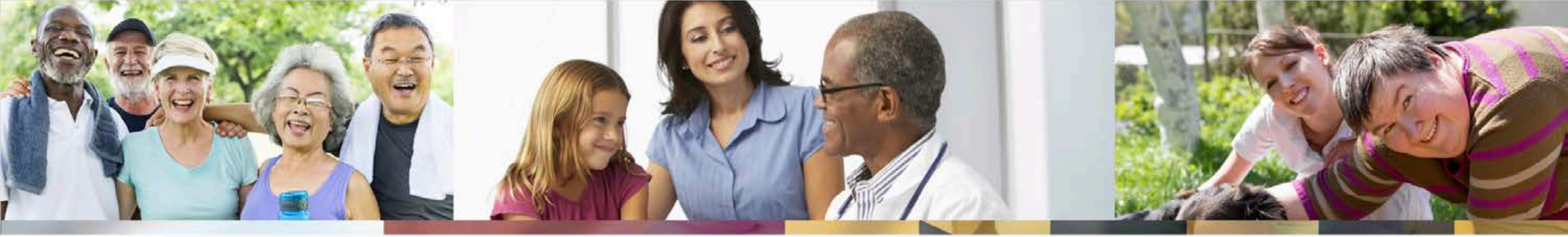
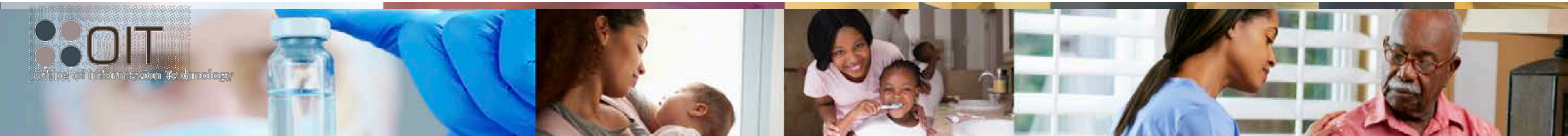


Maryland
DEPARTMENT OF HEALTH

# MDH Electronic Information Systems An Introduction to Required IT Security and Privacy Policies

Office of Information Technology 2018



# Key IT Security Points

- What is your role?
- Do you work with Protected Health Information (PHI)?
- Are you a Custodian of Records, DBA, or a Network/IT Services employee?
- Privacy and Security policies govern your actions
- When in doubt, ask your supervisor

# Orientation Required by Policy

- Employees:
  - Are required to read, sign and adhere to the IT and Data Privacy policies
  - Must sign the Combined Acknowledgement Form
  - Must comply with requirements
- When in doubt, ask your supervisor

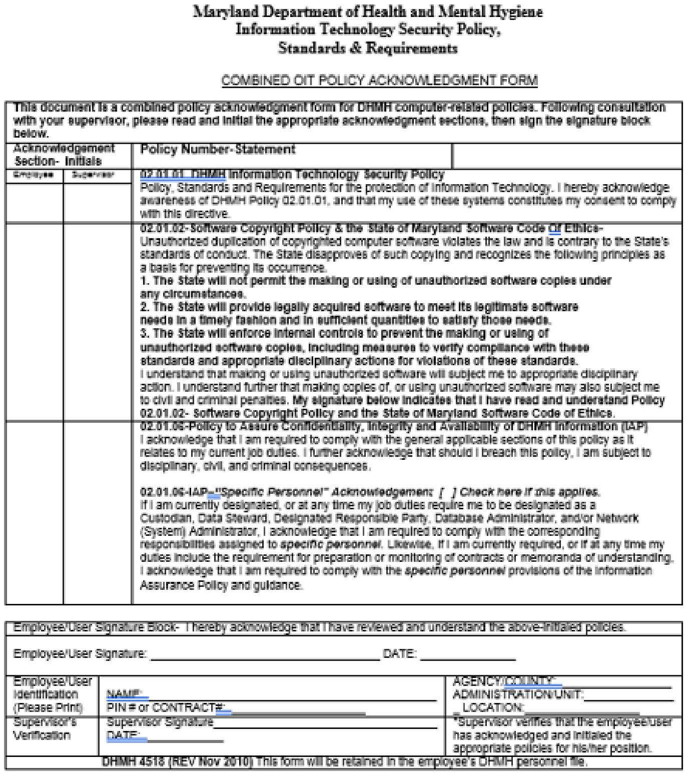
# MDH Office of Information Technology (OIT)

- OIT manages MDH IT enterprise services for more than 50 sites and direct user support for select MDH business units.  Other business units maintain their own local IT user support staffs.
- Some of the services offered by MDH OIT include:
  - Enterprise network services (MDH Wide Area Network, Internet and SwGI services)
  - Enterprise network security
  - HelpDesk, hardware and software end-user support (for some MDH business units)
  - Information Technology Asset Management services for software licensing
  - MDH liaison to Maryland State Department of Information Technology
  - Security requirements analysis for new system development and upgrades
  - Information Security training for users, developers and managers (online and in-person)
  - Assistance to access vendor-based IT systems security consulting services

# MDH Electronic Resource Use Principles

- Adherence to software licensing end-user agreements
- Protection of non-public data
- Hardware, software and network are state property made available to employees to conduct state business
- Use may be monitored by MDH and MD DoIT
- Use records and electronic correspondence may be public record
- No right or expectation of privacy while using state resources
- Use of personal devices must be approved by your manager
- Personnel actions and legal ramifications for violation of principles, policies and laws

# Appropriate Use of Electronic Resources



**Maryland Department of Health and Mental Hygiene**
**Information Technology Security Policy,**
**Standards & Requirements**

COMBINED OIT POLICY ACKNOWLEDGMENT FORM

**This document is a combined policy acknowledgment form for DHMH computer-related policies. Following consultation with your supervisor, please read and initial the appropriate acknowledgment sections, then sign the signature block below.**

| **Acknowledgement Section- Initials** | | **Policy Number-Statement** |
|---|---|---|
| Employee | Supervisor | **02.01.01 DHMH Information Technology Security Policy**<br>Policy, Standards and Requirements for the protection of Information Technology. I hereby acknowledge awareness of DHMH Policy 02.01.01, and that my use of these systems constitutes my consent to comply with this directive. |
| | | **02.01.02-Software Copyright Policy & the State of Maryland Software Code Of Ethics-**<br>Unauthorized duplication of copyrighted computer software violates the law and is contrary to the State's standards of conduct. The State disapproves of such copying and recognizes the following principles as a basis for preventing its occurrence.<br>**1. The State will not permit the making or using of unauthorized software copies under any circumstances.**<br>**2. The State will provide legally acquired software to meet its legitimate software needs in a timely fashion and in sufficient quantities to satisfy those needs.**<br>**3. The State will enforce internal controls to prevent the making or using of unauthorized software copies, including measures to verify compliance with these standards and appropriate disciplinary actions for violations of these standards.**<br>I understand that making or using unauthorized software will subject me to appropriate disciplinary action. I understand further that making copies of, or using unauthorized software may also subject me to civil and criminal penalties. **My signature below indicates that I have read and understand Policy 02.01.02- Software Copyright Policy and the State of Maryland Software Code of Ethics.** |
| | | **02.01.06-Policy to Assure Confidentiality, Integrity and Availability of DHMH Information (IAP)**<br>I acknowledge that I am required to comply with the general applicable sections of this policy as it relates to my current job duties. I further acknowledge that should I breach this policy, I am subject to disciplinary, civil, and criminal consequences.<br><br>**02.01.06-IAP–*"Specific Personnel" Acknowledgement: [ ] Check here if this applies.***<br>If I am currently designated, or at any time my job duties require me to be designated as a Custodian, Data Steward, Designated Responsible Party, Database Administrator, and/or Network (System) Administrator, I acknowledge that I am required to comply with the corresponding responsibilities assigned to *specific personnel*. Likewise, if I am currently required, or if at any time my duties include the requirement for preparation or monitoring of contracts or memoranda of understanding, I acknowledge that I am required to comply with the *specific personnel* provisions of the Information Assurance Policy and guidance. |

Employee/User Signature Block- I hereby acknowledge that I have reviewed and understand the above-initialed policies.

Employee/User Signature: ______________________________ DATE: ____________

| | | |
|---|---|---|
| Employee/User Identification (Please Print) | NAME: ______________________________<br>PIN # or CONTRACT#: ____________________ | AGENCY/COUNTY: ______________<br>ADMINISTRATION/UNIT: ____________<br>LOCATION: ______________ |
| Supervisor's Verification | Supervisor Signature ______________________<br>DATE: __________ | *Supervisor verifies that the employee/user has acknowledged and initialed the appropriate policies for his/her position. |

**DHMH 4518 (REV Nov 2010) This form will be retained in the employee's DHMH personnel file.**

- Important Policy Topics
  - 02.01.01 Information Technology Security Policy
  - 02.01.02 Software Copyright Policy & Code of Ethics
  - 02.01.06 Assure Confidentiality, Integrity and Availability of MDF Information (IAP)

***Review and signature required every year.***

OIT
Office of Information Technology

Maryland
DEPARTMENT OF HEALTH

# Policies and Required Acknowledgement Form

- Agency Information Technology Technical Security Policy, Standards and Requirements
- Information Assurance Policy (IAP) 02.01.06
- Policy for Prevention of Software Copyright Infringement

# What is Software Copyright Infringement?

- It’s the making and using of unauthorized copies of computer software
- Copying software is illegal!
- Federal copyright laws protect companies from users “stealing” their products
- Law is straight forward…illegal to copy software for any reason other than as a backup, unless expressly permitted by the copyright holder
- Purchasing doesn’t give you ownership…only the right to use according to the licensing agreement
- Policy written, MDH Policy 02.01.02

# General Rules!

- DO NOT COPY SOFTWARE, comply with the license
- DO NOT BRING IN YOUR OWN SOFTWARE
- DO NOT COPY MDH SOFTWARE for use at home
- All unauthorized software found on your pc will be removed immediately and you will be subject to disciplinary action
- Games are not allowed on any MDH pc
- No personal screen savers or backgrounds, use only those supplied by Windows

# Reminders

- Your computer, the software on it, and the network it's attached to are all STATE PROPERTY
- Supplied to you to do your job
- Keep in mind that any action you take with this state property can be and is monitored
- If the contents of these are found to be in violation of DHMH policy you may be subject to disciplinary actions
- You are ultimately responsible for what's on your computer

# Maryland.gov

- Google Apps for Government used by State of Maryland executive branch agencies
- Gmail, Google Drive, Google Docs, Sheets and Slides
- Email between Maryland.gov accounts is considered secure
- Email sent to any user outside of Maryland.gov system is not secure
- Email sent outside of Maryland.gov system containing Personally Identifiable Information (PII), Protected Health Information (PHI) or any non-public data must be encrypted using the State approved encryption solution (Virtru)
- Password protection of email attachments provides additional level of security

# Virtru Email Encryption

- Use for sending and/or viewing encrypted messages from within your Maryland.gov account
- Runs as an extension within Chrome or Firefox web browser
- Available for mobile devices
- MDH users must be approved and provisioned for Virtru; not by default
- If approved for your use, supervisor or manager must submit request on your behalf to your local IT support staff or contact the MDH OIT Service Desk directly (if your unit is directly supported by OIT)
- Reading and replying to received, encrypted emails is possible even without being provisioned as a Virtru user

# Infosec IQ - Security Awareness Training

- State of Maryland security awareness training for state employees
- Monthly online security lessons
- Email notice alerts users to new lesson
- If you do not receive email alerts for lessons, notify your local IT support staff to verify that you are enrolled

# MDH and OIT Websites

- MDH Employee Information
  - http://health.maryland.gov/Pages/empcentral.aspx
  - Contains information, policies and forms

- MDH Self Service Center
  - https://selfservice.health.maryland.gov
  - Users can unlock and/or change their own network passwords and enter work contact information that will be visible in the Maryland.gov Google directory

- OIT Service Desk
  - Web: http://helpdesk.health.maryland.gov (access from within MDH network only)
  - Phone: 410.767.6534
  - Email: mdh.oithelpdesk@maryland.gov

# Please Remember…

- Always follow applicable policies, procedures and laws!
- Always protect MDH/State of Maryland data; when in doubt err on the side of caution!
- Always protect MDH/State of Maryland hardware and software resources!
- Report any suspected or confirmed security breach immediately!
- Ask your supervisor or local IT support any questions about the proper, permissible and/or secure use of MDH/State resources!