7001 PRIVACY INCIDENT AND BREACH NOTIFICATION

REVISION DATE: 9/17/2025
REVIEW DATES: 4/12/2025, 8/23/2024
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) Workforce. 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 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. "Member" means the same as "Client," a person receiving developmental disabilities services from the Division, as defined in A.R.S. § 36-551.
5. "Protected Health Information" or "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.

c. PHI excludes information in:

i. Education records covered by the Family Educational Rights and Privacy Act as amended, 20 U.S.C. 1232g;

ii. Records described at 20 USC 1232g(a)(4)(B)(IV);

iii. Employment records held by a Covered Entity in its role as an employer; or

iv. Regarding a person who has been deceased for more than 50 years.

6. "Unreasonable delay" means action based on a lack of good faith or justifiable reasons for the delay.

7. "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 document the date the Breach was discovered as of the first day the Breach is known by someone who is part of the Workforce excluding the individual who committed the Breach.
2. Anyone in the 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 online form on the Division's website.

B. BREACH INVESTIGATION

1. The Division shall presume an impermissible use or disclosure of PHI is a Breach until the Division's Privacy Compliance Unit determines the outcome.
2. The Division's Privacy Compliance Unit shall be responsible for the:
    a. Management of the investigation,
    b. Completion of the risk assessment tool,
    c. Coordination with the Workforce as applicable, and
    d. Breach notification.

3. The individual from the Workforce who has knowledge of the privacy incident shall assist the Division's Privacy Compliance Unit in the investigation and provide information as requested.

C. BREACH RISK ASSESSMENT

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.

D. NOTIFICATION

1. Member Notices

   a. If a Breach of PHI has occurred, the Division shall notify the affected Members without Unreasonable Delay and in no case later than 60 days after the Breach is discovered.

b. The Division shall ensure the notice includes:

   i. A brief description of what happened,

   ii. A description of the types of information affected,

   iii. Steps that 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 shall notify the Member by first class mail to the Member's last known address or by email if agreed to in writing by the Member.

d. If the Division lacks sufficient contact information to provide direct written notice by mail to the Member, the Division shall document and use a substitute form of communication to reach the Member.

   i. If there is insufficient contact information for fewer than 10 affected Members, the Division shall provide notice by telephone, email, or other

means.

ii. If there is insufficient contact information for 10 or more affected Members, the Division shall work with the Department of Economic Security (DES) Chief Privacy Officer to complete one of the following:

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.

e. The Division 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 shall mail the written notice 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 shall document the lack of sufficient contact information and that no notice was provided.

3. Notice to Health and Human Services (HHS)

   a. In the event a Breach of PHI affects 500 or more of the Division’s Members, the Division 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 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 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 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

The Division shall maintain a process to record or log all Breaches of PHI, regardless of the number of Members affected.

F. WORKFORCE TRAINING

1. The Division shall ensure that everyone in the Workforce is trained how to identify and report Breaches within the Division.
2. 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.

G. RETALIATION

1. The Division shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any Member for exercising their 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.

H. SANCTIONS

1. The Workforce shall not unlawfully disclose Personal Health Information (PHI) or Personal Identifiable Information (PII).

2. The Division shall refer anyone in the Workforce who fails to comply with this policy to the Program Integrity Unit as a referral for misconduct.
3. Misconduct of any individual in the Workforce regarding HIPAA shall be subject to disciplinary action up to and including dismissal.

Tyra Oliver

Signature of Corporate Compliance Bureau Administrator

Tyra Oliver

Name

09/05/2025

Date