Critical Incident Reporting and Analysis System (CIRAS)

Manual
Division of Developmental Disabilities

Purpose of CIRAS

The Division of Developmental Disabilities (DDD) has developed the Critical Incident Reporting and Analysis System (CIRAS) to capture electronic reports from providers and Independent Service Coordination (ISC) agencies of certain incidents involving participants in the State’s Medicaid Waiver programs for individuals with developmental disabilities. The types of incidents to be reported are listed and defined below within this manual.

The DDD will use the information reported to:

- Inform ISC agencies of potential issues involving the participants whose general health and well-being the ISCs are monitoring,
- Ensure incidents are addressed appropriately, and
- Analyze potential systemic issues and take steps to enhance overall system quality.

CIRAS is not a reporting system for alleged incidents of abuse, neglect, or exploitation. Providers should continue to report alleged cases of abuse, neglect or exploitation to the Department of Human Services’ Office of the Inspector General (OIG), Department of Children and Family Services (DCFS), Department on Aging / Adult Protective Services (APS), and/or Department of Public Health as appropriate and required in accordance with the type of service involved.

CIRAS: an Overview

When a community-provider is aware that an individual has experienced a critical incident as defined below, the community provider will use CIRAS to report the incident to the DDD. The CIRAS information technology will automatically notify the appropriate ISC agency. The ISC agency will perform the appropriate follow-up and notify the Division of its findings. For some types of incidents, the Division will be included on the notification and reserves the right to have DDD staff investigate the incident.

In addition to being the primary responder to CIRAS reports, ISC agencies will also be CIRAS incident reporters. If an ISC agency becomes aware of a CIRAS incident, they will create a CIRAS report and complete the appropriate follow-up action. Being a reporter will allow ISC agencies to enter the incident in CIRAS, making the report complete and keeping the Division aware of all CIRAS incidents.
CIRAS will compile data based on the CIRAS incidents reported. The Division will have the ability to review all submitted CIRAS data while the ISC agencies will be able to review data relevant to them. Community providers will be able to review the CIRAS data relating to incidents they have reported.

**Critical Incidents Defined**

Critical Incidents are the alleged, suspected, or actual occurrence of an incident when there is reason to believe the health or safety of an individual may be adversely affected or an individual may be placed at a reasonable risk of harm. Excluded in this context from the definition of critical incident are abuse, neglect, and exploitation as defined in Part 50. The definitions of CIRAS critical incidents are below.

**Deaths:** Deaths of participants that receive services while living in their own or their family’s home. Deaths of participants residing in residential settings are not reported as part of this data process since they are reported to OIG as per Rule 50.

**Known injury:** A known injury is any injury from a known cause that is not considered abuse or neglect and that requires immobilization, casting, five or more sutures or the equivalent, second or third degree burns, dental injuries, eye injuries, or any injury that prohibits the individual from participating in routine daily tasks for more than two consecutive days.

**Law enforcement:** Any incident that results in the individual being charged, incarcerated, or arrested.

**Medical emergency:** Any incident where emergency medical intervention is required to save an individual’s life (e.g., Heimlich maneuver, cardiopulmonary resuscitation, intravenous for dehydration).

**Missing individual:** An incident that is not considered neglect and the individual cannot be located for a period of time longer than specified in the personal plan, and the individual cannot be located after actions specified in the personal plan are taken, and the individual cannot be located in a search of the immediate surrounding area; or circumstances indicate that the individual may be in immediate jeopardy; or law enforcement has been called to assist in the search for the individual.

**Peer-to-peer acts:** Acts committed by one individual against another when there is physical abuse with intent to harm; verbal abuse with intent to intimidate, harass, or humiliate, resulting in emotional distress or maladaptive behavior; any sexual abuse; any exploitation; or intentional misappropriation of property of significant value.
**Unauthorized restraint:** Any use of restraint beyond the provisions outlined in Appendix G of each Waiver.

**Unknown injury:** Any injury of an unknown cause that is not considered possible abuse or neglect and that requires treatment that only a physician, physician’s assistant, or nurse practitioner can provide.

**Unscheduled hospitalization:** Any hospital admission that is not scheduled unless the hospital admission is due to a condition that is specified in the personal plan or nursing care plan indicating the specific symptoms and criteria that require hospitalization.

**Critical Incident Tracking Data Elements**
All reporters, community providers and ISC agencies, will need to gather the following details to complete a CIRAS report.

<table>
<thead>
<tr>
<th>DATA ITEM</th>
<th>DEFINITION/COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participant’s Name (3 separate data fields for First, Last, Middle Initial)</td>
<td>Enter the name of the individual served under the Medicaid Waiver program.</td>
</tr>
<tr>
<td>Participant’s Social Security Number</td>
<td>Enter the individual’s social security number</td>
</tr>
<tr>
<td>Participant’s Date of Birth</td>
<td>Enter individual’s date of birth</td>
</tr>
<tr>
<td>Participant’s Gender</td>
<td>Enter individual’s gender</td>
</tr>
<tr>
<td>Waiver Type</td>
<td></td>
</tr>
<tr>
<td>Provider’s Name</td>
<td>Enter the name of the provider organization reporting the critical incident.</td>
</tr>
<tr>
<td>Provider’s FEIN</td>
<td>Enter reporting organization’s FEIN</td>
</tr>
<tr>
<td>Date and Time of Report (2 separate items)</td>
<td>Enter date and time incident occurred.</td>
</tr>
<tr>
<td>Name of Reporter</td>
<td>Enter the name of the individual making the report on behalf of the provider.</td>
</tr>
<tr>
<td>Date of Critical Incident</td>
<td>Enter the date the incident occurred.</td>
</tr>
<tr>
<td>Time of Critical Incident</td>
<td>Enter the time the incident occurred.</td>
</tr>
<tr>
<td>Type of Critical Incident</td>
<td>Enter type of critical incident</td>
</tr>
<tr>
<td>Location of Critical Incident</td>
<td>Choose one of the following from the drop-down menu: Residence, Day Program Site, School, Work Location, Community Outing, Family Visit, or Other.</td>
</tr>
<tr>
<td>Narrative Description of the Critical Incident</td>
<td>Provide a brief narrative of the incident including information on where the incident occurred and any staff or other individuals that were involved.</td>
</tr>
</tbody>
</table>
How ISC Agencies Enroll in CIRAS

ISC agencies must enroll in CIRAS to be able to report CIRAS incidents, receive critical incident notifications, and review CIRAS reports. The enrollment process consists of completing the documents below. Examples of each form are included as attachments at the end of this manual.

- Data Sharing Agreement
- Model Business Associate Agreement
- Data Sharing Agreement Questionnaire
- Certificate of Understanding and Acknowledgment for CIRAS
- IL444-2022 Comm. Provider/External User ID and System Access Request
- IL444-4144 Request for MIS Hardware, Software and Services

DATA SHARING AGREEMENT

DDD will supply a Data Sharing Agreement to all ISC agencies. ISC agencies will have a unique agreement number included in their enrollment packet. Once completed, it must be submitted to the Division of Developmental Disabilities (DDD) at: DHS.DDD.CIRAS@illinois.gov

MODEL BUSINESS ASSOCIATE AGREEMENT

The Model Business Associate Agreement is a standard form required by the DHS General Counsel Division to establish confidentiality standards related to the Health Insurance Portability and Accountability Act (HIPAA). Have the appropriate person sign on the last page under, “Business Associate Representative.” Return the signed form to the address included in enrollment packet. It will be kept by the DHS General Counsel Office.

DATA SHARING AGREEMENT SECURITY AND PRIVACY CONTROLS QUESTIONNAIRE

In order to ensure that baseline security and privacy controls are met, each ISC agency will need to complete the Data Sharing Agreement Security and Privacy Controls Questionnaire. The first page includes completion instructions. A Data Sharing Agreement Questionnaire will be sent to each ISC agency for initial enrollment with the individual ISC’s designated DSA number included. Upon completion forward the document to: DoIT.DHS.MISSecurity@illinois.gov

CERTIFICATE OF UNDERSTANDING AND ACKNOWLEDGEMENT FOR CIRAS

Each ISC agency is required to have the designated agency reporter(s) complete and sign this form. Additional forms are updated as designated reporters are added. The copies are
maintained at the ISC agency and are part of a security audit trail. The Certificate is available at this link:  [http://www.dhs.state.il.us/page.aspx?item=29749](http://www.dhs.state.il.us/page.aspx?item=29749).

**COMMUNITY PROVIDER/EXTERNAL USER I.D. AND SYSTEM ACCESS REQUEST (IL444-2022)**

1. ISC Providers will have to request an external user I.D. by clicking on the link below:

   [https://www2.illinois.gov/sites/doit/support/Pages/DoITIdentityManagement.aspx](https://www2.illinois.gov/sites/doit/support/Pages/DoITIdentityManagement.aspx).

   Once at the DoIT website, choose the option for Create Illinois.gov account and then follow the prompts.

   The DoIT website will generate the external user I.D.

2. Submit the IL444-2022 after the provider is assigned an external user I.D.

   The IL444-2022 is used to provide DHS system access for a variety of functions, including now, CIRAS. An IL444-2022 is included in initial enrollment packets and is available from the DHS website at:


   For ISC agencies, the following steps should be taken to complete the IL444-2022 for CIRAS access:

   **Action Requested block:** check the box for System Access Only (ID Previously Assigned);

   **Community Provider Information block:** for the IGA/DSA field, provide the ISC CIRAS designation number provided with initial enrollment packet. Complete other information fields as requested;

   **User Information block:** complete information for the designated CIRAS reporter; The IDHS ID will be the external user I.D. (for example, [John.Doe@external.illinois.gov](mailto:John.Doe@external.illinois.gov)) that was assigned to the ISC provider.

   **User System Access Requested block:** check the “Other” box and on the line provided, write “CIRAS_issa, CIRAS_user” for ISC providers. Write “CIRAS_reporter, CIRAS_user” for ISC reporters.

   **Signature block:** the designated CIRAS reporter should sign and date.

   Once completed, the form should be forwarded to:  [DHS.DDD.CIRAS@illinois.gov](mailto:DHS.DDD.CIRAS@illinois.gov). After receipt and review, an email will be sent to the user confirming access to CIRAS.
3. The IL444-4144 is used to provide access to the reports, viewed through the InfoView portal, from the Reports tab on the CIRAS site. An IL444-4144 is included in initial enrollment packets and is available from the DHS website at:

http://intranet.dhs.illinois.gov/onenetlibrary/12/documents/Forms/IL444-4144.pdf

For ISC agencies, the following steps should be taken to complete the IL444-4144 for CIRAS report access:

**Requester block:** complete the requester information.

**Recipient block:** complete the recipient information. Location Code, Project/Program and CPU Tag # can be blank. User I.D. # will be the external user I.D. (for example, John.Doe@external.illinois.gov) that was assigned to the ISC provider.

**Data processing block:** check the “Other” box.

**Narrative Description of Request block:** Write “Add the user below to the AD group shown in the item list:”

Write the external user I.D. of the ISC provider.

**Item block:** Write “DHS.G.CIRAS_ISCProviderExternalReporting”

**Justification:** Write “Required for reporting.”

Once completed and signed, the form must be emailed to DoIT.DHS.MISSecurity@illinois.gov

**How Community Providers Enroll in CIRAS**

In order to enroll in CIRAS, Community Providers will need to complete these forms:

- Certificate of Understanding and Acknowledgment for CIRAS;
- IL444-2022 Comm. Provider/External User ID and System Access Request
- IL444-4144 Request for MIS Hardware, Software and Services

**CERTIFICATE OF UNDERSTANDING AND ACKNOWLEDGEMENT FOR CIRAS**
Each Community Provider is required to have the designated agency reporter(s) complete and sign this form. The form is updated as designated reporters are added. The copies are maintained at the ISC agency and are part of a security audit trail. A copy of the form is available at: [http://www.dhs.state.il.us/page.aspx?item=29749](http://www.dhs.state.il.us/page.aspx?item=29749).

**COMMUNITY PROVIDER/EXTERNAL USER I.D. AND SYSTEM ACCESS REQUEST (IL444-2022)**

1. Community providers will have to request an external user I.D. by clicking on the link below:

   [https://www2.illinois.gov/sites/doit/support/Pages/DoITIdentityManagement.aspx](https://www2.illinois.gov/sites/doit/support/Pages/DoITIdentityManagement.aspx).

   Once at the DoIT website, choose the option for Create Illinois.gov account and then follow the prompts.

2. Submit the IL444-2022 after the provider is assigned an external user I.D.

   The IL444-2022 is used to provide DHS system access for a variety of functions, including now, CIRAS. An IL444-2022 is included in initial enrollment packets and is available from the DHS website at: [http://www.dhs.state.il.us/onenetlibrary/12/documents/Forms/IL444-2022.pdf](http://www.dhs.state.il.us/onenetlibrary/12/documents/Forms/IL444-2022.pdf).

   For Community Providers, the following steps should be taken to complete the IL444-2022 for CIRAS access:

   **Action Requested block:** check the box for System Access Only (ID Previously Assigned);

   **Community Provider Information block:** for the IGA/DSA field, leave blank. Complete other block fields as requested;

   **User information block:** complete information for the designated CIRAS reporter; The IDHS ID will be the external user I.D. (for example, [John.Doe@external.illinois.gov](mailto:John.Doe@external.illinois.gov)) that was assigned to the provider.

   **User System Access Requested block:** check the “Other” box and on the line provided, write “CIRAS_reporter, CIRAS_user.”

   **Signature block:** the designated CIRAS reporter should sign and date.

   Once completed, the form should be forwarded to: [DHS.DDD.CIRAS@illinois.gov](mailto:DHS.DDD.CIRAS@illinois.gov). After receipt and review, an email will be sent to the user confirming access to CIRAS.
3. The IL444-4144 is used to provide access to the reports, viewed through the InfoView portal, from the Reports tab on the CIRAS site. An IL444-4144 is included in initial enrollment packets and is available from the DHS website at:
   http://intranet.dhs.illinois.gov/onenetlibrary/12/documents/Forms/IL444-4144.pdf

For community agencies, the following steps should be taken to complete the IL444-4144 for CIRAS report access:

**Requester block:** complete the requester information.

**Recipient block:** complete the recipient information. Location Code, Project/Program and CPU Tag # can be blank. User I.D. # will be the external user I.D. (for example, John.Doe@external.illinois.gov) that was assigned to the provider.

**Data processing block:** check the “Other” box.

**Narrative Description of Request block:** Write “Add the user below to the AD group shown in the item list:”

Write the external user I.D. of the provider.

**Item block:** Write “DHS.G.CIRAS_ProviderExternalReporting”

**Justification:** Write “Required for reporting.”

Once completed and signed, the form must be emailed to DoIT.DHS.MISSecurity@illinois.gov

**How to Report Incidents Through CIRAS**

The beginning of this user manual contains a list of definitions and data elements that will aid in completing the Incident Report.

Community Providers and ISC agencies (The Reporter) will access CIRAS through a web link: https://circas.dhs.illinois.gov/cirassecure/ciras/

The Reporter will see the System Login screen.
After entering the User ID and password, the following screen will appear.

To report a critical incident, the Reporter will select the “Search” tab located in top left of the page. The Participant Search screen will appear.
The Reporter will enter the individual’s Social Security Number in the “Participant SSN” field and select the Search button.

If an incident has not been reported for the individual, the Participant Search Results screen will appear like this.

In situations when no results are found, the agency is required to complete a ROCS case entry on the individual in order to submit a critical incident report.
If an incident has been reported for the individual, the Participant Search Results screen will appear like this:

Upon successful entry of the individual’s SSN, the provider will verify the Provider Name, Participant Name, Gender and Date of Birth. After verifying, the provider can select a case by clicking the SSN. The Incident report will open.

All text boxes and drop down boxes on the Incident Report must be completed.
Once the mandatory fields and narrative blocks have been completed, click on the Save button. The incident will be reported to the Independent Service Coordination Agency (ISC), and when appropriate, DDD.

**How ISC Agencies Receive CIRAS Incident Notifications**

Once a provider reports an incident through CIRAS, a report alert is sent to the default email address for each ISC agency.

ISCs may change the preloaded email address or they may also add additional email addresses. Once an ISC agency receives their User ID and password, the email address changes may be made.

**What Should ISC Agencies Do Once CIRAS Notification is Received?**

ISCs will receive notification via e-mail of each incident reported. They will incorporate the report information into their next scheduled monitoring event. The notifications listed below will be flagged as priority for review within one working day following receipt of the e-mail and necessary action.

- Law Enforcement
- Missing Individual
- Unscheduled Hospitalization

ISCs will follow the Problem Resolution Protocol in determining whether and when incidents should be referred to the Division for action.

**CIRAS Data Reports for ISC Agencies and Community Providers**

Community providers and ISC agencies have the ability to review standardized reports from the CIRAS system. ISC agencies will be able to review reports for all incidents sent to them. Community providers will be able only to see the reports regarding the incidents they have reported.

Reports may be viewed from the Reports tab on the CIRAS site. The reports are viewed through the InfoView portal which requires the external user I.D. to login.


**DDD Region Staff Responsibilities for Individual Incident Review**

The system will alert Division Region staff of all incidents involving:
• Death (of individual who received services while living in their own or their family’s home)
• Law Enforcement
• Missing Individual
• Home Uninhabitable

Region staff will contact ISCs within one working day following receipt of the e-mail to ensure necessary action is underway. Region staff will continue to monitor the situation until it is resolved.

The Division will track and address all incidents referred to the Division for action by ISC agencies. Each referral will be logged and assigned by the Service Issues staff to appropriate Region staff. Region staff will follow the Problem Resolution Protocol and its time frames.

**DDD Bureau of Quality Management Staff Responsibilities for Provider Reporting Compliance**

Quality Management staff will be made aware of incidents reported regarding participants selected for the annual review sample prior to conducting on-site visits. Staff will review follow-up of the incidents reported involving sample participants. Should any unreported incidents be identified, staff will cite that as part of the review and require a plan of correction.

**DDD Bureau of Program Development and Medicaid Administration Responsibilities for Incident Reporting Compliance and Remediation**

Program Development staff will review a random sample of reported incidents selected by the OA’s Information Technology section to ensure reports are complete and that appropriate action steps were taken in response to the incident.

**Summary Reports and Trend Analysis**

Summary reports will be developed for trend analysis as follows:

- **Deaths.** This report will be sorted by Service Facilitation agency and will display all data elements, including the narrative detail. BQM and Executive Management staff will review this information on a quarterly basis.
- **Type of Critical Incident.** This report will count and display the types of critical incidents in descending order of the most frequently reported types for the previous quarter and fiscal year-to-date.
- **Time of Critical Incident.** This report will count and display the number of incidents reported in each hour of the day for the previous quarter and fiscal year-to-date.
• Date of Critical Incident. This report will count and display the number of incidents reported in each month of the year for the current fiscal year.

• Location of Critical Incident. This report will count and display the number of incidents reported at each location type for the previous quarter and fiscal year-to-date.

• Participant’s Age. This report will count and display the number of incidents reported by age groupings (e.g., 18 through 21, 22 through 29, 30 through 39, 40 through 49, 50 through 59, 60 through 69, 70 through 74, 75 through 79, 80 through 84, 85 through 89, 90 and above) for the previous quarter and fiscal year-to-date and compare that data to the number of participants by age groupings.

• Participant’s Gender. This report will count and display the number of incidents reported for males vs. females for the previous quarter and fiscal year-to-date and compare that data to the number of male vs. female participants.

• Number of Critical Incidents by Provider. This report will count and display the number of critical incidents for the previous quarter and fiscal year-to-date for each provider and compare that data to the number of participants at each provider. The report will be sorted in descending order with the providers with the highest incident rate per 100 census listed first.

• Type of Critical Incident by Provider. This report will count and display the types of critical incidents in descending order of the most frequently reported types for the previous quarter and fiscal year-to-date for each provider.

Review of Trend Reports

Reports will be produced by the system on a quarterly basis. They will be reviewed and discussed by OA and MA staff at the quarterly Quality Management Committee meetings. Additional reports may be identified and developed as needed.