



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

CHAPTER Regulatory Compliance	SUBCHAPTER HIPAA Regulations	EFFECTIVE DATE 6/26/13	NUMBER OF PAGES 6	PAGE NUMBER 1 of 6
SUBJECT User Access to Electronic Data		AUTHORITY 630.050	History See below	
PERSON RESPONSIBLE General Counsel			Sunset Date 7/1/16	

Purpose: The policy of the Missouri Department of Mental Health (DMH) is to secure consumer's protected health information in compliance with federal law and federal regulations at 45 CFR Sections 164(c)(1) and (2), and 42 CFR Part 2. The practice of DMH is to ensure that its workforce recognizes the importance of such security provisions, and affirmatively acknowledge those guidelines. (Please also see DOR 6.675)

Application: DMH, its facilities and workforce.

(1) Definitions:

(A) Computer Systems: Computers connected to local and statewide communication networks, database storage or electronic records systems, Internet or email or other DMH portable computing devices.

(B) 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.

(C) Consumer: Any individual who has received or is receiving services from the Department of Mental Health (D Client Work Program: Any number of DMH programs that employ consumers of DMH.

(D) Chief Security Officer (CSO): Individual designated to oversee all activities related to the development, implementation, maintenance of, and adherence to DMH and facility policies and procedures covering the electronic and physical security of, and access to, protected health information and other DMH data in compliance with federal and state laws and regulations.

(E) ITSD: Information Technology Services Division. A division in the Office of Administration that is responsible for the operation of computer systems within affected departments.

(F) ITSD Account Management Group: The ITSD staff responsible for granting access to DMH systems and acting as DMH's liaison to other agencies. This group shall ensure compliance with the standards outlined in this document through routine audits.

(G) Local Security Officer (LSO): Individual designated to oversee facility information and physical security practice and policy compliance and to coordinate those activities with the CSO.

(H) Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in any form or medium, by a covered entity, health plan or clearinghouse as defined under the Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and 164.



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

SUBJECT User Access to Electronic Data	EFFECTIVE DATE 6-26-13	NUMBER OF PAGES 6	2 of 6
---	---------------------------	----------------------	--------

(I) Social media: Media for social interaction, using highly accessible web based mobile communication techniques.

(2) General

(A) Management's Right to Access Information

1. Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq), DMH has complete access to all email and Internet activities. No electronic communications sent or received are considered private to the employee. DMH has the right to monitor messages and Internet use as necessary to ensure efficient and appropriate use of the technology.

2. Each of the electronic communications technologies may create electronic records that are easily saved, copied, forwarded, retrieved, monitored, reviewed, and used for litigation. All electronic records are the property of DMH and can be accessed and used by management when:

- a. A legitimate business need exists; or
- b. The involved employee is unavailable and timing is critical to a business activity; or
- c. There is reasonable cause to suspect criminal activity or policy violations, or other misuse; or
- d. Law, regulation, or third-party agreement requires such monitoring; or
- e. During the course of any DMH, state or federal audit.

3. These disclosures of electronic records may be made without prior notice to the staff members who sent or received the communications. Staff members should not assume that any electronic communications are private.

(3) User Access to Electronic DMH Data

To gain access to any DMH systems or data containing PHI, DMH workforce members are required to complete the DMH Staff Access Request Form. Such access shall be limited to the minimum necessary amount of PHI to accomplish the purpose of any requested use or disclosure of PHI.

1. The appropriate supervisor or manager must approve the request(s) in writing.
2. The appropriate LSO must approve the request(s) in writing.
3. The request form(s) must be submitted each time a user's access status changes or a user leaves DMH.
4. User IDs shall be password protected.
5. User IDs shall be created using the DMH naming standard outlined in the attached procedure.
6. Passwords will expire every 60 days.
7. Staff may obtain electronic access to other state agency data with the approval of their supervisor and LSO by completing the required forms.

(C) Customer Information Management, Outcomes & Reporting (CIMOR)



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

SUBJECT User Access to Electronic Data	EFFECTIVE DATE 6-26-13	NUMBER OF PAGES 6	3 of 6
---	---------------------------	----------------------	--------

1. Users shall log on to the CIMOR portal to request access.
2. The appropriate supervisor or manager shall approve or deny the request(s).
3. The appropriate LSO shall approve or deny the entire request.
4. An assigned divisional business owner shall approve or deny the entire request.
5. ITSD Account Management shall grant final approval and grant the requested, approved access.

(C) Users shall be required to protect confidential data pursuant to DOR 8.040, Access to Consumer Protected Health Information by DMH Staff, Volunteers or Students.

(D) Removal of access for a terminated employee

1. DMH Human Resources staff shall notify ITSD Account Management when employees leave employment.
2. Accesses will be deleted according to the attached procedure for disabling accounts.
3. Email access will be terminated according to the attached procedure for termination of email.

(E) No DMH consumer, volunteer, or student shall have access to another person's PHI, any DMH client demographic system, or be allowed to input information to local systems that may be used to feed or modify those systems unless they are employed under the Client Work Program defined in this policy, or have data entry as part of their volunteer or student duties and responsibilities, and have signed the confidentiality statement, or unless authorized by the consumer. Any proposed consumer access shall include documentation of the consumer reviewing and agreeing to a confidentiality statement. Documentation shall include: the types of systems and files accessed.

(F) Such consumer access shall be approved by the facility director, or designee with notification and documentation provided to the CSO.

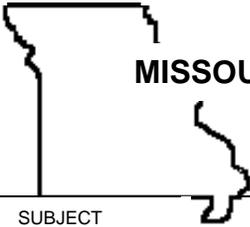
(G) All employees shall sign the USE OF ELECTRONIC RESOURCES AGREEMENT form attached to this DOR prior to being given access to any DMH system.

(H) All employees shall complete mandatory HIPAA training.

(4) Access to Internet and Electronic Mail (Email)

(A) Users are required to abide by the following guidelines when using DMH email systems and Internet access systems.

1. The Internet and email are intended to be used primarily for business purposes.
2. The Internet may be used to access external databases and files to obtain reference information or to conduct research.
3. Email may be used to disseminate business-related newsletters, press releases, or other documents to groups of people.
4. Email and the Internet may be used for discussion groups on job-related topics.



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

SUBJECT User Access to Electronic Data	EFFECTIVE DATE 6-26-13	NUMBER OF PAGES 6	4 of 6
---	---------------------------	----------------------	--------

5. Access is permitted only to social media sites (such as Facebook, MySpace, Twitter, etc.) that are specifically authorized for job related duties and related to DMH business.

6. Personal use of email must be limited and must not interfere with the performance of work duties.

7. DMH users as well as staff supporting DMH, must add a confidentiality notice to their email signature similar to the following:

Confidentiality Notice:

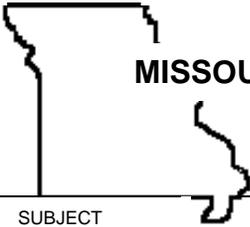
This e-mail and any attachments may contain confidential and privileged information for the use of the designated recipients named above. If you are not the intended recipient, you are hereby notified that you have received this communication in error and that any review, disclosure, dissemination, distribution or copying of it or its contents is prohibited by federal or state law. If you have received this communication in error, please contact me immediately.

8. Calendar events in Outlook that contain a consumer name or other identifying consumer information shall be marked private.

9. Users shall not access DMH email using a personal device unless prior approval has been granted by the user's supervisor and the user has signed the iPhone agreement. Use of personal devices to access DMH email may result in a personal device being wiped out or confiscated if required for litigation.

(B) Email and/or the Internet may not be used for:

1. Any illegal or unethical purpose;
2. Private purposes such as advertising products or services, business transactions, or for private business activities;
3. Operating a business, sending chain letters, or soliciting money for any purpose except for employee relations committee activities, coworker retirements or other milestone events, or events sanctioned by the Office of Administration such as blood drives or charitable campaign;
4. Transmitting, downloading or viewing material that is obscene, pornographic, threatening or harassing, or information that may reasonably be perceived to be obscene, threatening or harassing to another individual;
5. Disseminating, copying, or printing copyrighted materials (including articles, software, music and movies) in violation of copyright laws;
6. Subscribing to mailing lists and broadcast services that do not relate to the business of the Department;
7. Downloading software of any kind without prior approval of ITSD;
8. Participating in Internet chat rooms or instant messaging, including but not limited to, AOL Instant Messenger and Internet Relay Chat (IRC), for other than authorized DMH business purposes.;
9. Playing games;



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

SUBJECT User Access to Electronic Data	EFFECTIVE DATE 6-26-13	NUMBER OF PAGES 6	5 of 6
---	---------------------------	----------------------	--------

- 10. Conducting any political activity;
- 11. Conducting any religious activities that are not directly business related (e.g. chaplains doing research on the Internet); or
- 12. Accessing social media sites for other than authorized DMH business purposes.

(C) An internet filter will be used and maintained to ensure that sufficient bandwidth is available for department business, to maintain the security and integrity of department networks and databases, and to prevent employees from accessing websites that may be offensive or inappropriate for state business. The filter will block or allow websites based on categorization.

(5) Training on Access. All DMH employees, consumers, volunteers and students must receive the privacy training required by DOR 8.090.

(6) Required Confidentiality Agreement

(A) DMH workforce members that receive or maintain PHI shall be required to agree to the security of such PHI in accordance with the state and federal laws as set forth above. These workforce members shall sign a confidentiality statement pursuant to DOR 8.040. A copy of the signed confidentiality statement shall be maintained in the personnel file of DMH staff.

(7) Password Management

(A) Passwords shall not contain the user account number (userID) and shall contain no less than seven (7) characters (no maximum) to include three (3) of the four (4) following elements:

- 1. English upper case characters (A..Z);
- 2. English lower case characters (a..z);
- 3. Base ten (10) digits (zero (0)..nine (9));
- 4. Non-alphanumeric (For example, !,\$#,%)

(B) Passwords should:

- 1. Be changed immediately if user is aware that someone else knows it;
- 2. Not be entered or changed when others may see them;
- 3. Have no obvious connection to the user. i.e. user name, children's name, etc.;
- 4. Changed completely when it expires with no easily discernable pattern and
- 5. Not be written down and left in a location it could be found and used to access DMH systems.

(8) LSO's shall be responsible for auditing, monitoring, and maintaining adherence to this DOR as it applies to any and all local systems that contain PHI that is located in their facility

(9) There shall be no facility policies pertaining to this topic. DMH Operating Regulations shall control.

(10) Sanctions. Failure of workforce members to comply or ensure compliance with the DOR may result in disciplinary action, up to and including dismissal.



MISSOURI DEPARTMENT OF MENTAL HEALTH

KEITH SCHAFFER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.300

SUBJECT User Access to Electronic Data	EFFECTIVE DATE 6-26-13	NUMBER OF PAGES 6	6 of 6
---	---------------------------	----------------------	--------

(11) Review Process. The CSO will collect information from the LSOs during the month of April each year for the purpose of analyzing trends and issues associated with compliance with this regulation.

(12) Attachment, USE OF ELECTRONIC RESOURCES AGREEMENT, DMH User ID Naming Standard, Email Termination Procedure, Disabling User Accounts.

History: Emergency DOR effective January 15, 2003. Final DOR effective September 1, 2003. Amendment effective July 1, 2005. On July 1, 2008 the sunset date was extended to July 1, 2011. Amendment effective July 1, 2008. On June 29, 2011 the sunset date was extended to July 1, 2014. Amendment effective June 29, 2011. Amendment effective June 26, 2013.

STATE OF MISSOURI
DEPARTMENT OF MENTAL HEALTH
USE OF ELECTRONIC RESOURCES AGREEMENT

To: Human Resources	RE: Use of Electronic Resources Agree
<p>I have been made aware of and have read the State of Missouri, Department of Mental Health's Department Operating Regulations regarding:</p> <ol style="list-style-type: none">1. User Access to Electronic Data (DOR 8.300); and2. Information Security Incidents (DOR 8.350). <p>By signing this form, I confirm that I understand and will comply with all the guidelines outlined in these regulations.</p> <p>I also understand that failure to comply with any of these regulations may result in disciplinary action up to and including dismissal.</p>	
EMPLOYEE NAME (PRINTED)	DIVISION/OFFICE/FACILITY
EMPLOYEE SIGNATURE	DATE

DMH UserID Naming Standard 4 (A) (7)

Definitions:

Resource Account: Accounts created for service accounts, kiosks, training rooms, etc.

Non-staff Account: Accounts created for vendors, consultants, contractors (excluding contract providers)

Procedure:

All userIDs will begin with the following characters:

- Character one (1) = "m"
- Character two (2) = location identifier (see table)

USER ACCOUNTS:

User accounts for state employees and contract providers will be assigned the following standard:

- Characters three (3) – six (6) = the 1st four (4) letters of the user's last name
- Character seven (7) = the first letter of the user's first name (preferred name)

In the event a new user account will create a duplicate, the last character of the last name (position six (6)) will be replaced with a numeric beginning with one (1). If more than nine (9) duplications occur, the preceding letter will be replaced with a numeric beginning with one (1), and so forth. The location identifier must match the location that employs the user.

User accounts for DMH employees will be renamed in the following circumstances:

- If an individual changes names (email address shall also be changed)
- If an individual changes employment from one location to another unless the user will retain the duties from the previous location
- Mainframe accounts will not be renamed

The procedure for a name change is:

- The LSO (requestor) completes a "DMH Staff Access Request Form"
- On the form, check "change" and complete "PART 1" with the user's new information
- Write "NAME CHANGE" on the form, and include the user's previous name and userID
- The ITSD Account Management Group will complete any additional forms on the requestor's behalf

The ITSD Account Management Group will notify the requestor when the new access is in place.

RESOURCE ACCOUNTS & NON-STAFF ACCOUNTS:

Resource accounts shall be assigned the following standard:

- Character one (1) "m"
- Character two (2) location identifier (see table)
- Characters three (3) characters representing the account's function ("con" for consultant; "int" for intern)

Suggested examples:

- A consultant named John Smith working for IBM at Rolla: "mqconSmithJ"
- Quadramed support account: "mzquadramed"
- A shared training room account used at Fulton: "mbtraining1"

LOCATION IDENTIFIER TABLE:

ID - Location

- B - Fulton State Hospital
- C - Northwest Missouri Psychiatric Rehabilitation Center
- D - Southwest Missouri Psychiatric Rehabilitation Center
- E - Southeast Missouri Mental Health Center
- F - Saint Louis Psychiatric Rehabilitation Center
- G - Marshall Habilitation Center
- H - Bellefontaine Habilitation Center
- I - Metropolitan Saint Louis Psychiatric Center
- K - Albany Regional Center
- L - Kirksville Regional Center
- M - Hannibal Regional Center
- N - Kansas City Regional Center
- P - Springfield Regional Center
- Q - Rolla Regional Center
- R - Poplar Bluff Regional Center
- S - Sikeston Regional Center
- T - Saint Louis DDTC
- U - Center for Behavioral Medicine (including Paseo)
- V - Higginsville Habilitation Center
- W - Saint Louis Regional Center
- X - Nevada Habilitation Center
- Z - Central Office
- 1 - Hawthorn Child Psychiatric Hospital
- 3 - Central Missouri Regional Center
- 4 - Cottonwood Residential Treatment Center
- 6 - Southeast Missouri Residential Services
- 7 - Missouri Sexual Offender Treatment Center
- 9 - Joplin Regional Center
- Y - All contract providers

EMAIL TERMINATION PROCEDURE (3) (D)

Mailboxes that need to be accessed by another user

1. ITSD Account Management shall be notified if a mailbox will need to be viewed by someone else before the user leaves..
2. This access will remain available until ITSD Account Management is notified to remove the access and delete the mail box.

Mailboxes that do not need to be accessed by another user

1. Disable the terminated employee's email account.
2. Delete all email content of the terminated employee on the next work day after the fourteen (14) day retention period.

Terminated employee's manager responsibilities

1. Review the email content of the terminated employee.
2. Request specific content to be made permanently available to them.
3. Notify likely future senders of email to the terminated employee who they should be corresponding with in the future.

Disabling User Accounts (3, D, 1)

1. The ITSD Account Management Group is notified by DMH HR or the facility LSO when employees terminate employment.
2. The ITSD Account Management Group will immediately disable the account through Active Directory.
3. The LSO will forward, to the ITSD Account Management Group, any applicable security access forms marked REVOKE.
4. The ITSD Account Management Group will remove the terminated user from any distribution and security groups in Active Directory.
5. The ITSD Account Management Group will check to see if the user had CIMOR access, and revoke access if indicated.
6. The ITSD Account Management Group will forward any additional Security Access Forms to the appropriate agency for termination (i.e., SAM II HR, SAM II Financial, MAIRS, etc.). Upon receiving notification back from the agency that the access has been revoked, the document will be scanned for electronic filing by CO.
7. One hundred, eighty (180) days after a CO user's account was disabled, End User Support will delete the user's home directory. Thirty (30) days after a facility user's account is disabled, End User support will delete the user's home directory. NOTE: Any files from a user's home directory that need to be permanently retained will be copied to CD and given to the user's supervisor. Special arrangements for permanent retention can be requested by DMH Legal Counsel.