Mental Health Association of Columbia-Greene Counties

Breach Notification Policies and Procedures

The Mental Health Association of Columbia-Greene Counties (MHACGC) is committed to protecting consumer health information. We have an ethical and legal responsibility to protect the privacy of consumers and to maintain the confidentiality of their health information. I do hereby agree to abide by the patient confidentiality policy of the Association. To this end, we develop this policy re: Breach Notification and Reporting.

Purpose: To provide guidance for breach notification by covered entities when impermissible or unauthorized access, acquisition, use and/or disclosure of the organization's patient protected health information occurs. Breach notification will be carried out in compliance with the American Recovery and Reinvestment Act (ARRA)/Health Information Technology for Economic and Clinical Health Act (HITECH) as well as any other federal or state notification law.

The Federal Trade Commission (FTC) has published breach notification rules for vendors of personal health records as required by ARRA/HITECH. The FTC rule applies to entities not covered by HIPAA, primarily vendors of personal health records. The rule is effective September 24, 2009 with full compliance required by February 22, 2010.

Scope: The provisions of this policy apply to all MHA employees, contractors, and others, who process, store, transmit, or have access to any MHA information.

Definition of a Breach: A breach is, generally, an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information such that the use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual.

There are three exceptions to the definition of "breach." The first exception applies to the unintentional acquisition, access, or use of protected health information by a workforce member acting under the authority of a covered entity or business associate. The second exception applies to the inadvertent disclosure of protected health information from a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate. In both cases, the information cannot be further used or disclosed in a manner not permitted by the Privacy Rule. The final exception to breach applies if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information.

Breach Notification Requirements:
Following a breach of unsecured protected health information, MHACGC, will provide notification of the breach to affected individuals, the Secretary of the United States Department

of Health and Human Services (DHHS), and, in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

Procedures:

Anyone discovering a potential breach shall immediately contact the Compliance/Security Officer and utilize the **Security Incident Reporting Form within 24 hours.**

Following the discovery of a potential breach, the Security officer shall begin an investigation, conduct a risk assessment, and based on the results of the risk assessment, begin the process to notify each individual whose PHI has been, or is reasonably believed to by the organization to have been, accessed, acquired, used, or disclosed as a result of the breach. A Response Team shall be assembled consisting of the HIPAA Privacy/Security Officer, Executive Director and Division Director. This Response Team shall begin the process of determining what external notifications are required or should be made (e.g., Secretary of Department of Health & Human Services (HHS), media outlets, law enforcement officials, etc.) All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

Based on the outcome of the risk assessment (i.e. there is significant risk of harm to the individual as a result of the impermissible use or disclosure), the Agency will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
B. The type and amount of PHI involved.
C. The potential for significant risk of financial, reputational, or other harm.

Upon determination that breach notification is required, the notice shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the MHA or the business associate involved.

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

A. If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting of the timer period specified by the official; or
B. If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

The notice shall be written in plain language and must contain the following information:

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).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what the Agency is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, Web site, or postal address.

Individual Notice:

MHACGC will notify affected individuals following the discovery of a breach of unsecured protected health information. MHACGC will provide this individual notice in written form by first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If MHACGC has insufficient or out-of-date contact information for 10 or more individuals, the Agency will provide substitute individual notice by either posting the notice on the home page of our web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If MHACGC has insufficient or out-of-date contact information for fewer than 10 individuals, the Agency may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the Agency is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the Agency. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

Media Notice:

In the event that MHACGC experiences a breach affecting more than 500 residents of New York State in addition to notifying the affected individuals, MHACGC will provide notice to prominent media outlets serving the State or jurisdiction. MHACGC will provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification will be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

Notice to the Secretary:

In addition to notifying affected individuals and the media (where appropriate), MHACGC will

notify the Secretary of the United States Department of Health and Human Services (DHHS) of breaches of unsecured protected health information. The Agency will notify the Secretary by visiting the HHS web site, www.hhs.gov, and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, the Agency will notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, MHACGC may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

1. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the Agency shall maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected. The following information should be collected/logged for each breach (see attached Breach Notification Log):
    A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
    B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
    C. A description of the action taken with regard to notification of patients regarding the breach.
    D. Resolution steps taken to mitigate the breach and prevent future occurrences.

2. Business Associate Responsibilities: The business associate (BA) of the Agency that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, without unreasonable delay and in no case later than 60 calendar days after discovery of a breach, notify the organization of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide the Agency with any other available information that the Agency is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, the Agency will be responsible for notifying affected individuals, unless otherwise agreed upon by the BA to notify the affected individuals (note: it is still the burden of the Covered Entity to document this notification).

3. Workforce Training: The Agency shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within the organization.

4. Complaints: The Agency provides a process for individuals to make complaints concerning the organization's patient privacy policies and procedures or its compliance

with such policies and procedures. Individuals have the right to complain about the organization's breach notification processes. Complaints may be directed to the Compliance officer.

5. Sanctions: The Agency has a sanction policy in place and applies appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

6. Retaliation/Waiver: Agency staff may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The Agency may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

ATTACHMENTS

Examples of Breaches of Unsecured Protected Health Information

- Workforce members access the electronic health records of a celebrity who is treated within the facility.
- Stolen lost laptop containing unsecured protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Posting of patient's HIV+ health status on Facebook by a laboratory tech who carried out the diagnostic study.
- Misdirected e-mail of listing of drug seeking patients to an external group list.
- Lost flash drive containing database of patients participating in a clinical study.
- EOB (Explanation of Benefits) sent to wrong guarantor.
- Provider accessing the health record of divorced spouse for information to be used in a custody hearing.
- Workforce members accessing electronic health records for information on friends or family members out of curiosity/without a business-related purpose.
- EMT takes a cell phone picture of patient following a MVA and transmits photo to friends.
- Misfiled patient information in another patient's medical records which is brought to the organization's attention by the patient.
- Medical record copies in response to a payers request lost in mailing process and never received.
- Misdirected fax of patient records to a local grocery store instead of the requesting provider's fax.
- Briefcase containing patient medical record documents stolen from car.
- PDA with patient-identifying wound photos lost.

- Intentional and non-work related access by staff member of neighbor's information.
- Medical record documents left in public access cafeteria.

I hereby acknowledge receipt of the MHA of Columbia-Greene Counties' Policy and Procedures re: Breach Notification. I particularly understand the following concepts:

The basic definition of a Breach;

The exclusions to what constitutes a Breach;

Whom to report a breach to;

Specific examples of what constitutes a Breach.

Name:_____ Date:_____

Printed Name:_____