CENTERS FOR MEDICARE & MEDICAID SERVICES
CENTER FOR MEDICAID & CHIP SERVICES

Using Data to Inform and Improve 1915(c) HCBS Incident Management Systems

Division of Long-Term Services and Supports

Disabled and Elderly Health Programs Group

Center for Medicaid and CHIP Services

Training Objectives

- Review federal guidance that underscores the priority of protecting waiver participant health and welfare through effective incident management.
- Explore the importance of data-driven decision-making throughout the six key elements of incident management and system-wide quality improvements.
- Provide examples of various data sources and analytic processes states may use for critical incident management and system improvements.

Incident Management and Quality Improvement Systems (QIS)

1915(c) QIS Sub-Assurances

- There are six 1915(c) waiver Quality Improvement Systems (QIS) assurances that link directly to appendices in the waiver application.
  - Appendix A: Administrative Authority
  - Appendix B: Level of Care
  - Appendix C: Qualified Providers
  - Appendix D: Service Plan
  - **Appendix G: Health and Welfare**
  - Appendix I: Financial Accountability
- Each Appendix consists of assurances and sub-assurances to measure state quality reporting discovery and remediation activities.
- States develop and report on performance measures that address each sub-assurance.

Health and Welfare in the Social Security Act § 1915(c)

Health and Welfare Assurance: The state demonstrates it has designed and implemented an effective system for assuring waiver participant health and welfare.

Sub-assurance #	Sub-assurance Description
G-i	The state demonstrates on an ongoing basis that it **identifies, addresses and seeks to prevent** instances of abuse, neglect, exploitation and unexplained death.
G-ii	The state demonstrates that **an incident management system is in place** that effectively **resolves** those incidents and **prevents** further similar incidents to the extent possible.
G-iii	The state policies and procedures for the use or prohibition of restrictive interventions (including restraints and seclusion) are followed.
G-iv	The state establishes overall health care standards and monitors those standards based on the responsibility of the service provider as stated in the approved waiver.

What is an Incident Management System?

- In the context of this presentation, an “incident management system” includes all technologies and processes implemented within a state to manage instances of abuse, neglect, exploitation, unexpected death, and other critical incidents among individuals receiving 1915(c) waiver services.
- According to the 1915(c) Technical Guide, page 239, an incident management system must be able to:
  - Assure that reports of incidents are filed.
  - Track that incidents are investigated in a timely fashion.
  - **Analyze incident data** and develop strategies to reduce the risk and likelihood of the occurrence of similar incidents in the future.

2018 Joint Report on HCBS

- The Department of Health and Human Services (HHS) Office of Inspector General (OIG), Administration for Community Living (ACL), and Office for Civil Rights (OCR) published a joint report in 2018 titled "**Ensuring Beneficiary Health and Safety in Group Homes Through State Implementation of Comprehensive Compliance Oversight**."
- The 2018 Joint Report identified four key components of health and safety oversight:
  1. "Reliable incident management and investigation processes;
  2. Audit protocols that ensure compliance with reporting, review, and response requirements;
  3. Effective mortality reviews of unexpected deaths; and
  4. Quality assurance mechanisms that ensure the delivery and fiscal integrity of appropriate community-based services."

Office of Inspector General, *Ensuring Beneficiary Health and Safety in Group Homes Through State Implementation of Comprehensive Compliance Oversight*. Available Online: https://oig.hhs.gov/reports-and-publications/featured-topics/group-homes/group-homes-joint-report.pdf

2018 CMCS Informational Bulletin

- In a 2018 Center for Medicaid and CHIP Services (CMCS) Informational Bulletin (CIB) released in response to the Joint Report, CMS expresses support for the state infrastructure outlined in the Model Practices for Incident Management and Investigation.
- Regarding trend evaluation and systematic intervention, CMS also emphasizes the importance of:
  - Accurate incident reports and information generated at the provider/individual level and communicated to the state.
  - State reviews of data for timely trend analysis.
  - State identification and analysis of emerging trends to determine whether systemic controls need improvements to prevent future incidents of abuse, neglect, and exploitation (ANE).

Center for Medicaid and CHIP Services, CMCS Informational Bulletin: *Health and Welfare of Home and Community Based Services (HCBS) Waiver Recipients*. Available Online: https://www.hhs.gov/sites/default/files/cmcs-informational-bulletin-062818.pdf

2019 Incident Management Survey

- As part of their response to implementing Joint Report recommendations and to support states in improving incident management, CMS conducted a National Incident Management System Survey in 2019.
- The survey requested responses from all states operating 1915(c) waivers.
- Survey responses spanned 101 unique incident management systems across 45 states and 237 waivers.
- The survey included sections on system processes and technologies, reporting activities, incident resolution procedures, quality improvement strategies, collaboration, training programs, and prevention strategies.
- Overall, the survey results provide insight into common incident management strengths, challenges, and strategies used among states, aligning with key elements of incident management processes.

Key Elements of Incident Management Systems

The following are six key elements that states must consider when implementing an effective incident management system:

- The incident management system does not end with tracking and trending. Systematic changes and quality improvements should follow based on trends identified in the system, which may be elicited through data analysis.

Roles of Data Throughout the Incident Management Process

- Comprehensive data allows states to design, maintain, and improve an effective incident management system.
- Data plays many roles throughout the incident management process and relates to each of the key elements of incident management, such as:

Identifying & Reporting	• Initial data collection through incident reports and other sources to identify all incidents and ensure all incidents were reported.
Triaging	• Preliminary data analysis to triage a reported incident and determine potential risk level.
Investigating	• Detailed data collection and analysis for incident investigation.
Resolving	• Follow-up data collected on provider response, corrective actions, and participant well-being to ensure incident resolution.
Tracking & Trending	• Tracking, trending, and system-level data analysis to inform necessary quality improvements to the incident management system(s).

Selected Types of Incident Data

Incident Reports

- Formal reports submitted by providers, caregivers, participants, or others to the state contain significant data regarding the type of incident, provider, and individual, at the level of detail required by the state.

Medicaid Claims

- Claims may be reviewed and cross-checked with incident reports to detect potential occurrences of fraud, waste, and abuse (FWA) and to identify unreported incidents.
- Encounter data may provide similar detail when claims not available.

FWA and EVV Information

- FWA data may be checked with incident reports to find providers who may have committed ANE.
- Information collected through electronic visit verification (EVV) systems may inform fraud, abuse, or neglect.

External Sources

- States can review other states' trend reports to identify promising practices.
- National, state, and local stakeholders can offer unique perspectives and expertise through incident-related reports or trainings.

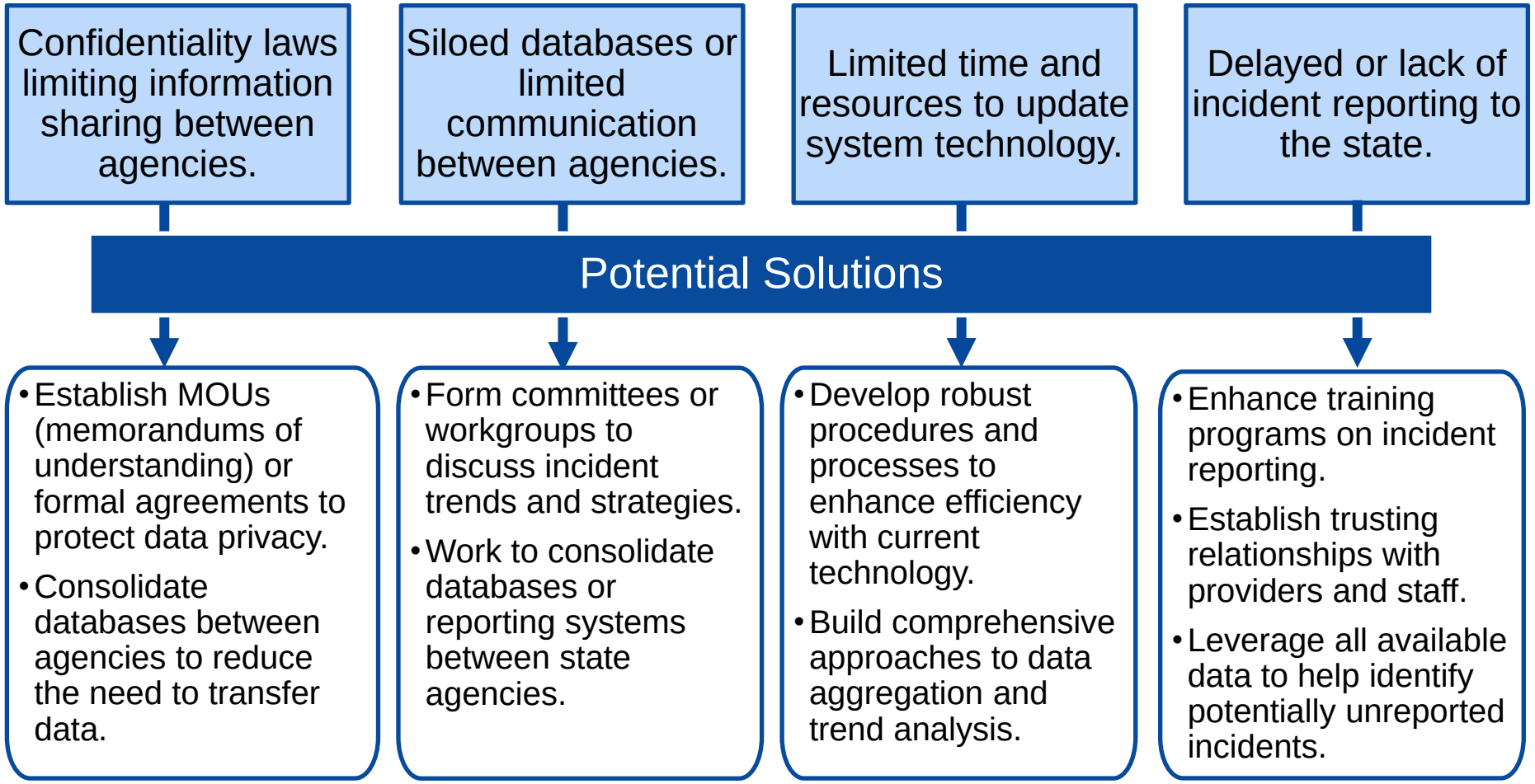
Common Challenges with Incident Data Collection and Analysis

Common challenges for states involving data collection, monitoring, and analysis include:

- Confidentiality laws limiting information sharing between agencies.
- Siloed databases or limited communication between agencies.
- Limited time and resources to update system technology.
- Delayed or lack of incident reporting to the state.

The Health Insurance Portability and Accountability Act (HIPAA) contains an exception for treatment, payment, and operations (TPO), permitting states and state agencies involved in the care of an individual to share such data while respecting all requirements for ensuring the confidentiality of the data.

Overcoming Data Challenges



Identifying & Reporting Incidents

Critical Incident Definitions

- There is no standardized, federally defined term for “incident” or “critical incident” that outlines the scope of reportable incidents.
  - Consequently, incident definitions vary across states and even across systems within the same state.
- However, according to the 1915(c) Technical Guide, page 240, states should, at a minimum, include alleged abuse, neglect, and exploitation in their Appendix G-1-b reportable incident definition(s).
- While not mandatory, there are additional incident types that states commonly include in Appendix G-1-b and are listed in the Technical Guide, such as:

Unauthorized use of restraint or restrictive interventions	Serious injuries that require medical intervention	Criminal activity or law enforcement intervention	Financial Exploitation	Medication Errors	Other incidents that involve harm or risk

Impact of Definition Scope on State Incident Reports

The inclusion of certain incident types in a state's definition of reportable and/or critical incidents directly affects the amount and types of incident data identified and reported to the state.

- States can improve comprehensive data collection and reporting by strengthening incident definitions in Appendix G-1-b.
- States can include specific incident types that extend beyond the minimum requirements of abuse, neglect, exploitation, and unexpected death (e.g., unauthorized use of restraints, financial exploitation, medication errors, and others).
- States may also want to tailor incident definitions by waiver to align with the age, disability, or other waiver-specific participant characteristics.
  - For example, states may choose to define falls as a reportable incident for waivers which serve older adults or individuals with ambulatory issues or transfer needs, but not necessarily for waivers whose target groups may not need for a focus on falls.

Example: Falls

- Falls are a frequent and harmful occurrence among HCBS populations, particularly older adults – and are the leading cause of fatal and nonfatal injury among older adults.[1]
  - In 2015, eight percent of all Medicaid spending for older adults ($9 billion total) was for medical costs to treat falls.[2]
- States may improve their ability to adequately respond to each incident, track the prevalence and recurrence of falls, and develop systematic fall prevention strategies by:
  - Explicitly defining falls as reportable incidents in Appendix G-1-b of their 1915(c) waiver applications.
  - Leveraging falls intervention guides from the Centers for Disease Control and Prevention (CDC).
  - Implementing HCBS services (e.g., home modifications) as interventions to prevent falls when a need or risk is identified.

[1] ACL. (2021). Falls Prevention: Background and Goals. Accessed from https://acl.gov/programs/health-wellness/falls-prevention
[2] National Conference of State Legislatures. (2021). Elderly Falls Prevention Legislation and Statutes. Accessed from https://www.ncsl.org/research/health/elderly-falls-prevention-legislation-and-statutes.aspx

Data to Identify Unreported Incidents

Given various barriers to reporting, incident report data is not always comprehensive. Thus, many states rely on retroactive reviews of additional data sources.

- Data from each of the following sources is key for ensuring all incidents were reported and in retroactively identifying any unreported incidents:
  - Medicaid claims data (emergency room, hospital, etc.).
  - Case notes and medical records.
  - Electronic visit verification (EVV) data.
  - Fraud, waste, and abuse (FWA) data.
- Data matching processes that compare incident reports to other incident data sources may be used to **identify unreported incidents** and inform systematic improvements for incident management reporting.

Reporting Timelines

The speed at which incidents are reported can affect timeliness of data collection, which impacts triage, investigation, analysis, and eventual remediation. Overall, reporting timelines differ slightly between states.

- According to results from the national survey, incident management systems most often required high-profile critical incidents to be reported "immediately" or within 24 hours after an incident is identified.
- Various critical incident reporting timeframes required by states include "upon discovery," "within three or four hours," "within 24 hours," and "within one business day."
- For non-critical incidents, systems often allowed providers to report within two to five business days.
- Differentiating reporting timelines based on incident severity initiates the process of triaging incidents and directly affects the availability of incident report data to the state.

Triaging & Investigating Incidents

Data Used in Incident Triage and Investigation

- During the triage and investigation steps, states often collect and analyze more data on the incident to uncover details not captured in the initial incident report (e.g., incident timing, location, root causes, and background information on involved parties).
  - These details may be pivotal for informing follow-up and remediation of the incident.
- Risk assessment tools for triaging and root cause analyses for investigating can help to gather comprehensive data on incidents and ensure the highest-risk incidents are prioritized for investigation and follow-up action.
  - **Risk Assessment**: Conducted to triage an incident and determine the associated risks of harm and immediacy of need for intervention.
  - **Root Cause Analysis**: Conducted to identify and address the systems and processes that contributed to an incident.

Methods for Sharing Incident Data

Data sharing between agencies and other stakeholders may be necessary to properly resolve incidents, analyze data trends, and develop systematic improvements.

Type of Data Sharing	Description	Example Approach
Interagency	• State agencies collaborate throughout the incident management process and may share data, reports, and lessons learned. • Agencies may include the state Medicaid agency, state operating agencies, law enforcement, protective services, licensing/credentialing agencies, and others.	Interoperable databases
State-Provider	• By exchanging data with providers and leveraging hospital claims or provider case notes data for incident analysis, state agencies can identify unreported incidents and prevent future incidents from occurring. States must be deliberative of when to share data with a provider agency that may be under investigation.	Data sharing agreements

Benefits of Joint Investigations

Joint investigations and accompanying data sharing agreements can help foster collaboration between the state Medicaid agency, Adult Protective Services (APS), Child Protective Services (CPS), law enforcement, and other state agencies.

- **Formal agreements** like memorandums of understanding often guide data sharing between APS and other state entities.
- In the 1915(c) Technical Guide, page 242, CMS notes that "…if the state's adult protective services (APS) agency has primary oversight responsibility for incident management, there should be processes whereby the APS agency regularly furnishes the Medicaid agency and/or operating agency with information about critical incidents that involve waiver participants and that **the agencies work together** to identify strategies to reduce the occurrence of critical incidents."
- By conducting **joint investigations**, states can help ensure all parties are fully informed of investigation results.

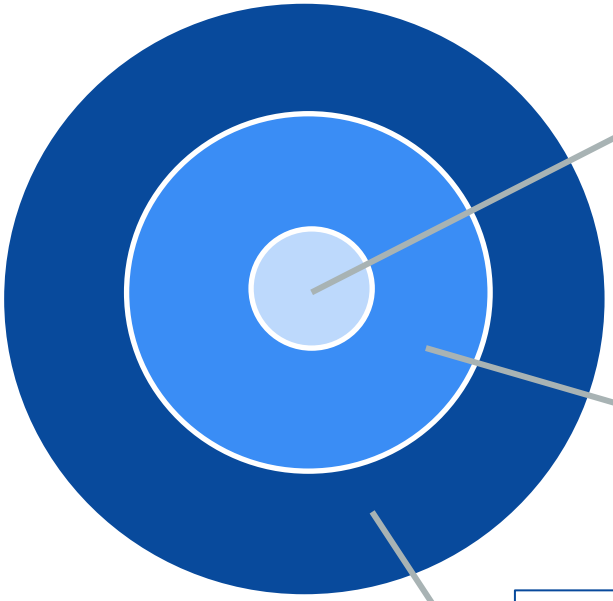
Resolving, Tracking & Trending, and Systematically Preventing Incidents

Strategies for Tracking and Trending Data

- There are several strategies states may use to collaborate with stakeholders and share relevant incident data to resolve, track, trend, and initiate system improvements, including:
  - Establishing formal partnership agreements with APS / CPS, law enforcement agencies, and other state agencies.
  - Convening multidisciplinary committees to review incident data and identify trends.
  - Leveraging shared technologies to communicate and transfer data between incident management entities.
- While stakeholder collaboration helps with tracking and trending, states can incorporate collaboration throughout all steps of the incident management process.

Multi-Level Data Analysis

Data analysis can be conducted at multiple levels.



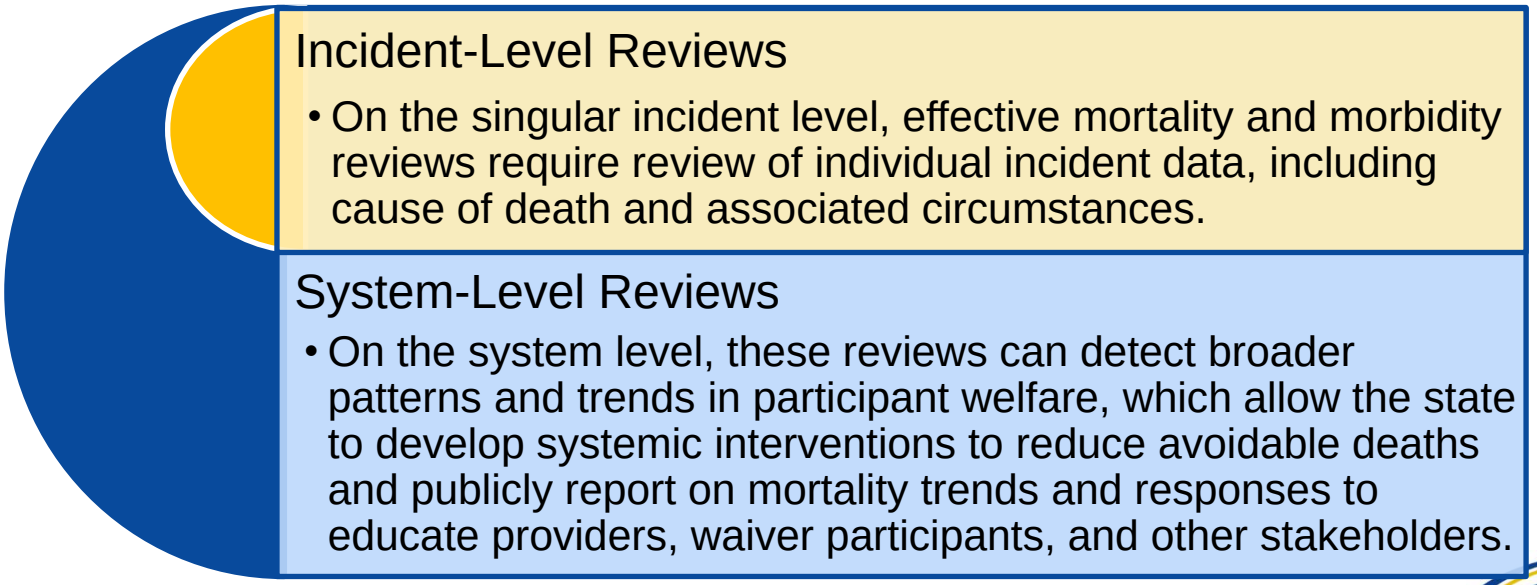
Provider/Participant: Incident data can be evaluated at the individual provider or participant level to ensure each individual incident is appropriately resolved.

Subset: States can analyze data by region, service, provider or other subset to determine any potential areas of concern and regional or program-specific outreach needed.

Statewide: States can monitor trends in data across the state, including across waiver programs and, if a state has multiple incident management systems, across systems.

Mortality and Morbidity Reviews

- Mortality and morbidity reviews are another key step in developing quality improvements for a state's incident management system.
  - "Effective mortality reviews" are listed as one of the four key compliance oversight components in the 2018 Joint Report.
  - Including morbidity studies in mortality reviews may ameliorate issues before reaching the level of death.



Summary & Takeaways

Takeaways

Accurate, comprehensive, and timely data can enable states to:

- **Improve** incident reporting practices and prevent incidents from going unreported or unresolved.
- **Ensure** all incidents are appropriately triaged, investigated, and resolved in a timely fashion.
- **Enhance** tracking and trending efforts to inform necessary quality improvements to the incident management system.

Summary of Incident Management Data Approaches

- States can use data throughout every step of the incident management process and to inform systemic quality improvements.
- Data used for incident management can come from state incident reports, other state internal sources, or external stakeholder sources.
- Collaboration between state agencies and with other stakeholders increases and improves the data collected and analyzed for incident management purposes.
- When data is tracked and analyzed at various levels, states can identify prominent incident trends and should consider how to most effectively incorporate these into systematic improvements.

Questions & Answers

For Further Information

For further information, contact:

HCBS@cms.hhs.gov