
# Allegany County Health Department

12501 Willowbrook Road SE, Cumberland, MD 21502

## Information Security Policy

### Introduction

Allegany County Health Department has adopted this Security Policy to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Department Health and Human Services ("DHHS") security and privacy regulations, the Joint Commission on Accreditation of Healthcare Organizations ("JCAHO") accreditation standards, Maryland Department of Health - Information Technology Security Policy Standards & Requirements ("MDH"), as well as our duty to protect the confidentiality and integrity of confidential medical information as required by law, professional ethics, and accreditation requirements. All personnel of Allegany County Health Department must comply with this policy. Familiarity with this policy and demonstrated competence in the requirements of the policy are an important part of every employee's responsibilities.

### Assumptions

This Security Policy is based on the following assumptions:

- All personnel of Allegany County Health Department must preserve the integrity and the confidentiality of medical and other sensitive information pertaining to our patients.
- The purpose of this Security Policy is to ensure that Allegany County Health Department and its officers, employees, and agents have the necessary medical and other information to provide the highest quality medical care possible while protecting the confidentiality of that information to the highest degree possible so that patients do not fear to provide information to Allegany County Health Department and its officers, employees, and agents for purposes of treatment.

### Policy

To that end, Allegany County Health Department and its officers, employees, and agents will—

- Recognize that medical information collected about patients must be accurate, timely, complete, and available when needed. Consequently, Allegany County Health Department and its officers, employees, and agents will—
    - Use their best efforts to ensure the accuracy, timeliness, and completeness of data and to ensure that authorized personnel can access data when needed.

- Not alter or destroy an entry in a record, but rather designate it as an error while leaving the original entry intact and create and maintain a new entry showing the correct data.
- Implement reasonable, cost-effective measures to protect the integrity of all data maintained about patients.
- Act as responsible information stewards and treat **all** individual medical record data and related financial, demographic, and lifestyle information as sensitive and confidential. See MDH Policy 02.01.01 under "B. Labeling" for more information.

**Data Backup Plan**.

- Timely access to health information is crucial to providing high quality health care.
- A number of risks to health information exist, such as power spikes or outages, natural disaster, viruses, hackers, and improper acts by employees and others.
- Reliable backup of data is crucial to Allegany County Health Department's operations.
- The Information Technology Department is responsible for performing daily backups on Allegany County Health Department's network, including shared drives containing application data, patient information, financial data, and crucial system information.

**Email**

- The email system is part of Allegany County Health Department's business equipment.
- Email is not guaranteed to be secure. Communications can be forwarded, intercepted, printed, and stored by others.

  Email containing information pertaining to a patient's diagnosis and/or treatment constitutes a part of the patient's medical records.
- All email may be discoverable in litigation regardless of whether it is in a patient's medical record.
- Allegany County Health Department must adhere to the State of Maryland's Department of Information Technology Policy which states that any State Employee (defined as any employee who receives a paycheck from the Comptroller's Office) using email should be using a Maryland.gov email account. The Department of Health and Mental Hygiene, under this policy, has identified Maryland.gov Gmail as the standard for email communications. No other email product or domain name is approved for use by MDH employees. For more information see: http://employeecentral.mdh.maryland.gov/infosec/pdf/MDH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf Security Policy SAR-14.
- All email regardless of content will include a confidentiality statement developed by Maryland's Department of Information Technology (DoIT). It reads as follows:

"CONFIDENTIALITY NOTICE: This message and the accompanying documents are intended only for the use of the individual or entity to which they are addressed and may contain information that is privileged, confidential, or exempt from disclosure under applicable law. If the reader of this email is not the intended recipient, you are hereby notified that you are strictly prohibited from reading, disseminating, distributing, or copying this communication. If you have received this email in error, please notify the sender immediately and destroy the original transmission".

**Secure Access to Equipment and Media**

- See MDH Policy 02.01.01 section "E. Secure Access to Equipment and Media and "F. Password Protection.
- Any computer workstation in the covered entity can access confidential patient information if the user has the proper authorization defined on a need to know basis.
- All computer users will monitor the computer's operating environment and report potential threats to the computer and to the integrity and confidentiality of data contained in the computer system. For example, if air conditioning fails, so that the temperature around the computer may exceed a safe level, the user must immediately notify [the director of information systems] [other] and maintenance.
- No personnel may upload, download or install any unauthorized software or data. The Information Technology Department must approve any software or data that an employee wishes to upload. This rule is necessary to protect against computer viruses from being transmitted into the covered entity's system. See http://employeecentral.dhmh.maryland.gov/infosec/pdf/MDH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf SAR-2 and MDH Policy 02.01.02.

**Portable Computer and Media Controls**

- Allegany County Health Department has issued the following computer equipment to you for the uses for which you have been specifically trained. The hardware, software, all related components, and data are the property of Allegany County Health Department and must be safeguarded and be returned upon request and upon termination of your employment.
- Data, media, and computer assets are the physical property of Allegany County Health Department, wherever located.
- Portable computers pose a significant security risk because they may contain confidential patient information and, being portable, are more at risk for loss, theft, or other unauthorized access than the Allegany County Health Department's less easily movable computers.
- Data, media, computers, and other information assets may not be removed from Allegany County Health Department without the written consent of the appropriate department director. Such consent may consist of a blanket authorization for certain personnel, such as employed physicians, to remove and use such assets offsite. Allegany County Health Department personnel who remove data or information assets from the facility must be responsible for safeguarding such assets. Department directors will provide the Allegany County Health Department security officer a copy of all such blanket consents for off-site use for his or her review. For more information see http://employeecentral.dhmh.maryland.gov/infosec/pdf/MDH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf SAR-9 and MDH Policy 02.01.01 Section D.

**USB and Flash Drive Security**

**All USB and Flash Drives must be encrypted if they are to contain Non-Public Health Information. They must also be kept in a log of date, department and employee name using device. There will be periodic inventory checks of items listed on the log.**

**Internet Security**

- Allegany County Health Department can improve the efficiency and benefit from access to and use of the internet and its resources, services, and interconnectivity
- Improper use of the internet puts Allegany County Health Department and its employees at risk.
- The content of all web pages under Allegany County Health Department's jurisdiction must comply with local, state, and federal laws and Allegany County Health Department's policies and procedures.
- A policy for the proper use of the internet is necessary to maintain the accuracy, security, and confidentiality of individually identifiable health information and other sensitive data.
- All electronic communications created, received, or stored on the State's electronic communications systems are the sole property of the State and not the author, recipient, or user.
- Except where security is explicitly provided to meet federal or state laws or regulations for data security, no user should have any expectation of privacy in any message, file, image or data created, sent, retrieved or received by use of the MDH equipment and/or access e.g. financial information, credit card or account information or transactions.
- Intentional misuse includes, but is not limited to, receiving, displaying, storing, or transmitting threatening or sexually-explicit images, messages, or cartoons as well as epithets or slurs based upon race, ethnic or national origin, gender, religious affiliation, disability, or sexual orientation and harassing, offensive, discriminatory, or defamatory communications or images. It also includes attempting to access a secured system or database, whether private or public, without permission.
- Certain activities are prohibited at all times when using State/MDH information equipment, systems, or Internet or electronic communications for personal use. These include, but are not limited to creating, copying, accessing, attempting to access, installing, uploading, downloading, transmitting, printing, sharing, or storing:
    - lengthy private messages,
    - religious/faith-based or politically-related messages,
    - sexually explicit information or content;
    - fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
    - unauthorized computer software, programs, or executable files contrary to software copyright and use policy
    - music and video downloaded files or streaming transmissions including news and entertainment, and Engaging in Social Media networks outside of authorized business uses.
    - Access or attempt to access an account or information to which you are **not authorized**
- The Internet Policies listed are adopted in part from http://employeecentral.dhmh.maryland.gov/infosec/pdf/MDH-INFO-TECH-SEC-2013-ver-3.0-3-19-2013.pdf SAR-14 Appropriate Internet and other Electronic Communications and Use page 104.

**Telemedicine Security**

*Work in process - not currently available*

**Enforcement**

All officers, agents, and employees of Allegany County Health Department **must** adhere to this policy, and all supervisors are responsible for enforcing this policy. Allegany County Health Department will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with Allegany County Health Department's medical information sanction policy and personnel rules and regulations.

| | |
|---|---|
| _____ | _____ |
| Signature | Date |
| _____ | _____ |
| Title | Printed Name |
| _____ | _____ |
| Witness | Printed Name of Witness |