The goal for states is not to eliminate incidents, but to minimize preventable incidents from occurring. A robust incident management system (IMS) allows states to proactively respond to incidents and implement actions that reduce the risk and likelihood of future incidents.

Does DHS[1]:	Y/N	Evidence:
1. Conduct additional oversight regarding the administration and operation of their incident management systems		
2. Provide clarity and transparency on the operation and collection of information from their incident management systems		
3. Have standardized definitions for incidents		
4. Have standardized how incident reports are collected		
5. Have standards for how to respond to incidents (i.e. by providing guidelines for prioritizing what incidents need to be investigated and resolved)		
6. Have standardize requirements for annual reporting for MCOs and ICAs (so these can be combined in a report)		
7. Identify, track, trend, and mitigate preventable incidents		
8. Work with the MCOs and ICAs to implement promising practices and performance improvements that help maximize resources and improve current incident management systems		

Incident Management Promising Practices[2]

- Electronic, web-based, supporting real-time notifications and tracking
- System supports the ability to track and trend critical incidents
- Clear processes outlined for reporting, including timelines and responsibilities for individuals with access to the reporting system (e.g., State Medicaid Agency/Operating Agency staff, Adult Protective Services, etc.)
- Case manager involvement and follow-up
- Use of standardized forms to collect information
- Communication and cooperation between individuals involved in incident resolution, including between the investigative agency and State Medicaid Agency and/or Operating Agency

[1] Criteria are based on the recommendations made to states by CMS based on the findings from HHS-OIG, GAO reports, and CMS audits 2016-2018

[2] From FINDINGS FROM THE 1915(C) WAIVER INCIDENT MANAGEMENT SURVEY: INCIDENT MANAGEMENT SYSTEMS AND PROCESSES, Centers for Medicare and Medicaid Services

6 Key elements states must consider when implementing an effective IMS*:

1. Identifying the Incident
2. Reporting the Incident
3. Triaging the Incident
4. Investigating the Incident
5. Resolving the Incident
6. Tracking and Trending Incidents

* https://www.medicaid.gov/sites/default/files/2019-12/incident-management-101.pdf

Identifying the Incident	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Definition:			
Definitions are clear and understandable so stakeholders can easily identify which incidents are reportable			
Same definitions are used across all waiver populations - if not, variances accounted for			
A list of categories and examples is provided			
Clear guidelines on what should be reported			
Critical vs. Noncritical:			
Clear guidelines on what reportable incidents are critical or noncritical			
Clear guidelines on response for critical and noncritical incidents			
Clear guidelines on frequency of occurrences and impact on determination of critical vs. noncritical			
Categories of a Reportable Incident:			
There is an established list of incidents into applicable categories (abuse, neglect,			

exploitation, as well as potential or actual)			
Clear guidelines on who is responsible for identifying the incident and their roles and responsibilities			
Requirements/assurances that all possible reporters have received appropriate training to identify an incident			

Reporting the Incident	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Method of Reporting:			
Clear whether reporting methods are paper or electronic			
There are multiple avenues for reporting an incident (so all stakeholders can report, email, call center, online form, etc.)			
Recognize and account for the different costs associated with the method and volume of reporting			
Identify Information to Report:			
Information is collected in a way that will assist in the review, triage, tracking and trending of an incident			
Additional training is provided to help and encourage individuals to identify incidents			
The type of information collected from reports is standardized to expedite the review of the incident			

The type of information collected from reports is standardized to maintain transparency about what is collected and the process that occurs after the reporting through public policies and procedure guidelines, training courses, or in provider and program participant handbooks			
Key Responsibilities:			
It is clear who is responsible for reporting the incident			
Mandated reporters are identified			
All individuals who are responsible to report have access to the incident reporting system			
Timeline for Reporting:			
Clear timelines are established for reporting based on the incident severity			
Methods of reporting support the established timelines			
Communicating Reports to Others:			
There is a clear process for communicating to necessary partiers within required timelines that incidents have been reported			
If (MCOs) are managing the incident management process (such as reporting, investigating, and following up), it is clear how the state and MCO can share and monitor the reported incidents (for example: requiring a summary report of incident management in the MCO RFPs; Or regularly reviewing the reports and meeting with MCO special			

investigative units (SIUs) or other parties performing the incident management.			

Triaging the Incident	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Identify Responsibilities			
It is clear who is responsible for evaluating incident reports			
Reviewers have a firm understanding of what and how to review incident reports (e.g., conduct trainings or encourage use of a standardized checklist)			
Potential conflicts of interest are considered when selecting who reviews and/or investigates the incident			
Identify Severity			
There are criteria in place to determine and validate the severity of a reported incident			
Severity of an incident is a predictor of the type of investigation that is necessary and is classified correctly			
Clear guidelines when there is a need for follow-up communication with other affiliated agencies/individuals (APS, law enforcement, etc.) and how follow up should be conducted			
There is a review of any existing licensure or certification actions against providers involved			

Timeline for Reviewing Reports			
Timelines for reviewing and triaging the different types of reports are in place			
These timelines differentiate timelines between critical and noncritical incidents			
These timelines account for coordination with other agencies			
Determine Next Steps			
The triage process is used to determine if an investigation is necessary as a response to the incident			
Triage process is consistent with waiver language			
Follow Up			
There is guidance on the types of follow-up that must occur during the course of the investigation with the individual, family member/guardian, and provider of service based on incident severity. – Critical incidents considered high risk may require immediate, more aggressive follow-up, including: • Notifying parent, family member, or guardian; • Removing individual from place of incident; • Conducting a medical examination of the individual; • Taking licensing and certification action; and • Taking necessary lawful action			

Investigating the Incident	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Type of Investigation			
There is guidance on the method of investigation needed for the incident (e.g. desk review, onsite review)			
The type of information required by each method of investigation is clearly described (i.e. type of review, description of information to be gathered, example of an incident requiring such review)			
Timeline for Completing an Investigation			
Determine the appropriate length of an investigation. – The timeline of an investigation may differ based on severity of the incident, e.g., critical incidents may require a longer period of time due to the need for a more extensive investigation.			
Establish realistic timelines based on required activities of the investigation. – The state should consider the time commitment required for different types of investigations, e.g., interviews with stakeholders may require additional time due to availability and other circumstances.			
Establish policies and procedures to follow if an investigation extends beyond the designated timeframe			

Determine the amount of evidence necessary to take licensing/certification action.			
Identifying Responsibility			
Identify the agency(ies) responsible for conducting and resolving an investigation. – Responsibilities may vary based on how the waiver is organized. • For example, the operating agency may be responsible for the waiver, but the SMA may conduct the investigation.			
Establish clear guidelines on next steps to refer cases to law enforcement or external agencies when sufficient level of evidence standards are met for the incident. – If the severity of the incident and/or the factors involved in the incident meet the criteria for investigation by an external agency, such as law enforcement officials, coordinate with the referring agencies and understand the role for the investigator versus law enforcement official.			
Minimize conflict of interest by ensuring that the investigator is independent from waiver operations and has no financial interest from service providers.			
Staff Qualifications			
Ensure that individuals responsible for conducting the			

investigations are adequately qualified and trained. – The state should consider requiring investigators to receive a standard set of trainings so that investigators are adequately prepared to conduct different types of investigations as appropriate and fully understand related policies and procedures.			
Consider requiring individuals conducting investigations to have experience and training and/or have resources immediately available (e.g., nurse consultant, etc.) in areas specific to the incident category. – For example, require medical coding and documentation experience or in-depth understanding of such concepts for those who review and investigate any type of physical abuse requiring hospitalization. – All investigators should have knowledge of their state's Medicaid system and waiver programs.			
Safeguards for Individuals			
Establish safeguards for individuals in cases of serious allegations of abuse or hospitalization. – For example, if an individual was injured from abuse in a residential			

facility, the provider agency or state agency may remove all individuals from that setting within 24 hours.			
States should develop a registry of providers that have previously substantiated instances of abuse, neglect or exploitation, and inform individuals of the list during beneficiary selection of service providers. – If an allegation of abuse, neglect or exploitation committed by the provider agency was substantiated, then include the names of the responsible owners and not only the agency name. – Registry should reflect any license revocations and any criminal conduct that prohibits Medicaid participation in the state.			
Processes for Conducting Investigations			
Establish policies and procedures for investigators when conducting investigations.			
Define the procedures on how to gather and obtain access to other needed data sources (e.g., claims data, medical records, case management notes, etc.), particularly if it requires assistance from other state agencies or private sources			
Determine ways to keep invested individuals, families, and providers apprised of the investigation process. The state may: – Consider requiring routine			

updates for these stakeholders. – Develop a centralized system, with access given to stakeholders, so that the process and results of an investigation are transparent. NOTE: Provider rights and privacy concerns must be considered.			
Collaboration with Other State Agencies			
Identify if the investigation requires referral to other agencies or external stakeholders. The state should: – Determine a clear tracking process if fraudulent activities or other activities require involvement of law enforcement agencies, APS, CPS, Medicaid Fraud Control Unit (MFCU), or licensing/certification agencies. – Establish how findings are established and communicated for instances when inter-agency coordination is necessary for the investigation. • According to a recent OIG report, 42 out of 50 MFCUs reported that they are not informed of the outcomes of the cases after they refer the complaints to investigative authorities for non-facility-setting abuse, neglect or exploitation complaints.			
Update all relevant agencies on the ongoing investigations. – Schedule regular meetings to discuss cases. – Allow all relevant agencies to have access to a centralized			

system to view the investigation status and report summary			
Investigation Results – Burdens of Proof			
The state should determine the burden of proof threshold that substantiates an allegation. Such as: – Preponderance of evidence (over 50%); – Clear and convincing (greater than 51% and less than 75%); and – Beyond a reasonable doubt (greater than 95%).			

Resolving the Incident	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Other Resolutions from the Investigation			
Determine what types of resolutions are necessary based on findings from the investigation, including: – Corrective Action Plan (CAP); – Provider suspension/ termination after repetitive convictions of abuse, neglect or exploitation; – Inclusion in the provider abuse registry; and			

– Legal ramifications.			
Identify safeguards for ensuring that when individuals are the victims of abuse, neglect or exploitation by HCBS providers, additional services are available to: – Treat all injuries; and – Provide supports (e.g., mental health professional) for any subsequent emotional/psychological trauma.			
Determining Monitoring and CAPs			
Determine if CAPs are necessary, based on findings from the investigation. The state must: – Clearly specify the goals and objectives of the CAP. • For example, the state can require direct service providers to implement policies and procedures to clarify how they will identify potential cases of financial exploitation in a CAP. – Determine a timeline for the development and implementation of the CAP.			
Determine how to monitor the implementation of the issued CAPs. The state should identify: – Milestones to measure success; – Timelines for reporting progress of such milestones (e.g., weekly, monthly, etc.) for CAPs that require ongoing monitoring; and – Methods in which implementation will be monitored (e.g., the implementation of an electronic tracking system or phone-calls)			

Evaluate to determine if the CAP ameliorated the issues identified.			
Recouping Costs			
Determine and establish methods of recouping costs from providers if abuse, neglect or exploitation is substantiated.			
Determine if the incident requires: – The offer of a provider appeals process; – Imposition of fines; – Moratorium on admission; – Contract termination; – Decertification; and/or – Other			
A backup plan may be necessary for providing alternative provider options to waiver enrollees when providers are under investigation or a CAP for abuse, neglect or exploitation			
Communicating Results			
Determine how to share results with other relevant agencies or departments in the state. – Inter-agency communication and collaboration is integral in monitoring and preventing future occurrences.			
Identify the method of communicating the results of the investigation to relevant stakeholders. – A standard method of sharing results allows for transparency and ease of communicating the results of the investigation. – Methods of communication may include the state's intranet, letters or memos sent to stakeholders, or an electronic portal, if available.			

Tracking and Trending Incidents	DHS (Present? Y/N) If No, Add Note	MCOs (Present? Y/N) If No, Add Note	ICAs (Present? Y/N) If No, Add Note
Data Collection Priorities			
Identify the trends of interest to the state. – Determine what data is available and what needs to be collected. • Has the state committed to collecting data they aren't? • Is the state collecting data, but not trending or using for quality improvement?			
Determine what types of reports are most beneficial. – The 1915(c) Technical Guide, on page 228 suggests gathering information for system-wide oversight, including the following: • Participant and provider characteristics; • How quickly reports are reviewed, investigated, and followed-up; and • Results of the investigation			
Identify how often and who will receive the trend analysis reports (e.g., Ombudsman office, disability office, etc.). – Identifying common or reoccurring incidents will help the state prioritize what data to collect.			
Data Collection and Analysis			
Determine the types of analysis to conduct from the collected data such as: – Recurring deficiencies; – Types of incidents;			

– Types of providers/provider analysis; – Location of incidents; – Alleged perpetrators; – Investigation findings of: • Outlier incidents; • Abuse, neglect or exploitation; • ER visits/hospitalizations; – Incident resolution timelines; and – Other medical findings			
• Identify the types of data that need to be collected and tracked. <u>Sources of data:</u> • Findings and recommendations from previous investigations; • Previous unsubstantiated incidents; • Current CAPs and status of CAPs, if applicable; and • Clinical claims review. <u>Types of data to collect from the incidents include:</u> • Initial incident reports: Type of incident, Alleged perpetrator and victim, Treatment, Timeframe, and other. • Findings and recommendations of investigations; • Unsubstantiated incidents; • CAPs and status of CAPs, if applicable; and • Clinical claims review			
Determine how often data is aggregated and analyzed. – States should commit to a regular schedule for aggregating and analyzing findings and trends of the incident management system that is no less than annual. – This will require the training of staff to conduct the analysis of the			

findings and identifying trends from the incident reports.			
Tracking and Trending Incidents			
Identify areas of improvement to address adverse trends and patterns. – Page 228 of the 1915(c) Technical Guide states that “a critical element of effective oversight is the operation of data systems that support the identification of trends and patterns in the occurrence of critical incidents or events to identify opportunities for improvement and thus support the development of strategies to reduce the occurrence of incidents in the future.” – The state may need to implement corrective actions to address adverse trends and patterns.			
Consider establishing interventions that are proactive. – For example, an alert sent to all providers at the beginning of summer to remind providers to not leave individuals alone in vehicles.			
Identify performance metrics as benchmarks that guide incident management activities. The state can: – Use the Quality Improvement System (QIS) Appendix G standard requirements highlighted in the 1915(c) Technical Guide to develop metrics that are appropriate for their waiver program. – Update the CMS-			

372(s) report with any performance metrics related to incident management and Appendix G that demonstrate deficiencies.			
Regularly conduct audits of the incident management process to determine the efficacy of implemented activities. – Results of the audits should be made available to CMS at least annually. – CMS will offer technical assistance upon request.			
Interventions and Safeguards			
Use the data to identify training opportunities for stakeholders to help prevent and mitigate incidents from occurring, including: – Trainings around risk factors to help individuals identify and mitigate situations that could potentially lead to an incident. – Trainings to help state agencies address any adverse findings from trend analysis and reports. – Trainings to assess proper compliance with trend analysis findings and CAPs issued to address adverse patterns.			
Conduct outreach to stakeholders based on findings from the data, strengthening collaborations in identifying, reporting, tracking, trending, and preventing incidents. – The 1915(c) Technical Guidance provides an example on page 228, that if the state's APS agency has primary oversight			

responsibility, the state's APS agency is responsible for sharing and communicating incident information shared with the SMA and/or operating agency. – Stakeholder participation is necessary for ensuring a comprehensive approach to gathering data regarding incidents			