POLICY: It is the policy of the Division of Mental Health and Developmental Services (MHDS) to provide timely notification to an individual if it is determined that a breach has occurred involving the individuals protected health information. The notification, when applicable, will also be provided to the Secretary of Health and Human Services and the news media.

PURPOSE: The purpose of this policy is to provide guidance for the Division of Mental Health and Developmental Services and its agencies to comply with the breach notification requirements included in law and regulation.

SCOPE: Division wide

I. REFERENCES:

American Recovery and Reinvestment Act (ARRA)

Health Information Technology for Economic and Clinical Health ACT (HITECH) Health Insurance Portability and Accountability Act

NRS 603A.220

II. DEFINITIONS:

Access: The ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach: The unauthorized acquisition, access, use, or disclosure of protected health information that violates the Privacy Rule, or compromises the security or privacy of PHI. *Compromises the security or privacy of PHI* means poses a significant risk of financial, reputational, or other harm to the individual.

A. Breach Exceptions:
    1. Unintentional access or use of PHI by staff, if made in good faith and within their scope of authority, and does not result in further use or disclosure that violates HIPAA.
    2. Inadvertent disclosure by a person who is authorized to access PHI, such as overheard discussions with another consumer or staff
    3. Improbable retention (unable to retain), such as a bill sent to wrong address and is returned undeliverable.

Business Associate: Organization or individual who performs any function or activity on the behalf of the covered entity involving the use or disclosure of PHI and is not a member of the covered entity's workforce.

Covered Entity: A health plan, a health care clearinghouse, or a health care provider who transmits any protected health information in electronic form in connection with a standard transaction

Disclosure: The release, transfer, provision of, access to, or divulging in any other manner of information outside the covered entity holding the information

Individually Identifiable Health Information: Health information in any form or media, including demographic information collected from an individual, that is created or received by a covered entity or business associate and relates to individual, that relates to the past, present, or future physical or mental health condition of an individual, providing health care to an individual; or the past, present, or future payment for the individual's health care; that identifies the individual or could reasonably be used to identify the individual; and that is transmitted or maintained in any form or medium.

Protected Health Information: Individually Identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium

Secretary: Secretary of the Department of Health and Human Services (DHHS), federal level, or the Secretary's designee

Secured Protected Health Information: Protected Health information that is rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary in the guidance issued under HITECH. Secured PHI includes the following;

1. Electronic PHI that has been encrypted
2. Media on which the PHI is stored or recorded has been destroyed in one of the following ways:
   a. Paper, film, or other hard copy media have been shredded or destroyed so it is unreadable
   b. Electronic media have been cleared, purged, or destroyed such that PHI cannot be retrieved

This includes data at rest (i.e., data that resides in databases, file systems, and other structured storage systems), data in motion (i.e., data that is

moving through a network, including wireless transmission), data in use (i.e., data in the process of being created), and data disposed (i.e. discarded paper records)

Workforce: Employees, contractors, temporary workers, students, interns, externs, volunteers, or other workforce members 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.

III. PROCEDURES:

A. DISCOVERED BREACH:

A breach is deemed to have been discovered as of the first day on which the breach is known or reasonably should have been known by any workforce member other than the person who committed the breach.

B. NOTIFICATION OF PRIVACY OFFICER:

Upon discovery of a potential breach, the agency's workforce member or business associate will notify the Agency's HIPAA Privacy Officer. An incident report will be completed.

C. RISK ASSESSMENT:

The Risk Assessment is performed to determine if an impermissible use or disclosure of unsecured PHI constitutes a breach.
Each Agency or the Business Associate has the burden of proof for demonstrating that all notifications were made as required or that the use or disclosure did not constitute a breach. The risk assessment should include the following in order to assess the risk of harm:

1. To whom the disclosure was made
2. Date and time of occurrence and/or discovery
3. Number of affected individuals
4. Types of PHI and amount of information disclosed
5. Possible imminent misuse of PHI (i.e., is the information properly protected by encryption; can the stolen PHI be sold?)
6. Likelihood of potential harm (i.e. disclosure of information of victims of abuse or social security numbers to commit identity theft)
7. Compliance of "minimum necessary" standards
8. Immediate actions to minimize the risk of harm caused by disclosure.
9. Steps taken to prevent future similar events

D. INVESTIGATION OF BREACH:

Agency Director, in consultation with the Privacy Officer, will review the risk assessment and determine the need for investigation.
If after review, there is no significant risk of harm, a breach notification is not required.

E. DOCUMENT RETENTION:

Documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

F. TIMELINE OF NOTIFICATION:

If it is determined that a breach of PHI has occurred, notification will be sent to:

1. affected consumer(s);
2. Division of MHDS;
3. Nevada Department of Health And Human Services (to be notified by MHDS)
4. U.S. Department of Health and Human Services and, in some cases, local media in the form of a press release if more than 500 people are affected.

The notice will be sent out as soon as practicable and in no case later than 60 calendar days after the breach was discovered. A notice may be delayed if requested by law enforcement for investigations.

G. DELAY OF NOTIFICATION AUTHORIZED FOR LAW ENFORCEMENT PURPOSES:

If a law enforcement official states to the Agency, Division, or Business Associate that a notification or posting would impede a criminal investigation or cause damage to national security, the Agency, Division, or Business Associate shall:

1. Specify the time for which a delay is required
2. Delay such notification/posting of the time period specified by the official
3. Document an oral statement, if not written, including the identity of the official, and delay the notification/posting no longer than 30 days after request for delay is received.

H. CONTENT OF THE NOTICE:

The breach notice will contain:

1. A brief description of what happened including date of discovery of the breach.
2. A description of the type(s) of unsecured PHI involved in the breach, such as name, Social Security numbers, birthdates, address, diagnosis, etc.
3. Steps the consumer should take to protect themselves from potential harm resulting from breach.
4. Brief description of what has been done and what is being done to investigate the breach, mitigate harm to the individual, and protect against further harm or breaches.
5. Contact procedures for the consumer to ask questions an receive information, to include a toll-free number, email address, website or postal address.

I. METHODS OF NOTIFICATION:

1. Notice to the individual(s) must be in writing, sent by first class mail or with the consumer's express affirmative consent, by email.
2. If the consumer is deceased and contact information is known for the next of kin or personal representative, the notice will be sent to that person. If next of kin or personal representative cannot be contacted, no additional steps need to be taken.
3. Notice may also be provided by phone if no other means of contact is known.
4. One or more mailings can be sent as more information is available.
5. Detailed documentation of contact attempts will be entered in the Risk Assessment.
6. If there is insufficient contact information for 10 or more affected consumers, a conspicuous notice on the home page of the Agency's website for 90 days, or a conspicuous notice in the local media (print or broadcast) will be posted in the area where the consumer likely resides. A toll-free number that remains active for 90 days will be provided.
7. If a breach of unsecured PHI involves more <u>than 500 residents in a state</u>, a notice must be posted in a prominent media in that state. The notice will be provided within 60 days after the discovery of the breach and will contain the same information that is included in the notice to the consumer.
8. If a breach affects the unsecured PHI <u>of 500 persons or more</u>, the Agency shall notify the Secretary of Health and Human Services (HHS) at the time the consumers are notified of no more than 10 days after the breach is discovered.

9. If the breach involves less than 500 consumers, the Division shall maintain a log of those breaches and annually submit to HHS within 60 days of the calendar year. Instructions for submitting the log are provided at www.hhs.gov/.

J. BREACH LOG AND DOCUMENTATION:

All suspected breaches are Serious Incident Reports (SIR)and must be logged into the Incident Tracking System of AVATAR. Each Agency shall maintain a process to record or log all suspected breaches of PHI regardless of the number individuals affected. The following information should be collected and logged for each breach:

1. A description of what happened, the date of the breach or suspected breach, the date of the discovery, and the number of consumers affected, if known.
2. A description of the types of protected health information that were involved in the breach (i.e., name, Social Security numbers, date of birth, diagnosis, address, account number, etc)
3. Resolution steps taken to mitigate the breach and prevent future occurrences

K. BUSINESS ASSOCIATE REQUIREMENTS:

A Business Associate of the Division will notify the Division Privacy Officer upon discovery of breach or suspected breach of PHI as soon as practicable. Prompt corrective action by the Business Associate must be taken to mitigate any significant harm that may have occurred to the individual(s) whose information was disclosed inappropriately. The Business Associate will be responsible for the following:

1. Risk Assessment to determine a breach has occurred
2. All breach notifications whether to the individual, media, or Secretary of HHS,
3. Evidence to the Division that appropriate notification has occurred
4. Corrective action

WORKFORCE TRAINING:

Each Agency shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for them to carry out their job responsibilities. Workforce members will also be trained as to how to identify and report breaches.

L. COMPLAINTS:

Each agency has a Complaint Procedure which provides a process for individuals to make complaints concerning the Division's individual privacy policies and procedures or its compliance with such policies and procedures, to include the breach notification process. Contact Division office for further information.

M. SANCTIONS:

DHHS prohibition and penalties specify the sanctions applicable to members of the workforce who fail to comply with HIPAA policies and procedures. The prohibition and penalties can be found at www.hhs.gov.

1. The types of sanctions will vary depending on the severity of the violation, whether the violation was intentional, unintentional, whether the violation indicates a pattern or practice of improper access, use, or disclosure of PHI, and similar factors.
2. These sanctions may include, but are not limited to, retraining, verbal and written warnings and dismissal. In addition, employees who knowingly and willfully or improperly use or disclose a consumer's PHI are subject to criminal investigation, prosecution and/or civil monetary penalties. In addition, the HIPAA civil and criminal penalties assessed as a result of an audit, breach, or violation of HIPAA or HITECH laws or regulation may be applied to the Division or Business Associate as well as the individual workforce members.

N. RETALIATION:

Neither the Agency nor the Division of MHDS can intimidate, threaten, coerce, discriminate against or take any other retaliatory action against an individual for reporting an alleged HIPAA violation or breach.

O. Each agency of the Division is responsible to implement a procedure to comply with this policy directive.

Harold Cook

ADMINISTRATOR

ATTACHMENTS:

A: RISK ASSESSMENT TOOL
B: SAMPLE NOTIFICATION LETTER TO CONSUMERS

EFFECTIVE DATE: 11/20/06
REVIEWED / REVISED DATE: 11/13/07, 08/06/10, 5/20/11
APPROVED BY MHDS ADMINISTRATOR: 08/06/10, 5/20/11
APPROVED BY MHDS COMMISSION: 5/20/11

ATTACHMENT A
RISK ASSESSMENT TOOL:
NOTE: For an acquisition, access, use or disclosure of protected health information (PHI) to constitute a breach, it must be a violation of the HIPAA Privacy Rule.

	Questions	Yes - Next Steps	No - Next Steps
	UNSECURED PHI		
1.	Was the impermissible used/disclosure unsecured PHI (e.g. the data was not encrypted or destroyed through the use of technology specified by the regulation)?	Continue next question.	Notifications not required. Document decision.
	MINIMUM NECESSARY		
2.	Was more than the minimum necessary PHI for the purpose accessed, used, or disclosed.	Continue to next question.	May determine low risk and not provide notifications. Document decision.
	DID THE USE/DISCLOSURE MEET ANY OF THE SPECIFIC BREACH DEFINITION EXCLUSIONS?		
3.	Was it an unintentional access/use/disclosure by a workforce member acting under the Division's authority, made in good faith, within his/her scope of authority and did not result in further use/disclosure (e.g. MHDS staff emails an individual's PHI to another Division employee in error. The other Division employee notifies staff of the error and deletes the email)?	Not a breach. Division appropriate corrective action. Document decision.	Continue to next question.

ATTACHMENT A
RISK ASSESSMENT TOOL:
NOTE: For an acquisition, access, use or disclosure of protected health information (PHI) to constitute a breach, it must be a violation of the HIPAA Privacy Rule.

4.	Was it an inadvertent use or disclosure of PHI by a person authorized to access PHI at the Division to another person authorized to access PHI at the same Division and the information was not further used or disclosed (e.g. PHI exchanged between Division workforce members authorized to have such access and PHI was not further used or disclosed)?	Not a breach. Division appropriate corrective action. Document decision.	Continue to next question.
5.	Was a use or disclosure of PHI made, but there is a good faith belief that the unauthorized person who received the PHI would not have reasonably been able to retain the information (e.g. a nurse mistakenly hands an individual discharge papers belonging to a different individual, but quickly realizes the mistake and recovers the PHI from the individual, and the nurse reasonably concludes the individual could not have read or otherwise retained the information)?	Not a breach. Division appropriate corrective action. Document decision.	Continue to next question.
	WHAT TYPE AND AMOUNT OF PHI WAS INVOLVED IN THE IMPERMISSIBLE USE OR DISCLOSURE?	Yes – Next Steps	No – Next Steps
6.	Did the improper use or disclosure only include the name and the fact services were provided?	May determine low risk and not provide notification. Document decision.	Continue to next question.
7.	Did the improper use or disclosure only include the name and types of service received, identify services from a specific provider, or did the information	High risk should provide	Continue to next question.

ATTACHMENT A
RISK ASSESSMENT TOOL:
NOTE: For an acquisition, access, use or disclosure of protected health information (PHI) to constitute a breach, it must be a violation of the HIPAA Privacy Rule.

	contain specific identifiers (e.g. Social Security number, date of birth, account number, etc.) that would increase the risk of identification theft?	notification.	
8.	Did the improper use or disclosure of PHI not include the 16 limited data set identifiers in 45 CFR 164.514 (e) (2) nor the zip codes or dates of birth? Note: Consider the risk of re-identification; the higher the risk, the more likely notification should be made.	May determine low risk and not provide notification Document decision.	High risk should provide notification.
9.	Is the risk of re-identification so small that the improper use/disclosure poses no significant harm to any individuals? (e.g. limited data set included zip codes that are based on population features does not create a significant risk an individual can be identified)?	May determine low risk and not provide notification decision. Document decision.	Continue to next question.
	WAS THERE A SIGNIFICANT RISK OF HARM TO THE INDIVIDUAL AS A RESULT OF IMPROPER USE OR DISCLOSURE		
10.	Does the access, use, or disclosure pose a significant risk of financial, reputational, or other harm	High risk should report.	May determine low risk and not provide notification.
11.	Was the PHI received and/or used by anther entity governed by HIPAA Privacy and Security Rules?	May determine low risk and not provide	Continue to next question.

ATTACHMENT A
RISK ASSESSMENT TOOL:
NOTE: For an acquisition, access, use or disclosure of protected health information (PHI) to constitute a breach, it must be a violation of the HIPAA Privacy Rule.

		notification decision. Document decision.	
12.	Were immediate steps taken to mitigate the improper use of disclosure? (e. g. obtained assurance from the individual who received the PHI information will not be further used/disclosed or will be destroyed)?	May determine low risk and not provide notification decision. Document decision.	Continue to next question.
13.	Was the PHI returned prior to being accessed for an improper purpose (e.g. laptop is lost/stolen, then recovered)?	May determine low risk and not provide notification decision. Document decision. Do not delay notifications based on the hope the PHI will be recovered.	Continue to next question.

ATTACHMENT A
RISK ASSESSMENT TOOL:
NOTE: For an acquisition, access, use or disclosure of protected health information (PHI) to constitute a breach, it must be a violation of the HIPAA Privacy Rule.

14.	Does the improper use or disclosure of PHI create potential harm? Such harm may include the effect of a breach of confidentiality, the potential of blackmail, the disclosure of private facts, mental pain and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary use of the information, which could results in fear or uncertainty or the unwarranted exposure leading to humiliation or loss of self-esteem (e.g. name and address or other personal identifying information, the lost may also pose a significant risk of harm if it appears on a list of individuals receiving treatment at a mental health facility).	High risk should provide notification	May determine low risk and not provide notification. Document decision.

ATTACHMENT B

SAMPLE NOTIFICATION LETTER TO PATIENTS

[DATE]

[Name Here]

[Address 1 Here]

[Address 2 Here]

[City, State, Zip Code]

Dear [Name of Organization or Patient's Name]

The [Division Name] takes our commitment to safeguarding your personal information very seriously. We are writing to inform you of a recent incident that [may have] involved your personal identifiable information, including [delineate information here as applicable, Name, SSN, etc.]. We are sending you this letter not only to notify you of the incident, but to share information on some steps you can take to safeguard your personal information to ensure that it is fully protected if you believe it may have been compromised.

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).

[Optional-include steps they can take to mitigate the effects of the breach if applicable, for instance if a mailing was misdirected they can return unopened or opened envelopes to us.]

[Optional-if applicable]

At present, we have no indication that your personal identifying information has been compromised or misused and it is likely that you are not affected by this incident.

We recommend that you consider monitoring your financial accounts carefully for any suspicious activity and take appropriate steps to protect yourself against

potential identity theft if you believe your personal identifying information may have been compromised.

The Federal Trade Commission has a comprehensive online guide that may provide you with valuable information to protect yourself at:

http://www.ftc.gov/bcp/edu/micorsites/idtheft/consumers/compromised.html

You may also want to monitor your credit report and consider a fraud alert. A fraud alert is a consumer statement added to your credit report to alert creditors of possible fraudulent activity and request that creditors contact you prior to establishing accounts in your name. To place a fraud alert on your credit report your an contact any of the three credit reporting agencies and make such a request at no cost to you. Online links to each can be found at the website above or you can use the contact information below.

Equifax

1-800-525-6285

www.equifax.com

P.O. Box 740241

Atlanta, GA 30374-0241

Transunion

1-800-680-7289

www.transunion.com

Fraud Victim Assistance Division

P.O. Box 6790

Fullerton, CA 92834-6790

Experian

1-888-EXPERIAN (397-3742)

www.experian.com

P.O. Box 9532

Allen, TX 75013

We take seriously our role of safeguarding your personal information and using it in an appropriate manner. (If appropriate, direct blame where it lies, for example- despite our stringent policies and procedures, it appears that this is a deliberate intrusion into our records…) The (Division Name) apologizes for the stress and worry this situation has caused you. We are doing everything we can to rectify the situation.

If you have any questions please contact (reference HIPAA Privacy Officer if letter is from another sender in Division or self if Privacy Officer is signer. Provide name and phone number.)

(Insert Closing Paragraph Based on Situation)

Sincerely,

(Insert Applicable Name/Contact Information)