ADMINISTRATIVE PRACTICES MANUAL

Privacy and Security Incident and Breach Policy

PURPOSE

To establish processes and procedures to handle privacy and security incidents and breaches of Protected Health Information (PHI).

PROCEDURE

1. Any workforce member who becomes aware of a potential improper use, access, and disclosure of PHI is required to immediately:
    a. Limit any further improper use, access, and disclosure; and
    b. Report the matter to their supervisor, who should report the incident to the HIPAA Privacy & Security Officer, Dane County Risk Manager, and the designee from the Dane County Corporation Counsel Office.
2. Incident investigation. Upon receipt of incident report, the HIPAA Privacy & Security Officer will investigate the incident utilizing the **Privacy and Security Incident Report** to determine whether an incident or a breach occurred. If it determined to be an incident, follow the mitigation steps and log reporting steps in this policy. If it is determined to be a breach, follow all the procedures in the rest of this policy.

Breach Notifications

1. The HIPAA Privacy & Security Officer will immediately notify the Risk Manager of the breach to determine if notification of cyber insurance carrier is necessary.
2. A breach is treated as discovered on the first day when an incident that could be a breach is known, or if by exercising reasonable diligence would have been known, to Dane County or any BA.
3. Notifications will be completed or reviewed by the HIPAA Privacy & Security Officer.
    a. Notice must be provided to the affected client(s)/patient(s) without unreasonable delay, and in no case, no later than 60 days after the discovery of the breach by Dane County or the BA. Notice will be provided in the following form:
        i. Written notification by first-class mail to the client/patient at the last known address of the individual or by email if the client/patient has agreed to electronic communications. If Dane County knows that the client/patient is deceased, it will notify the next of kin or personal representative.
        ii. Substitute Notice:
            1. In a case where there is insufficient or out-of-date contact information for fewer than 10 clients/patients, the substitute notice may be provided by an alternative form of written notice, telephone, or other means.
            2. In the case in which there is insufficient or out-of-date contact information for 10 or more clients/patients, the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of Dane County's website, or a conspicuous notice in

media outlets in Dane County's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where individuals can learn whether their PHI may be included in the breach.

iii. If the Department determines that notification requires urgency because of possible imminent misuse of unsecured PHI, notification may be provided by telephone or other means, as appropriate in addition to the methods noted above.

b. Where less than 500 individuals are affected notifications must be made to Secretary no later than 60 days after the end of that calendar year in which the breach(es) were discovered.

c. Where 500 or more individuals are affected notifications must be made to the Secretary and the media without unreasonable delay, and in no case, no later than 60 calendar days after the discovery of the breach. For the media, notice must be provided in the form of a press release to prominent media outlets serving the geographic areas where the individuals affected by the breach likely reside.

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

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

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

   iii. Any steps the client/patient should take to protect themselves from potential harm resulting from the breach.

   iv. A brief description of what Dane County did to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.

   v. Contact information for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or a postal address.

   vi. If a law enforcement official states to Dane County that a notification would impede a criminal investigation or cause damage to national security, the Department will:

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

Mitigation

The HIPAA Privacy & Security Officer will work with appropriate staff to determine if any updates are needed to policies or procedures to reduce the risk of a similar incident or breach occurring in the

future. Mitigation efforts will take place as soon as possible after the incident or breach. If the incident or breach involves a security incident, the HIPAA Privacy & Security Officer will work Dane County Information Management or City of Madison IT (as appropriate) to mitigate the risk of future incidents or breaches.

Discipline

Employees shall not be disciplined, suspended or discharged without just cause. The principle of progressive discipline shall ordinarily be followed and shall ordinarily include an oral reprimand, written reprimand, suspension without pay, and discharge. The specific discipline imposed in any particular case will, however, depend on the facts. Discipline is documented in workforce member's individual personnel files.*

DOCUMENTATION

Dane County will maintain the documentation associated with this policy for a minimum of seven years.

ROLES & RESPONSIBILITIES

The HIPAA Privacy & Security Officer is responsible for the implementation, maintenance, and adherence to this policy.

RELATED DOCUMENTS

Definitions
*Employee Benefit Handbook

DOCUMENT VERSION HISTORY

Original: 08/2023