



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 1 of 10
APPROVED BY: Director	SUPERSEDES 08/01/99	ORIGINAL ISSUE DATE 08/01/99	DISTRIBUTION LEVEL(S) 2

PURPOSE

- 1.1 This policy governs the use of Department of Mental Health (DMH) information technology resources. It includes rules in compliance with the **Health Insurance Portability and Accountability Act (HPAA) Standards for Privacy of Individually Identifiable Health Information**. (45 CFR Parts 160 and 164)
- 1.2 This policy communicates to all DMH employees, volunteers, contractors and consultants their responsibility for acceptable use of DMH information technology resources.
- 1.3 The term "user" as used throughout this policy/procedure document is used broadly and refers to paid employees, students, volunteers, interns, consultants, contractors and any other persons who represent the Department in the course of their work duties.
- 1.4 By logging on to the computer system, the user acknowledges that he/she understands and accepts the terms and conditions of this policy.

POLICY

- 2.1 The scope of this policy includes all aspects of the networked computing environment in DMH, whether or not the equipment is connected to the Departmental network (hereafter referred to as "DMH Network"). This includes all desktop and notebook computers as well as other information devices such as PDA's and wireless networks.
- 2.2 The DMH Network includes all servers and workstations connected to it, via direct or remote connection. By extension and for the purpose of this policy, it also includes portions of LANet and other County Information systems.
- 2.3 Where it comes into conflict with other existing departmental policies in the area of computing, this document shall take precedence (unless the other policies contain higher levels of security and control requirement, in which case the higher-level requirements supersede), until such time when the conflicting policies are reconciled.
- 2.4 The DMH Chief Information Office, Human Resources Bureau, Administrative Support Bureau, Contract Administration and managers of all units shall carry out the enforcement of this policy where appropriate.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 2 of 10
---	------------------------------	--	-------------------------

- 2.5 Failure to comply with this policy, in whole or in part, if grounds for disciplinary actions, up to and including discharge.

ADMINISTRATIVE CONTROL

- 3.1 The CIO Bureau's Information Technology Security Officer (ITSO) is the designated person with functional responsibilities for DMH Network security and control.
- 3.2 The ITSO is responsible to the DMH Chief Information Officer.
- 3.3 Training in areas of computing and security policies shall be provided to all users in appropriate forms (e.g., training sessions, manuals and other documents).
- 3.4 This policy shall be added to the list of policies each used must review and to be so certified on the Department's Annual Policy Certification form.
- 3.5 Certain projects/programs within DMH, because of their sensitive nature, might require a higher level of security than this document specifies. Users may be required to sign other documents when performing tasks that demand higher levels of security.
- 3.6 All managers are responsible for enforcing this policy in their respective units. Managers are also responsible to review the security compliance in their respective units at least quarterly.

DATA SECURITY

4.1 DATA CLASSIFICATION

- 4.1.1 Protected Health Information (PHI) Protected Health Information (PHI) is defined as any information, alone or in combination that allows a mental health client to be uniquely identified. PHI is accessible only to specifically authorized users.
- 4.1.2 Internal Data Internal data is confidential information that does not contain PHI. Only authorized DMH and contract agency users may access internal data.
- 4.1.3 Public Data Public Data is information that can be accessed by the general public.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 3 of 10
---	------------------------------	--	-------------------------

4.2.1 Network Storage

- 4.2.1.1 All users of networked workstations shall store PHI data in network folders that the CIO Bureau designates. This may include the user's electronic personal home folder.
- 4.2.1.2 The network staff shall backup the network servers and data residing on the designated network directory daily.

4.2.2 Local Storage

- 4.2.2.1 PHI shall not be stored locally (i.e., the hard drive of a desktop or notebook computer). Printing of hard copy of PHI requires approval of the user's manager. The hard copy shall be securely stored.
- 4.2.2.2 PHI data shall not be stored on removable devices (e.g., diskette, ZIP or JAZ cartridges, CDROM).
- 4.2.2.3 In the instance where PHI must be stored on notebook computers while not connected to the DMH Network, the hard drive on such computers shall be encrypted.

PHYSICAL SECURITY

5.1 SERVER

- 5.1.1 All server equipment shall be located in a secure area, inside a secured County building. Access to this area shall be controlled.
- 5.1.2 Any unauthorized access to the server area shall be reported to the ITSO>
- 5.1.3 Transport of any equipment in or out of the server area required prior approval of the CIO Bureau's Network Manager.

5.2 OTHER NETWORK EQUIPMENT

- 5.2.1 All routers, switches and storage devices shall be located in a secured area, or in locked cabinets, inside a secured County building. Only authorized personnel may have access to these areas/cabinets.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 4 of 10
---	------------------------------	--	-------------------------

5.3 WORKSTATIONS

- 5.3.1 Workstations are defined as all desktop and notebook computers and other data devices, whether connected to the DMH Network or not.
- 5.3.2 All workstations and related components (e.g., monitor, printer, scanner, external storage devices, etc.) shall be secured.
- 5.3.3 Computer equipment casing shall not be opened; staff from the DMH CIO Bureau must perform hardware repairs and upgrades.
- 5.3.4 Personal equipment (including computers and peripherals) are not permitted on the DMH Network.

LOGICAL SECURITY

6.1 NETWORK SECURITY

6.1.1 Network Access

- 6.1.1.1 Network Access Authorization Access to network resources must be specifically requested and granted based on the user's business need.
- 6.1.1.2 Procedure for Requesting Network Access Persons wishing network access must make their request by submitting a *Network Access Request Form* (Attachment I). A manager at the level of Program Head or Division Chief must sign the form.

6.1.2 User Passwords

- 6.1.2.1 Network Password A user's network password allows the user to access predefined network resources such as the user's specific data director on the server. In addition to ensuring authorized access, the use of a network password creates a method for audit. Each user is responsible for any activity carried out under his/her credential (User ID and password). To ensure accountability, individual users shall not share their network passwords with anyone (including the user's supervisor).
- 6.1.3 Other Passwords Applications, both commercial and those developed in-house, might provide password protection to specific resources or data. Users shall treat such passwords the same as the Network Password.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 5 of 10
---	------------------------------	--	-------------------------

- 6.1.4 Account Policy The DMH Network account policy is implemented via the Microsoft Windows 2000 operating system. It is defined as follows:
- 6.1.4.1 Maximum Password Age: 30 days
 - 6.1.4.2 Minimum Password Age: 1 day
 - 6.1.4.3 User ID: User's first initial and full last name (and, when necessary, middle initial). Official name on record with Human Resources shall be used to determine the User ID.
 - 6.1.4.4 Minimum Password Length: 8 characters
 - 6.1.4.5 Complexity required (must meet three of the following four conditions: uppercase letter, lowercase letter, number, punctuation mark).
 - 6.1.4.6 System remembers last six (6) passwords.
 - 6.1.4.7 Account lockout after three (3) bad attempts.
 - 6.1.4.8 After the lockout, user must contact the Help Desk to have it reset.
 - 6.1.4.9 Connection will expire after logon house expire. Logon hours to be based on need.
- 6.1.5 Remote Access Remote access to any DMH information system resources must be via CIO approved channels.
- 6.1.6 Control and Change Managers shall use the *Network Access Request Form* for addition of users, deletion of users, transfer of users, changing users' level of access and requesting data folder creation/access.

E-MAIL USAGE

7.1 Authorization

- 7.1.1 E-mail services are provided to all authorized DMH staff. Authorization for a person to have an e-mail account is granted along with the user's network access.
- 7.1.2 E-mail services are provided for County-related business needs only.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 6 of 10
---	-----------------------------	--------------------------------------	------------------------

- 7.1.3 All users are responsible for the regular maintenance of their e-mail account, which includes purging and archiving e-mail messages to ensure the mailbox has enough space to receive messages.
- 7.2 E-mail messages and their attachments are the property of the Department and not private communications, whether created or received, and may be subject to review by the Department at any time.
- 7.3 User may use e-mail to communicate with users in other entities so long as the communication meets professional standards of conduct and when such communication is related to legitimate business activities.
- 7.4 All users are responsible to report observed inappropriate use of e-mail (as defined in this policy).
- 7.5 E-mail communication may not contain any Protected Health Information (PHI) as defined in Section 4.1.1 of this policy.
- 7.6 Upon request of the DMH Chief Information Officer or Chief Deputy Director, DMH may access any user's electronic mail.
- 7.6.1 The above notwithstanding, the Department will **not** routinely monitor individual user's e-mail and will take reasonable precautions to protect the privacy of e-mail. Accordingly, supervisory and management staff may access an authorized user's e-mail when DMH operations require it (for example, when the employee is on vacation or otherwise absent from work).
- 7.6.2 Technical staff from the CIO Bureau may access a user's e-mail to diagnose and resolve technical problems involving system hardware, software or communications.
- 7.6.3 Except as noted above, a staff member is prohibited from accessing another user's e-mail without his/her permission.
- 7.6.4 E-mail messages may be retrieved by the Department (including messages deleted by users). Such messages may be used in disciplinary actions. The contents of e-mail will not be accessed or disclosed other than for investigative or security purposes, or as required by law.
- 7.7 Employees **may not** use e-mail for transmission of the following information:
- 7.7.1 Discrimination on the basis of race, creed, color, gender, religion, disability or sexual preference.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 7 of 10
---	------------------------------	--	-------------------------

- 7.7.2 Sexual or other forms of harassment or threats. This includes the display or transmission of sexually explicit images and text as well as the use of racial epithets or ethnic slurs.
- 7.7.3 Copyright infringement.
- 7.7.4 Personal political or religious beliefs.
- 7.7.5 Person business interests, including any activities such as sales, consulting for pay, moonlighting, etc.
- 7.7.6 Anonymous e-mail, or e-mail which impersonates or claims to be another individual.
- 7.7.7 Chain letters.
- 7.7.8 Spamming (e-mail to large numbers of people that contain unwanted solicitations or information).
- 7.7.9 Any messages or attachments that can adversely affect network performance (because of large size, etc.). Often it is better to distribute such information via the DMH Intranet or a network folder. Users who are uncertain about whether particular information should be distributed by e-mail should contact the Help Desk (213-351-2937).
- 7.7.10 Obscene language.
- 7.7.11 Virus alert. Users who suspect an e-mail contains a virus should contact the Help Desk (213-351-2937). The only individuals who are authorized to broadcast warnings about viruses to the rest of the Department are Executive Staff or Network staff.
- 7.7.12 Any other information that would jeopardize the legitimate interests of the Department.
- 7.7.13 Any unlawful or malicious activity.
- 7.8 To access e-mail, a user shall supply his/her network credential (User ID and password) either as part of the logon process to the DMH network or to OWA (Outlook Web Access).
- 7.9 In order to access DMH e-mail outside of the Los Angeles County network, a user needs a SecureID card.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 8 of 10
---	------------------------------	--	-------------------------

- 7.10 The content and maintenance of a user's electronic mailbox are the user's responsibility. The content and maintenance of a user's disk storage area are the user's responsibility. All users must regularly purge or archive outdated messages. All users must make sure their mailboxes have space to receive messages.
- 7.11 Directories of employee e-mail addresses shall not be made available for public access.
- 7.12 DMH may deem certain e-mail messages and/or their attachments business records. Such messages and attachments shall be retained as required by the Department's record retention policies.
- 7.12.1 Users shall retain all such messages and attachments, either as paper records or electronic file copies, in an existing filing system **outside the e-mail system** for as long as operational, legal, audit, research or other requirements dictate.
- 7.12.2 Users shall dispose of records in the e-mail system only after they have been filed in a record keeping system.
- 7.13 Protection Against Computer Viruses
- 7.13.1 Users shall not open e-mail messages, and particularly any attachment inside messages, if they suspect a virus might be present. Contact the Help Desk (213-351-2937) for directions.
- 7.13.2 CIO Bureau staff will make every attempt to notify all users of any viruses or worms that have infected e-mail messages. Upon such notification, all users shall completely delete the messages identified in the notification. In Microsoft Outlook, deleting completely requires deleting them from the Deleted Items folder as well as from the Inbox.
- 7.13.3 If you suspect an e-mail contains a virus, do not attempt to send out an alert. Instead, contact the Help Desk (213-351-2937). The only individuals who are to broadcast warnings about viruses to the rest of the Department are Executive Staff or Network staff.
- 7.14 Investigation of Suspected or Demonstrated Inappropriate E-Mail Usage
- 7.14.1 In appropriate e-mail usage by a user reported to (1) the Program Head or Manager at that departmental facility or division or, (2) a District Chief or Deputy Director shall be investigated promptly. The District Chief, Division Chief or Deputy Director shall first contact the CIO Data Security Unit. Together, they may take either or both of the following actions as appropriate:



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 9 of 10
---	------------------------------	--	-------------------------

- 7.14.1.1 Ask the employee how this e-mail message is related to Department business.
- 7.14.1.2 Review the e-mail message(s) and attachments involved.
- 7.14.2 If the investigation does not substantiate the report of inappropriate e-mail usage, the Program Head, District chief or Deputy Director shall stop the investigation immediately, advise the employee and take no further action.
- 7.14.3 If the Program Head, District chief or Deputy Director deems the e-mail message to be inappropriate for any reason, the Deputy Director shall check with the DMH Chief Information Officer to ascertain if there are/were any other known e-mail offenses by this employee.
 - 7.14.3.1 Disciplinary actions, if any, will be in accordance with relevant County regulations and civil service regulations.
 - 7.14.3.2 If the District Chief or Deputy Director determines that the employee's e-mail access privileges are to be suspended or revoked, the District Chief or Deputy Director shall promptly notify the DMH Chief Information Officer of such determination.
- 7.15 The DMH Chief Information Officer shall suspend/revoke e-mail access immediately upon being notified of the determination by the employee's District Chief or Deputy Director. The e-mail account will remain closed until the matter is resolved.

COMMERCIAL SOFTWARE

- 8.1 Standard
 - 8.1.1 The DMH approved list of commercial application software is shown in the Los Angeles County Department of Mental Health "Application Software Standard" (Attachment II).
 - 8.1.2 The installation of any other software requires the approval of the ITSO. Users or units must submit a written request with justification to the CIO Bureau.
 - 8.13 If non-standard software interferes with network security or the functions of the operating system, standard software or any hardware component, the non-standard software will be removed.
 - 8.14 Instant Messaging and peer-to-peer file sharing software are strictly prohibited.



DEPARTMENT OF MENTAL HEALTH POLICY/PROCEDURE

SUBJECT: NETWORKED INFORMATION SYSTEMS USAGE	POLICY NO. 302.14	EFFECTIVE DATE 10/01/03	PAGE 10 of 10
---	------------------------------	--	--------------------------

8.15 Any other software that bypasses the DMH and Los Angeles County network security perimeter control without specific authorization is strictly prohibited.

8.2 Copyright Compliance

8.2.1 DMH holds license agreements with makers of standard software. To comply with the license requirements, only authorized staff from the CIO Bureau are allowed to perform installations or upgrades.

8.2.2 Users of non-standard software (see Section 8.1) are responsible for copyright compliance.

8.2.3 Unauthorized copying and installation of any software are violations of Federal law. Removal or moving of software might be a violation of the license agreement.

8.2.4 Personal copies of software shall not be installed on any County computer.

8.3 Application Software Developed by DMH

8.3.1 All software developed by DMH, whether internally or by contracted entities is considered to be the property of DMH.

8.3.2 Software development must follow standard industry guidelines.

8.3.3 All software, prior to being put into production, requires review and approval by the ITSO.

AUTHORITY

Auditor-Controller Internal Control Certification Program (ICCP) Requirements, 1999

ATTACHMENTS

Attachment I Network Access Request Form
Attachment II Application Software Standard.

REVIEW DATE

This policy shall be reviewed on or before November 15, 2004 and annually thereafter.