



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.410

CHAPTER Regulatory Compliance	SUBCHAPTER HIPAA Regulations	EFFECTIVE DATE 6-27-2014	NUMBER OF PAGES 2	PAGE NUMBER 1 of 2
SUBJECT Electronic Device Use & Security		AUTHORITY 630.050 RSMo	HISTORY See Below	
PERSON RESPONSIBLE General Counsel			SUNSET DATE 7-1-2017	

PURPOSE: To establish the Department of Mental Health (DMH) policies and procedures regarding use and security of electronic devices used by DMH workforce to conduct DMH business.

APPLICATION: Applies to DMH, its facilities and workforce.

(1) Definitions

(A) DMH Workforce Members - Includes all state employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity (facility or Department). This shall include client workers employed by the Department of Mental Health or its facilities.

(B) Electronic Device - Workstations, laptops, tablets, phones or other state purchased electronic devices used to conduct DMH business.

(C) Electronic Protected Health Information (E-PHI) – Individually identifiable health information that is transmitted or maintained in electronic media; or transmitted or maintained in any other form or medium.

(D) Network – Electronic network allowing access to the DMH's personal computers, facility-based systems, and centrally-based systems (e.g. mainframe, server, desktop, etc.) and electronic data.

(2) Workforce Member Responsibilities

Work force members shall:

(A) Use electronic devices in an appropriate manner considering the sensitivity of the information contained therein and minimizing the possibility of unauthorized access to such information. Workforce members shall protect confidential data pursuant to DOR 8.040, Access to Consumer Protected Health Information by DMH Staff, Volunteers or Students.

(B) Request access to the DMH network and electronic systems by following the procedures in DOR 8.300, User Access to Electronic Data. The minimum amount of access necessary to perform job duties shall be granted.

(C) Review DOR 8.300, User Access to Electronic Data, and abide by the rules for appropriate uses of electronic systems from electronic devices.

(D) Not download or attempt to install any software including games or screen savers from any source including the internet, a CD, or any external device. Software shall only be loaded onto an electronic device by authorized ITSD staff.

(E) Sign the Portable Device Agreement attached to DOR 8.080, Ensuring Confidentiality of Protected Health Information for DMH Staff When Working Away from a Facility Setting, when taking electronic devices away from their normal work location.



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.410

SUBJECT Electronic Device Use & Security	EFFECTIVE DATE 6-27-2014	NUMBER OF PAGES 2	PAGE NUMBER 2 of 2
---	-----------------------------	----------------------	-----------------------

(F) Completely shut down portable devices before transporting them in order to initiate the encryption software.

(G) Connect portable devices to the DMH network at least monthly to ensure the anti-malware software is current.

(H) Lock their electronic devices any time they are unattended.

(I) Not disable the anti-malware software on any electronic device.

(J) Choose a secure password. Passwords should not be written down. Passwords should not be patterned from one cycle to the next. (i.e. Password1, Password2, Password3)

(K) Report anything suspicious on their electronic device.

(L) Not click on unknown links which may arrive in emails.

(3) Use of Electronic Devices

(A) Portable storage devices such as flash drives, thumb drives or CDs that store E-PHI shall be encrypted.

(B) Personal portable storage devices such as flash drives, thumb drives or CDs shall not be accessed via DMH electronic devices.

(C) Electronic devices shall be positioned to avoid viewing by anyone not authorized. Workforce members shall be responsible for keeping electronic devices out of public view.

(4) Security Methods

(A) ITSD shall configure all electronic devices to lock after 15 (fifteen) minutes of inactivity.

(B) ITSD shall load the state standard encryption software on all electronic devices.

(C) ITSD shall load anti-malware software on all electronic devices that will be used by DMH staff and systems.

(5) LOCAL POLICIES: There shall be no facility policies pertaining to this topic. The DMH DOR shall control.

(6) REVIEW PROCESS: The Chief Security Officer shall collect information from ITSD as needed to monitor compliance with this DOR.

(7) SANCTIONS: Failure of staff to comply or assure compliance with the DOR may result in disciplinary action, up to and including dismissal.

History: Original DOR effective June 27, 2014.