Deputy Secretariat for Operations - POLICY 02.01.06
Effective June 1, 2001

POLICY TO ASSURE CONFIDENTIALITY, INTEGRITY, AND AVAILABILITY OF DHMH INFORMATION

SHORT TITLE: INFORMATION ASSURANCE POLICY – IAP

I. EXECUTIVE SUMMARY

This policy provides direction for certain actions of Department employees to assure confidentiality, integrity, and availability of DHMH information assets. It clarifies the roles and responsibilities of employees to protect the interests of DHMH and consumers regarding the release of non-protected information and safeguarding of DHMH protected and proprietary information. It recognizes and defines a life cycle for information. It acknowledges existing security and confidentiality requirements and initiates new requirements. It specifies requirements for both general and specific levels of due diligence and due care to be exercised over DHMH information. Additionally, it provides for protection levels that are commensurate with an acceptable level of risk of loss or disclosure.

Based on a "need-to-know" approach, supervisors are to assign employees an appropriate access authority and grant to them corresponding system access levels. Employees are held accountable for reading and complying with the corresponding section(s) of this policy and to act accordingly based on their assigned duties and responsibilities.

Due to the size, complexity, and evolving nature of health policy, information systems, and communications technology, this document provides broad standards for the handling and security of DHMH information. To facilitate compliance with this policy a separate document entitled "Security Procedures for DHMH Information Assurance Policies and Programs," hereafter referred to as "DHMH Information Security Procedures", has been developed to provide: (1) the roles and responsibilities of specific personnel, (2) data classifications, and (3) directions for handling Department information. These procedures are issued and maintained by the DHMH Information Resources Management Administration to support this policy.

II. BACKGROUND

State Government records are public records, under the Maryland Public Information Act (PIA) (see http://www.oag.state.md.us/Forms/book.pdf). Upon request, these records are to be made available for inspection or copying unless a provision of the PIA or other law either prohibits or authorizes the custodian to refrain from such a disclosure. However, certain health and medical information may be exempt from disclosure in order to protect the privacy of individuals. Therefore, DHMH must balance its responsibility, together with its other federal and State responsibilities, to protect the privacy and confidentiality of health and medical information and transactions.

Our communications with the public needs to reinforce a sense of trust in DHMH and State government. The Department's employees may be required to work with both electronic and paper-based systems, which includes handling information, data, records, and documentation, hereafter generally referred to as information. Regardless of how information is obtained, created, or used in job performance, it must be handled with appropriate security precautions as established by this policy, or more restrictive applicable federal or State policies, procedures, regulations, or laws.

This policy seeks to both clarify the responsibilities of employees as well as to protect the interests of the Department and health consumers through the safeguarding of protected information. Any DHMH employees could be privy to information that is non-public, confidential, and/or intended only for Departmental use. Employees are cautioned that even seemingly appropriate disclosures of consumers' health and medical information may constitute an unwarranted 'invasion of privacy.'

The use of DHMH information systems by employees is explained in 02.01.01, Electronic Information Systems Policy (http://indhmh/top_poly/policies/p020101.htm). All DHMH employees are to sign and initial the appropriate section(s) of the Combined Policy Acknowledgment Form. To ensure employees' understanding and compliance with applicable provisions of this policy, the acknowledgment and signing of the form are to be done in consultation with supervisory staff who will also initial the form.

Because certain employees have duties that require them to have more extensive access, or require authority beyond that granted to the 'user' level, these employees are to read and comply with additional applicable provisions of this policy, as designated for *specific personnel* (see § III.A-Definitions) also in consultation with supervisory staff.

As a condition of access to DHMH information resources, non-DHMH employees, or other individuals who access or use DHMH information systems, will also need to sign the Combined Policy Acknowledgment Form (see Appendix). Those individuals who do not sign the Statement will no longer be given access to or use of DHMH protected or proprietary information or information systems, which may result in subsequent job reassignment.

This policy was developed with assistance from the Security and Confidentiality (SeCon) Workgroup of the DHMH Health Information Coordinating Council which reviewed and applied federal and State statutes and regulations including the Health Insurance Portability and Accountability Act (HIPAA), in addition to the "best practices" of government agencies and private industry. Given the complexity and evolving nature of information systems and communications technology, this policy is to be reviewed and revised periodically in coordination with the DHMH Health Information Coordinating Council.

III. POLICY STATEMENTS

A. DEFINITIONS

A comprehensive set of definitions for this policy is contained in *DHMH Information Security Procedures,* which may be accessed on the DHMH intranet homepage at http://indhmh/secpolcy/html/infosys.htm.

Specific personnel - For the purpose of this policy, the term specific personnel refers to the following positions, which are also described and defined in detail in the DHMH Information Security Procedures.

- **DHMH Institutional Review Board Official Custodian**
- **Custodian of Records**
- **Data Steward**
- **Designated Responsible Party**
- **Network (System) Administrator**
- **Database Administrator**
- **Data Technician**
- **Contract Monitor**
- **Contract Preparer**

B. INFORMATION SECURITY DIRECTIVES

1. **Information Is To Be Protected**. All information, in any format, which is created or used in support of DHMH business, is to be considered either owned by DHMH or in DHMH custody. This information is a valuable asset and must be protected from its point of origin through its life cycle of creation, collection, maintenance, authorized sharing, and storage, until its lawful disposal. It is to be maintained in accordance with federal and State regulations and DHMH policies in a secure and reliable manner. Such protection levels are to reasonably assure confidentiality, integrity, accuracy, and ready availability for authorized use.

2. **Information Custodians Are To Be Appointed.** Program Directors, facility CEO's, Health Officers, and other executive managers of DHMH units are responsible for the information in their custody. Unless such responsibility is to be retained by them personally, or is provided for otherwise in law or regulation, the executives are authorized to appoint an official Custodian, Data Steward, or Designated Responsible Party to manage their information. These functions are also defined in the *DHMH Information Security Procedures*.

3. **Information Is To Be Classified.** Based on legal requirements, sensitivity, retention criteria, and the type of access required by authorized users, all DHMH information will be classified by its custodians, or other authorized authority.

4. **Protection Levels Are To Be Based on Risk Assessment.** *Information assurance* is to be achieved by implementing a comprehensive set of policies and procedures that protect against accidental or malicious disclosure, modification, or destruction. The level of effort to protect information should reflect its confidentiality and its risk of loss or compromise. The risk and impact of loss and the relative value of the information is to be determined initially, and annually thereafter, by the Director or the appointed custodian of the information set, using an IRMA-accepted business impact analysis tool as found in the *DHMH Information Security Procedures*. Additionally, a comprehensive risk analysis is required to be completed in the development phase of new information systems, or when existing systems are modified between annual reviews.

5. Information Access Is To Be Granted On A "Need To Know" Basis. Access to information will be limited to authorized users who have a business need to know such information. This access and use will be further limited to appropriate job levels within legitimate job classifications. A higher level of access may be provided to persons who are designated to act in specialized support roles and who demonstrate a need to access, modify, or erase the information or to maintain the information system.

6. A Separation of Duties Is Required. No single individual will have complete control of a business process or transaction from inception to completion. Custodians are directed to assure that there is functional segregation of roles and duties performed by an employee, to limit error and the opportunity for unauthorized actions.

7. Employees and Contractors Are To Be Trained in Information Security Awareness and Ethics. Depending on job duties, all DHMH employees and contractors and agents will be provided with training in information ethics. This training will be provided prior to access to DHMH information systems, or prior to commencement of contractual services, and annually thereafter.

8. Employees Are to Be Aware of Their Obligation to Protect Information. Laws and regulations specifically require maintaining the confidentiality of certain records. DHMH employees are responsible for knowing, or determining, in consultation with their supervisor, the specific protective requirements for information in their care, and for understanding their obligations to protect these resources. Employees are to report any suspected or realized violations.

C. ROLES AND RESPONSIBILITIES

Every employee has a role and responsibilities to fulfill in *information assurance*. Employees' roles and responsibilities are described in more detail in the *DHMH Information Security Procedures*. They are necessary to direct, implement, enforce, and assess the effectiveness of security and privacy policy, planning, and administration. The success of this policy is dependent upon supportive management, appropriate role assignment, and employees' understanding of their roles and responsibilities for implementing and enforcing the policy. Every DHMH employee is assigned at least one role and its related responsibilities:

1. **Chief Information Officer (CIO)** - For the purpose of this policy, the DHMH CIO is responsible for providing guidance on all Information Technology issues. The CIO is also responsible for directing the management and administration of the DHMH information security program and initiating measures to assure and demonstrate compliance with security and privacy requirements.

2. **Information Assurance Officer (IAO)** - The IAO is directly responsible for the Department-wide coordination of all aspects of security and confidentiality, pursuant to applicable federal and State laws, regulations, and policies, and DHMH policies, procedures, and protocols. The following are the responsibilities of the IAO:

- develops and reviews system security and privacy policies and grants exceptions to them;
- provides guidance to assure the integrity of all DHMH information;
- reviews the security and confidentiality of the resources associated with the processing functions;
- reports security status of DHMH, as required;
- assures software controls are implemented;
- ensures procurement requirements of the IAP are met;
- supervises the resolving of security and privacy incidents;
- acts as Chief Privacy Officer (unless the role is otherwise assigned);
- coordinates with network security staff;
- assists in the preparation and review of IT risk assessments and contingency plans; and
- coordinates with internal and external audit staff to assure IAP requirements are included in audit reviews.

3. **Security Officer (SO)** - The DHMH SO serves as the single point of contact and as the access control agent for the daily IT security program. The following are responsibilities of the SO's:

- performs system audits, as directed;
- coordinates with DHMH Security Monitors for access controls;
- resolves authentication and authorization issues or concerns;
- participates in addressing general security issues;
- provides appropriate IT security awareness and training to all employees;
- assists in the development of DHMH systems contingency and disaster recovery plans;
- functions as the daily operational central point of contact for any type of IT security related incidents or violations;
- disseminates information concerning security alerts and potential threats to all DHMH system owners;
- notifies users of security-related policies and procedures;
- assists in preparing annual systems evaluations of major processes including incident handling and security awareness training; and,
- assists in risk management analysis to determine effectiveness in reducing security incidents.

4. **Security Monitors (SMs)** - The DHMH System Monitors serve as the central point of contact and as the authorization control agents in their designated units for the daily IT security program. The following are SM responsibilities:

- coordinates with the DHMH Security Officer in the preparation of lists of authorized users;
- makes changes to lists, and audits, as required;
- participates in addressing unit and DHMH security issues;
- participates in IT security awareness and training;
- performs as the central point of contact for unit-level IT security related incidents or violations;
- disseminates information concerning security alerts and potential threats to all DHMH system owners;
- ensures that users are aware of security-related policies and procedures; and,
- assists in the annual systems evaluation process.

5. **User** - The User is an employee or agent or contractor who has access to DHMH information. Users are responsible for consulting with supervisory staff to :

- determine the user's role and responsibilities to protect information resources in the user's control or possession
- understand and comply with all applicable DHMH and other security and privacy requirements, and
- to facilitate a better understanding of the general and specific requirements for the confidentiality of protected and/or proprietary information.

6. ***Specific Personnel*** - The positions previously listed under Section III A - Definitions -*Specific Personnel*, within the scope of their assigned duties, are instructed to implement the following provisions as necessary to protect information from inadvertent or intentional improper use or disclosure.

a. Information is to be Protected. Protection of information requires a diligent coordination of organizational and administrative requirements, physical security safeguards, and technological security measures further detailed in *DHMH Information Security Procedures*. http://indhmh/secpolcy/html/iaphic2.htm

b. Employees Are To Actively Comply with IAP Requirements. *Specific Personnel* are to act as required or directed in order to assure compliance with Federal, State, and DHMH directives. They are to report any known or suspected violations of these directives, throughout the lifecycle of the DHMH information resources in their custody.

c. Proprietary Interests In DHMH Information Are To Be Maintained. *Specific personnel* are to take appropriate steps to assure the Department's proprietary interest in information is protected through both legal and administrative means, describing and documenting the qualities and limitations of DHMH information in their custody.

d. Information Must Be Collected, Maintained, Transferred, Stored, and Disposed of As Authorized. In accordance with applicable laws and regulations, employees who have access to information must be diligent to protect consumer rights and DHMH interests. *Specific personnel* may not transmit information electronically unless permitted by approved written procedures.

e. Employees Are Authorized To Release Non-protected Information to the Public. *Specific personnel* will classify information in their custody, authorize certain employees, establish procedures to prevent unintended disclosure, facilitate and clarify the decision-making processes related to release/sharing in accordance with DHMH copyright requirements.

f. Employees Will Not Allow the Unauthorized Sharing of Protected and Proprietary Information. The sharing of DHMH protected or proprietary information is encouraged as a good business practice, however, such sharing must be as necessary, appropriate and legal, in accordance with an explicit written understanding. DHMH protected or proprietary information will not be physically or electronically removed or shared, without the explicit authorization of the official custodian of record or designee.

g. *Specific Personnel* Will Not Allow the Unauthorized Disclosure of Protected and Proprietary Information. DHMH protected or proprietary information may only be disclosed to others if necessary, appropriate, legal, and only as authorized by the official custodian of record or designee.

h. Certain *Specific Personnel* Will Monitor the Sharing of Protected or Proprietary Information - When information is shared or accessed, *Specific personnel* will establish and follow written procedures to hold all subsequently approved users to the same Department and/or other requirements and responsibilities. This includes an extension of the requirements and the continued strict adherence to all rules required by a DHMH recognized Institutional Review Board including resubmission requirements.

i. Certain Employees May Authorize Disclosure of Protected and Proprietary Information. Authorized *Specific personnel*, as defined in this policy, are permitted to disclose protected or proprietary information resources in the course of their official duties, only if the requirements of this policy or other more stringent requirements are met before such disclosure.

j. Employees Are To Notify Vendors Of The IAP And Other Applicable Requirements. - *Specific personnel* involved in the preparation and monitoring of DHMH contracts and memoranda of understanding (MOU) will ensure that vendors, agents, or other entities who provide work-for-hire, understand and comply with all applicable requirements for the protection of DHMH information resources. This will be required when such resources are shared, or when DHMH information systems are maintained, changed or developed.

k. *Specific Personnel* are Responsible for IAP Compliance. Persons designated or authorized to act in the capacity of *Specific personnel*, as defined above, are responsible for taking any and all reasonable, appropriate, and legal steps to ensure all employees comply with the terms of this policy.

D. DISCIPLINARY, CIVIL, AND CRIMINAL CONSEQUENCES

Violation of this policy may result in disciplinary action up to and including separation from State service and civil or criminal penalties. These remedies include, but are not limited to, those specified in the Annotated Code of Maryland, SG §10-626 through §10-628, HG §4-309, and Crimes and Punishments Article 27 §45A.

IV. REFERENCES

- Executive Order 01.01.1983.18- State Data Security Committee, State Agency Information Security Practices. http://209.15.49.5/01/01.01.1983.18.htm
- Annotated Code of Maryland, Article 27, Sections 45A and 146, Prevention of Software Copyright Infringement.
- Manual #95-1, Maryland Department of Budget and Fiscal Planning, June 1, 1995.
- DHMH Policy 02.01.01, Policy On The Use Of DHMH Electronic Information Systems, effective June 5, 1998. http://indhmh/top_poly/policies/p020101.htm .
- DHMH Policy 02.01.02 (formerly Policy DHMH 9170) -Policy On The Use Of And Copying Of Computer Software And The Prevention Of Computer Software Copyright Infringement, effective May 12, 1998. http://indhmh/top_poly/policies/p020102.htm.
- "Security Procedures for DHMH Information Assurance Policies and Programs," DHMH CIO, IRMA, 2000. http://indhmh/secpolcy/html/iaphic2.htm.

V. Appendices, Exhibits, & Addenda

- Combined Policy Acknowledgement Form

APPROVED:

Georges C. Benjamin

Georges C. Benjamin, M.D., Secretary

DATE: JUN 0 1 2001