



MISSOURI DEPARTMENT OF MENTAL HEALTH

MARK STRINGER, DEPARTMENT DIRECTOR



DEPARTMENT OPERATING REGULATION NUMBER
DOR
8.400

CHAPTER Regulatory Compliance	SUBCHAPTER HIPAA Regulations	EFFECTIVE DATE 7-24-2015	NUMBER OF PAGES 4	PAGE NUMBER Page 1 of 4
SUBJECT Breach Determination and Notification		AUTHORITY 630.050 RSMO	HISTORY See Below	
PERSON RESPONSIBLE General Counsel			SUNSET DATE 7-1-2019	

PURPOSE: To establish the Department of Mental Health (DMH) breach notification and response processes and identify the procedures, roles and responsibilities required.

APPLICATION: Applies to DMH, its facilities and workforce.

(1) DEFINITIONS:

(A) **Breach:** The acquisition, access, use or disclosure of protected health information in a manner not permitted under HIPAA law which compromises the security or privacy of the protected health information.

(B) **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.

(C) **Consumer:** Any individual who has received or is receiving services from the Department of Mental Health.

(D) **DMH Privacy Officer:** The person officially designated to oversee all ongoing activities related to the development, implementation, maintenance of, and adherence to the DMH Operating Regulations pertaining to the privacy of, and access to, consumer health information in compliance with federal and state laws and the DMH’s notice of privacy practices.

(E) **Department of Mental Health 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.

(F) **Information Security Management Office (ISMO):** The unit at the State of Missouri’s Office of Administration responsible for cyber security, responding to possible security incidents, monitoring the statewide network and notifying agencies of the State of Missouri’s threat level.

(G) **ITSD:** Information Technology Services Division of the Missouri Office of Administration.

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

(I) **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

MARK STRINGER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.400

SUBJECT Breach Determination and Notification	EFFECTIVE DATE 7-24-2015	NUMBER OF PAGES 4	PAGE NUMBER Page 2 of 4
--	-----------------------------	----------------------	----------------------------

(2) PROCEDURE:

If, after following the procedures in DOR 8.350, it has been determined a breach has occurred, the following steps shall be taken:

(A) The CSO shall:

1. Inform the DMH Privacy Officer of the breach; and

(B) Complete the Breach Notification Assessment to determine if a reportable breach has occurred.

The LSO, CSO, DMH Privacy Officer and any other required staff will work together to determine what steps need to be taken and then follow the appropriate procedure. The following should be determined:

1. If notification to consumer(s) is necessary;

2. If notification to US Department of Health & Human Services is necessary;

3. If mitigation steps are needed to prevent future risk of breach; and

(C) Who should send the notification based on the scope of the breach.

(D) ITSD shall assist DMH with technical assistance as requested.

(E) The ISMO will contact law enforcement if the need arises.

(F) The breach will be recorded in the appropriate database to be included in the annual report to the US Department of Health & Human Services.

(G) The CSO and DMH Privacy Officer will review DMH policies and procedures to determine if any changes are needed.

(H) If the breached data was supplied to DMH by the Social Security Administration (SSA), DMH must notify the SSA Systems Security contact named in the agreement within one (1) hour. If within one (1) hour DMH has been unable to make contact with that person, DMH must call SSA's National Network Service Center (NNSC) toll free at 877-697-4889 (select "Security and PII Reporting" from the options list). DMH will provide updates as they become available to SSA contact, as appropriate. The CSO will make these notifications and updates to SSA.

(3) NOTIFICATION:

If the breach requires a notification be sent to consumer(s), the following procedure shall be followed.

(A) Notifications must be sent no later than sixty (60) days following the date of the breach.

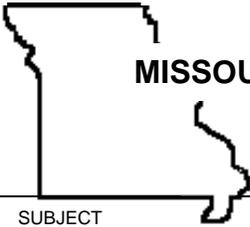
(B) The breach notification shall be written in plain English which is targeted to a third grade reading level if possible.

(C) The notification shall contain:

1. A brief description of how the information was breached including the date of breach and date of discovery, if known;

2. A description of the types of unsecured PHI involved;

3. Any steps the consumer should take to protect themselves from potential harm resulting from the breach;



MISSOURI DEPARTMENT OF MENTAL HEALTH

MARK STRINGER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.400

SUBJECT Breach Determination and Notification	EFFECTIVE DATE 7-24-2015	NUMBER OF PAGES 4	PAGE NUMBER Page 3 of 4
--	-----------------------------	----------------------	----------------------------

4. A brief description of what DMH is doing to investigate the incident, mitigate harm to the individual, and prevent future incidents; and

5. Contact procedures for individuals to ask questions or learn additional information. The contact information shall be in the form of a toll-free telephone number, email address, website address, or postal address.

(D) The breach notification shall be provided in writing, by first class mail, to the last known address of the consumer. If the consumer has agreed to receive notices via email, the notification may be sent electronically.

1. If the consumer is deceased:

i. The consumer's record will be searched to determine who has been approved to receive their PHI. The next of kin shall only be notified if formerly approved by the consumer in writing.

ii. If an address is contained in the file for an approved receiver of the consumer's information, the notice shall be sent.

iii. If the notification is returned due to an incorrect mailing address, no further notification is required.

iv. Documentation shall be added to the consumer's file stating the actions taken.

2. If less than ten (10) notifications are returned undeliverable due to bad mailing addresses, a phone call or face to face notification can be substituted for those notifications.

3. If ten (10) or greater notifications are returned undeliverable due to bad mailing addresses, a substitute notification shall be made by a posting on the DMH website including a toll free number where consumers may call to determine if their information was breached.

4. If the risk is high that the information breached may be immediately harmful to the consumer, a phone call or other means of communication is also required within ten (10) working days of the confirmed breach.

(E) If the breach involved five hundred (500) or more individuals, a notification must be sent to the local media in the area, as well as, the US Department of Health & Human Services as prescribed on the HHS website.

(4) **DOCUMENTATION:** A record of all breaches shall be kept for six (6) years. Annually, a report must be sent to the US Department of Health and Human Services. Incidents determined not to be reportable breaches must also be documented and all supporting evidence maintained.

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

(6) **LOCAL POLICIES:** There shall be no facility policies pertaining to this topic. The Department Operating Regulation shall control.

(7) **REVIEW PROCESS:** The CSO shall collect information from the LSOs during the month of April each year to monitor compliance with this DOR.

History: Original DOR effective July 19, 2013. Amendment effective July 24, 2015.



MISSOURI DEPARTMENT OF MENTAL HEALTH

MARK STRINGER, DEPARTMENT DIRECTOR



DEPARTMENT
OPERATING
REGULATION
NUMBER

DOR
8.400

<p>SUBJECT Breach Determination and Notification</p>	<p>EFFECTIVE DATE 7-24-2015</p>	<p>NUMBER OF PAGES 4</p>	<p>PAGE NUMBER Page 4 of 4</p>
--	-------------------------------------	------------------------------	------------------------------------

Attachments: Breach Risk Assessment Tool

--- Section 1 ---

Breach Notification Risk Assessment Tool

DOR 8.400

<p>1. Does this incident qualify as one of the following exceptions? <i>If Yes, then STOP here. No breach has occurred that requires notification.</i> <i>If No, then proceed to next section to work through the rest of the assessment to determine if the breach poses a significant risk to the financial, reputational, or other harm to the individual to the extent that it would require notification.</i></p>	<p align="center">Y/N</p>
<p>a. Good faith, unintentional acquisition, access or use of PHI by employee/workforce <i>Example- A billing employee receives and opens an e-mail containing protected health information about a patient which a nurse mistakenly sent to the billing employee. The billing employee notices that he is not the intended recipient, alerts the nurse of the misdirected e-mail, and then deletes it.</i></p>	
<p>b. Inadvertent disclosure to another authorized person within DMH or a contract provider <i>Example- a physician who has authority to use or disclose protected health information at a hospital by virtue of participating in an organized health care arrangement with the hospital is similarly situated to a nurse or billing employee at the hospital.</i></p>	
<p>c. Recipient could not reasonably have retained the data <i>Example- a covered entity, due to a lack of reasonable safeguards, sends a number of explanations of benefits (EOBs) to the wrong individuals. A few of the EOBs are returned by the post office, unopened, as undeliverable. In these circumstances, the covered entity can conclude that the improper addressees could not reasonably have retained the information.</i></p>	

Circle the appropriate score for each subsection.

--- Section 2 ---		
DOR 8.400	Breach Notification Risk Assessment Tool	
Variable	Options	Score
What is the likelihood the data could be reidentified?	<ul style="list-style-type: none"> • Low – name, SSN, etc. not included 	1
	<ul style="list-style-type: none"> • Medium – enough data present to identify after some analysis 	2
	<ul style="list-style-type: none"> • High – name, SSN, or other identifying data present 	3
Recipient(s)	<ul style="list-style-type: none"> • Your Business Associate • Another Covered Entity • Internal Workforce • Authorized staff but exceeds the minimum necessary 	1
	<ul style="list-style-type: none"> • Wrong Payor (not the patient's) • Unauthorized family member • Non-covered entity 	2
	<ul style="list-style-type: none"> • Media • Legislator • Unknown/Lost/Stolen • Member of the general public 	3
Was the data actually viewed or acquired?	<ul style="list-style-type: none"> • Accidental viewing only • Accidentally acquired. Returning without viewing 	1
	<ul style="list-style-type: none"> • Accidentally acquired & viewed but reported • Data unintentionally disclosed 	2
	<ul style="list-style-type: none"> • Unknown • Data intentionally disclosed 	3
Extent the risk has been mitigated.	<ul style="list-style-type: none"> • Information returned complete • Information destroyed and attested to 	1
	<ul style="list-style-type: none"> • Information properly destroyed (unattested) • Electronically Deleted (unsure of backup status) 	2
	<ul style="list-style-type: none"> • Sent to the Media • Unable to retrieve • Unsure of disposition or location • High (suspicion of pending re-disclosure) • Extremely High (PHI already re-disclosed) 	3
	<ul style="list-style-type: none"> • Data Wiped • Information/Device Encrypted, but does not meet compliance with NIST Standards 	1

