7001 PRIVACY INCIDENT AND BREACH NOTIFICATION

EFFECTIVE DATE: January 18, 2023
REFERENCES: 45 CFR § 164.402; 45 CFR § 164.404; 45 CFR § 164.410; 45 CFR § 164.408, 45 CFR § 164.412; 45 CFR § 164.502; 45 CFR § 164.530; A.R.S. § 12-2297

PURPOSE

This policy applies to all Division of Developmental Disabilities (Division) staff. It describes the process the Division follows when a privacy incident occurs.

DEFINITIONS

1. "Breach" means an impermissible use or disclosure of Protected Health Information (PHI) unless the Covered Entity or Business Associate, as applicable, demonstrates that there is a low probability that the PHI has been compromised. Breach excludes:
    a. Any unintentional acquisition, access, or use of PHI by the Division's Workforce or a person acting under the authority of a Covered Entity or Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further

use or disclosure in a manner not permitted under the Health Insurance Portability and Accountability Act (HIPAA).

b. Any inadvertent disclosure by a person who is authorized to access PHI at a Covered Entity or Business Associate to another person authorized to access PHI at the same Covered Entity or Business Associate, or organized health care arrangement in which the Covered Entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under HIPAA.

c. A disclosure of PHI where a Covered Entity or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2. "Business Associate" means a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a Covered Entity.

3. "Covered Entity" means health plans, health care clearinghouses, and health care providers who electronically transmit any health information in connection with transactions for which Health and Human Services (HHS) has adopted standards.
4. "Protected Health Information (PHI)" means individually identifiable health information about a member that is transmitted or maintained in any medium where the information is:
    a. Created or received by a:
        i. Health care provider,
        ii. Health plan,
        iii. Employer, or
        iv. Health care clearinghouse.
    b. Relates to the:
        i. Past, present or future physical or mental health condition of a member;
        ii. Provision of health care to a member; or
        iii. Payment for the provision of health care to a member.

PHI excludes information in:

a. Education records covered by the Family Educational Rights and Privacy Act as amended, 20 U.S.C. 1232g;
b. Records described at 20 USC 1232g(a)(4)(B)(IV);
c. Employment records held by a Covered Entity in its role as an employer; or
d. Regarding a person who has been deceased for more than 50 years.

5. "Workforce" means employees, volunteers, trainees, and other persons under the direct control of the Covered Entity, whether or not they are paid by the Covered Entity.

POLICY

A. DISCOVERY OF A BREACH

1. The Division shall treat a Breach as discovered as of the first day on which such Breach is known to the Division or, by exercising reasonable diligence, would have been known to the Division or any person, other than the person committing the Breach, who is part of the Division's Workforce or an agent of the Division.

2. Anyone in the Division's Workforce who believes that member information has been used or disclosed in any way that compromises the security or privacy of that information shall immediately notify the Division's Privacy Compliance Unit by completing the Division's online form.

3. Following the discovery of a potential Breach, the Division's Privacy Compliance Unit under the guidance of the Health Information Manager shall:

   a. Begin an investigation;

   b. Conduct a risk assessment; and

   c. Based on the results of the risk assessment, begin the process of notifying each member whose PHI has been, or is reasonably believed by the Division to have been, accessed, acquired, used, or disclosed as a result of the Breach.

B. BREACH INVESTIGATION

1. The Division's Privacy Compliance Unit shall be responsible for the:

a. Management of the Breach investigation,

b. Completion of the risk assessment,

c. Coordination with others in the Division as appropriate, and

d. Facilitation of all Breach notification processes.

2. Anyone in the Division's Workforce involved in the privacy incident shall assist the Division's Privacy Compliance Unit in the investigation and provide information as requested.

C. RISK ASSESSMENT

1. The Division shall presume an impermissible use or disclosure of PHI is a Breach unless the Division's Privacy Compliance Unit performs a risk assessment and the results demonstrate a low probability that the PHI has been compromised.
2. The Division's Privacy Compliance Unit shall complete a thorough risk assessment in good faith and the conclusions should be reasonable.
3. The Division shall include the following factors in a risk assessment:

a. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;

b. The unauthorized person who used the PHI or to whom the disclosure was made;

c. Whether the PHI was acquired or viewed; and

d. The extent to which the risk to the PHI has been mitigated.

4. The Division's Privacy Compliance Unit shall consider the factors listed above in subsection C(3), or more, to determine the overall probability that PHI has been compromised.

5. Based on the outcome of the risk assessment, the Division's Privacy Compliance Unit shall determine the need to move forward with Breach notification.

6. The Division's Privacy Compliance Unit shall document the risk assessment and the outcome of the risk assessment process.

D. NOTIFICATION

1. Notice to member

a. If a Breach of PHI has occurred, the Division's Privacy Compliance Unit shall notify the affected member(s) without unreasonable delay and in no case later than 60

days after the Breach is discovered. "Unreasonable delay" means action based on a lack of good faith or justifiable reasons for the delay.

b. The Division shall ensure the notice is written in plain language and includes the following to the extent possible:

   i. A brief description of what happened,

   ii. A description of the types of information affected,

   iii. Steps that affected members should take to protect themselves from potential harm resulting from the Breach,

   iv. A brief description of what the Division is doing to investigate, mitigate, and protect against further harm or Breaches.

c. The Division's Privacy Compliance Unit shall notify the member as follows:

   i. Unless otherwise authorized by the member, by first class mail to the member's last known address.

   ii. If agreed to in writing by the member, by email.

iii. In the form of one or more mailing as information becomes available.

d. If the Division lacks sufficient contact information to provide direct written notice by mail to the member, the Division's Privacy Compliance Unit shall use a substitute form of notice reasonably calculated to reach the member.

i. If there is insufficient contact information for fewer than 10 affected members, the Division's Privacy Compliance Unit shall provide notice by telephone, email, or other means.

ii. The Division's Privacy Compliance Unit shall document if the Division lacks sufficient information to provide any such substitute notice.

iii. If there is insufficient contact information for 10 or more affected members, the Division's Privacy Compliance Unit shall do one of the following after consulting with the Department of Economic Security (DES) Chief Privacy Officer:

1) Post a conspicuous notice on the homepage of the Division's website for 90 days with a hyperlink to the additional information required to be given to members as provided above, or

2) Publish a conspicuous notice in major print or broadcast media in the area where affected members reside. The notice shall include a toll-free number that remains active for at least 90 days so members may call to learn whether their PHI was Breached.

e. The Division's Privacy Compliance Unit shall provide immediate notice to the member by telephone or other means if they believe that PHI is subject to imminent misuse. Such notice shall be in addition to the written notice described above.

2. Notice to next of kin for a deceased member

a. If the member is deceased and the Division knows the address for the member's next of kin or personal representative, the Division's Privacy Compliance Unit shall

mail the written notice described above to the next of kin or personal representative.

b. If the Division does not know the address of the next of kin or personal representative, the Division is not required to provide any notice to the next of kin or personal representative.

c. The Division's Privacy Compliance Unit shall document the lack of sufficient contact information.

3. Notice to Health and Human Services (HHS)

a. In the event a Breach of unsecured PHI affects 500 or more of the Division's members, the Division's Privacy Compliance Unit shall coordinate with the DES Chief Privacy Officer to ensure HHS will be notified.

b. If fewer than 500 of the Division's members are affected, the Division's Privacy Compliance Unit shall maintain a log of the Breaches to be submitted to the DES Chief Privacy Officer annually.

4. Delay of notification authorized for law enforcement purposes for notices made to members, the media, HHS, and by the Division's Business Associates

   a. If a law enforcement official states in writing that a notification, notice, or posting would impede a criminal investigation or cause damage to national security and specifies the time for which a delay is required, the Division's Privacy Compliance Unit shall delay for the time period specified by the official.

   b. If a law enforcement official states orally that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, the Division's Privacy Compliance Unit shall:

      i. document the statement, including the identity of the official making the statement; and

      ii. 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.

E. MAINTENANCE OF BREACH INFORMATION

1. The Division's Privacy Compliance Unit shall maintain a process to record or log all Breaches of unsecured PHI, regardless of the number of members affected.

F. WORKFORCE TRAINING

1. The Division shall ensure that everyone in the Workforce is trained on the Division's policies and procedures with respect to PHI as necessary and appropriate to carry out their job responsibilities.
2. The Division shall ensure that everyone in the Workforce is trained how to identify and report Breaches within the Division.

G. SANCTIONS

1. The Division shall refer anyone in the Workforce who fails to comply with this policy to the Program Integrity Unit and/or Human Resources for disciplinary action.

H. RETALIATION/WAIVER

1. The Division shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any member for exercising his or her privacy rights.

2. The Division shall not require members to waive their privacy rights as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.