3008 Electronic Monitoring

REVISION DATES: 5/13/2026, 7/9/2025
REVIEW DATES: 9/8/2025, 1/22/2024
EFFECTIVE DATE: December 27, 2023
REFERENCES: 45 CFR Part 164, A.R.S. §36-551, and A.R.S. §36.568.

Purpose

This policy outlines the Division's oversight and monitoring of Service Providers and the use of Electronic Monitoring Devices in Service Settings, day service site, employment site, developmental homes, and vehicles used for transportation.

Definitions

1. "Business Day" means 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding holidays listed in A.R.S. § 1-301.
2. "Calendar Day" means every day of the week including weekends and holidays.
3. "Common Area" means a room, including a hallway, in a Group Home, Nursing-supported Group Home, or Intermediate Care Facility, that is designed for use by multiple individuals, including Residents. Bedrooms, toileting areas, and bathing areas are excluded from this definition, regardless of the number of individuals for which the area is designed.

4. "Community Residential Setting" means a residential setting in which persons with developmental disabilities live and are provided with appropriate supervision by the Service Provider responsible for operating the residential setting, as specified in A.R.S. § 36-551.
5. "Direct Support Professional" or "DSP" means a person who is trained, certified, or licensed to provide specific Home and Community Based Services.
6. "Electronic Monitoring Device" or "Device" means video surveillance camera or audio device that is installed in a common area, including a hallway, of a group home, nursing-supported group home or intermediate care facility, and does not include an electronic, mechanical or other Device that is specifically used for the nonconsensual interception of wire or electronic communications.
7. "Electronic Monitoring Record" means the data created by an Electronic Monitoring Device.
8. "Health Insurance Portability and Accountability Act" or "HIPAA" means the Health Insurance Portability and Accountability Act; also known as the Kennedy-Kassebaum Act, signed August 21,

1996 as amended, Health Insurance Portability and Accountability Act of 1996 (HIPAA), Security, and Breach Notification Rules ("HIPAA Rules") and as reflected in the implementing regulations at 45 CFR Parts 160, 162, and 164.

9. "Member" means the same as "Client," a person receiving developmental disabilities services from the Division, as specified in A.R.S. § 36-551.

10. "Private Residence" means a residential dwelling in which the Member is currently residing, that is not an Alternative Home and Community Based Services Setting, facility, institution, or a portion of any of the following that are licensed or certified by a regulatory agency of the State as a:

    a. Health care institution under A.R.S. § 36-401.
    b. Residential care institution under A.R.S. § 36-401.
    c. Community Residential Setting under A.R.S. § 36-551, or
    d. Behavioral health facility under 9 A.A.C. 20, Articles 1, 4, 5, and 6 (A.A.C. R9.101).

11. "Private Spaces" means the Member's private bedroom, toileting area, or bathing area; bedrooms and bathrooms occupied or

utilized by more than one Member or staff are not included in this definition.

12. "Responsible Person" means an adult with a developmental disability who is a Member, or an applicant for whom no guardian has been appointed, the parent or guardian of a minor with a developmental disability, or the guardian of an adult with a developmental disability.

13. "Service Provider" means a person or agency that provides services to Members pursuant to a contract, service agreement or Qualified Vendor Agreement with the Division.

14. "Service Setting," in regards to this policy, means Group Homes, Nursing-Supported Group Homes, Behavioral-Supported Group Homes, or Intermediate Care Facilities used to provide care or supervision and vehicles associated with these services used to transport members.

Policy

A. Electronic Monitoring Device Policy, Posting, Training and Monitoring Requirements

1. The Division shall permit Service Providers to install Devices in Common Areas of the Service Setting.
2. The Division shall require Service Providers to permit the installation of Devices by a Responsible Person(s) in Common Areas of a Service Setting, once consent has been obtained from each Responsible Person.
3. The Division shall not permit Service Providers, for Devices installed by Responsible Person(s) in a Service Setting, to:
    a. Turn the Device off or on;
    b. Cover up or in any way obscure the ability of the Device to have a full view of the area chosen by the Responsible Person;
    c. Move the Device;
    d. In any other way assist or hamper the operation and use of the Device; or

e. Access data from the Device without consent from the Responsible Person who installed the Device.

4. The Division shall require the Service Provider to follow HIPAA as outlined in 45 CFR Part 164 and other applicable state and federal laws addressing confidentiality when the Responsible Person shares the data from the Devices in the Service Setting with the Service Provider.

5. The Division shall require Service Providers to maintain updated information regarding Devices in the Contract Administration System for each Service Setting within two Business Days of any change.

6. The Division shall require Service Providers to develop electronic monitoring policies for Service Settings, Day and Employment sites, and vehicle(s) used for transportation, whether the Device was installed by the Service Provider or Responsible Person.

7. The Division shall require that Service Providers electronic monitoring policies:

   a. Meet minimum requirements as outlined in the policy development tool; and

b. Are submitted to the Division for review and approval before the installation of the Device(s).

8. When the Division has approved the Service Provider's electronic monitoring policies, the Division shall require, when Devices are installed by the Service Provider, to:

a. Evaluate, monitor, and maintain a log of Devices installed by the Service Provider at least quarterly to ensure the Devices are:

i. Functioning properly;

ii. Secure from access by unauthorized personnel; and

iii. Being used in compliance with this Policy;

b. Contain the following within each log:

i. The date of the monitoring;

ii. The name of the individual who performed the monitoring; and

iii. Any deficiencies identified during the monitoring.

c. Monitor adherence to policies and promptly address non-compliance;

d. Make policies, training records, training acknowledgments, evaluations, and monitoring logs available to the Division as requested.

9. The Division shall require the Service Provider installing or using Devices in Community Residential Settings, Day and Employment sites and vehicles to:

a. Comply with federal regulations for the Security and Privacy of Protected Health Information found at 45 CFR Part 164 (HIPAA) and other applicable state and federal laws addressing confidentiality;

b. Train staff on the Service Provider's electronic monitoring policy;

c. Notify Responsible Persons in writing of Devices in use prior to the Member receiving a service or Devices will be in use; and

d. Post a sign in a conspicuous place at the main entrance, for Service Settings and Day and Employment sites, that is:

i. Legible;

ii. Clearly visible; and

iii. Printed with a size and font that is easily readable from a reasonable distance and indicates;

a. Devices are in use on the premises;

b. The days and hours of the electronic monitoring; and

c. Reference A.R.S. § 36-568 as applicable.

10. The Division shall permit the Service Provider(s) to deny the Responsible Person's request for the Service Provider to install Devices in the Service Setting.

11. The Division shall require consent to be obtained from each Responsible Person prior to installation of Devices in Common Areas of the Service Setting by the Service Provider.

12. The Division shall require the Service Providers to assist with obtaining written consent from each Responsible Person(s) upon request from the Division, whether the Device is to be installed by the Service Provider or the Responsible Person in the Service Setting, utilizing the ~~form~~ Member Consent For The Use of Electronic Monitoring Devices Installed In Group Homes (DDD-2235A) form.

13. The Division shall require the Service Provider to maintain a current copy of the signed Member Consent For The Use of Electronic Monitoring Devices Installed In Group Homes (DDD-2235A) in the Service Setting.
14. The Division and Service Providers shall follow requirements as outlined in the Division Behavior Supports Manual 200 when evaluating if a Member is required to pay restitution costs when the -Member damages Devices or associated equipment.
15. The Division shall permit Service Providers to allow the Responsible Person(s) of Members who live at the Service Setting to share the cost of installation, oversight, and monitoring of the Devices maintained by the Service Provider if the Responsible Persons agree to the arrangement.
16. The Division shall not permit the Service Provider to use Devices to substitute for DSP supervision.

B. Removal of Devices In Common Areas of the Service Setting

1. The Division shall require a Support Coordinator to obtain a signature from a Responsible Person who chooses to revoke consent to use of Devices in Common Areas, regardless of

installation by the Service Provider or a Responsible Person(s) to update the Member Consent For The Use of Electronic Monitoring Devices Installed In Group Homes (DDD-2235A) form.

2. The Division shall notify the Service Provider when a Responsible Person has revoked their consent for use of Devices.
3. The Division shall require the Service Provider, once notified that a Responsible Person(s) has revoked consent of Devices installed by the Service Provider to:
    a. Immediately stop using the Device(s);
    b. Notify all Responsible Persons in writing of the discontinuation of Devices;
    c. Remove the Device(s) within two Business Days.
4. The Division shall require the Service Provider, once notified that a Responsible Person(s) has revoked consent of Devices installed by the Responsible Person(s) in Common Areas to:
    a. Request in writing to the Responsible Person(s) to immediately stop using the Devices;
    b. Notify all Responsible Persons in writing of the discontinuation of the Devices;

c. Request the Responsible Person(s) to remove the Devices within two Business Days; and

d. Request the Responsible Person(s) makes any necessary repairs, at the time of removal, caused by the installation and removal of the Device(s).

C. Devices In Private Spaces Installed By the Responsible Persons In A Service Setting

1. The Division shall require Service Providers to allow Responsible Person(s) to install Devices in a Member's Private Space(s).
2. When a Member moves out, the Division shall require the Service Provider to ensure the Responsible Person:
   a. Removes the Device(s) from the Member's Private Spaces within two Business Days; and
   b. Makes any necessary repairs, at the time of removal, caused by the installation and removal of the Device(s).
3. The Division shall not permit the Service Provider to move a different Member into the Private Space(s) until the previously installed Device(s) have been removed.

D. Maintaining and Sharing Electronic Records

1. The Division shall require Service Providers to maintain electronic records created by Devices.

2. The Division shall require Service Providers to produce Electronic Monitoring Records upon request of the Division, law enforcement, protective agencies, and other persons and entities entitled to access public records unless otherwise prohibited by this policy or law.

3. The Division shall not permit Service Providers to share recordings containing images of more than one Member unless:
   a. Required by law enforcement, protective agencies, other persons and entities entitled to access public records, or Division contract; and
   b. The images of other Members for whom they have not received a signed release of information have been de-identified.

4. The Division shall require Service Providers with Service Settings to provide access to the Service Provider's Device records from the Service Setting where the Member receives services,

including live recordings and video feed when requested by the Responsible Person(s) unless the Electronic Monitoring Record contains evidence of a suspected criminal offense.

5. The Division shall require Service Providers to retain, store, and ensure any Electronic Monitoring Record generated by a Device, regardless of format, is accessible for a minimum of 30 Calendar Days.
6. The Division shall require the Service Provider to retain Electronic Monitoring Records for longer than 30 Calendar Days when:
    a. The Service Provider anticipates legal actions for which the records may be relevant;
    b. A court order or other legal process requires the retention of all or some of the records for a longer period of time; or
    c. A law or regulation that supersedes this Policy requires a longer period of record maintenance.
7. The Division shall require the Service Provider, prior to the disposal of any Electronic Monitoring Record, to determine if the record has been used for Member diagnosis or treatment.
8. The Division shall require the Service Provider to treat any

Electronic Monitoring Record that has been used for Member diagnosis or treatment as a medical record and maintained in compliance with the HIPAA Privacy Rule, HIPAA Security Rule, A.R.S. § 36-568.0 and any other applicable federal and state laws.

E. Private Residences

1. The Division shall not permit the Service Provider to install Devices in the Member's Private Residence.
2. The Division shall not provide oversight when the Responsible Person installs Devices in the Private Residence.
3. The Division shall not require the Service Provider to provide oversight when the Responsible Person installs Devices in the Private Residence.
4. The Division shall not permit the Service Provider or the Service Provider's staff to collect, retain, or monitor the data collected from the Device(s) installed in the Member's Private Residence.

Supplemental Information

The following items need to be considered prior to the installation of Devices:

a. The cost of the Device(s) and who is responsible for covering those costs;

b. The cost of the internet usage for the Device(s);

c. Installation, maintenance, and removal costs of the Device(s);

d. Subscription costs associated with using the Device(s);

e. Repairs, including when the Devices malfunction or are damaged by other Members or staff in the home;

f. Any other costs or responsibilities associated with the Device(s).

ARIZONA DEPARTMENT OF ECONOMIC SECURITY

Megan Taylor
Megan Taylor (May 1 1, 2026 12:3 9: 50 PDT)
Signature of Chief Network Administrator

Megan Taylor
Name

05/11/2026
Date