OSAC 2024-N-0008
Mass Fatality Incident Data Management: Best Practice Recommendation for the Medicolegal Authority

Medicolegal Death Investigation Subcommittee
Medicine Scientific Area Committee
Organization of Scientific Area Committees (OSAC) for Forensic Science

OSAC Proposed Standard

DRAFT OSAC 2024-N-0008 Mass Fatality Incident Data Management: Best Practice Recommendation for the Medicolegal Authority

Prepared by
Medicolegal Death Investigation Subcommittee
Medicine SAC
Version: 1.0
March 2024

Disclaimer:

This OSAC Proposed Standard was written by the Organization of Scientific Area Committees (OSAC) for Forensic Science following a process that includes a registry approval process. This Proposed Standard will be submitted to a standard developing organization and is subject to change.

There may be references in an OSAC Proposed Standard to other publications under development by OSAC. The information in the Proposed Standard, and underlying concepts and methodologies, may be used by the forensic-science community before the completion of such companion publications.

Any identification of commercial equipment, instruments, or materials in the Proposed Standard is not a recommendation or endorsement by the U.S. Government and does not imply that the equipment, instruments, or materials are necessarily the best available for the purpose.

Foreword

Disaster Victim Identification (DVI) necessitates the management of multiple layers of data. Regardless of the DVI data management format, incident scale, and complexity, there are overarching principles and regulations that dictate the management of data. Management of digital data introduces challenges associated with data compatibility, accuracy, reliability, and exchange that do not exist with non-digital records. The best practices presented in this document pertain to creating systems and strategies for managing digital DVI data.

These best practices are put forth by the Medicolegal Death Investigation Subcommittee Disaster Victim Identification Task Group within the OSAC. This document originated from the Scientific Working Group on Disaster Victim Identification (SWGDVI).

Mass Fatality Incident Data Management: Best Practice Recommendation for the Medicolegal Authority

1. Scope

This document identifies the best practices for DVI data management systems and reconciles them with general digital data management standards. Case management systems used in daily operations are primarily a repository for decedent data, whereas DVI data management systems are more specific to decedent identification in the context of a mass fatality incident. These recommendations include strategies for the reporting and collection of antemortem, postmortem, and scene operations data.

2. Normative References

There are no normative reference documents. Annex A and the Bibliography contain informative references.

3. Terms and Definitions

3.1. DVI

Disaster victim identification (DVI) is the process of identifying the remains of people who have died in a mass fatality incident. DVI teams are typically made up of forensic experts from a variety of disciplines, including pathologists, anthropologists, odontologists, and DNA analysts.

3.2. MFI

A mass fatality incident (MFI) is a disaster in which the number of fatalities exceeds the local resources available to find, identify, and process the victims' remains.

4. Requirements

4.1. Data Management

Data management involves the systematic collection, organization, validation (including quality assurance and control), analysis, interpretation, protection, reporting, and storing of data, to ensure reliability, accuracy, and quality. The primary goal of DVI data management is to facilitate the efficient use of antemortem, scene and recovery, postmortem, and contextual information to identify the victims of a mass fatality incident. The following is a list of data management considerations that are relevant to the DVI process:

- Data collection
- Data Ownership
- Data security/confidentiality/protection
- Data storage/retention
- Data protection
- Data verification/validation
- Data compatibility
- Data centralization/analysis
- Data reporting
- Data exchange

Each principle and its applicability to DVI data management operations are described below.

4.1.1. Data Collection

Data collection is the process of gathering discrete data elements for the purpose of identifying victims in a mass fatality incident (MFI). These elements may include information provided by the family, gathered through subsequent investigation, or collected during morgue operations. The acquisition of data is governed by protocols ensuring the integrity, reliability, and validity of the data.

These protocols should outline what data is collected, how it is collected, and where it is recorded for archival purposes. Data collection procedures should facilitate the reproduction of results, and evaluation of data reliability, integrity, and validity.

Data collection should be done in an efficient and effective way to facilitate subsequent validation, exchange, analysis, and reporting. It should support efforts to achieve identifications, enhance global compatibility and fidelity across medicolegal jurisdictions, and strengthen the accuracy and efficiency of the process.

4.1.2. Data Ownership

Ownership of DVI data rests with the medicolegal authority. Data management systems should include security protocols and end-user permissions to mitigate data loss or unauthorized access. The archival repository and access to DVI data of all types must be determined in advance of an MFI response. During a response multi-agency collaboration may necessitate the sharing of data, however once archived it is important to understand who maintains legal rights to access the data, and via what type of transmission protocols.

4.1.3. Data Security and Confidentiality

Data collected as part of a DVI response may include private or confidential non-public data, criminal history, or protected health data. Additionally, if the incident includes a criminal investigation, there will be a chain of custody considerations. All personnel conducting data entry, or with access to DVI data management systems should be credentialed. Systems access should be permission based and include auditing capabilities. When using internet-based systems, information technology protocols should protect them from unauthorized access.

Systems should inventory and store data on decedents in a discrete manner to mitigate the potential for data entry errors.

Medicolegal jurisdictions should maintain protocols to ensure data that is part of the public record is communicated first to the decedent's next of kin, and that non-public records are securely maintained in accordance with a data storage and retention strategy.

4.1.4. Data Storage and Retention

A comprehensive data storage strategy including data sharing policies and procedures can mitigate data breaches and silos that complicate the DVI process. Medicolegal authorities should consider what types of data are being stored, and the necessary space requirements for archiving it. Centralized storage of data facilitates selection, analysis, and comparison during the disaster victim identification process. Statutory requirements may require the retention of "official records" and permit the destruction of other data following a prescribed retention period. Sufficient data should be retained to reconstruct the incident response effort and validate identification methods.

4.1.5. Data Verification/Validation

The ability to make scientifically reliable identifications is dependent on the reliability of the data that is collected and maintained. Quality reviews should be performed to assess the accuracy and completeness of the data. If issues exist, they need to be addressed to prevent unrecognized erroneous data from having detrimental effects later in the process.

4.1.6. Data Compatibility

Compatibility means that data is in a format that can be exchanged with other parties. Ensuring compatibility with paper-based data is less complicated than ensuring compatibility with digital data, particularly for large scale incidents. For digital data, compatibility can be assumed if the data adheres to common digital data exchange standards.

4.1.7. Data Reporting

Data reporting involves the communication of results and conclusions drawn from the data analysis to stakeholders. The stakeholders may be the families, DVI responders, media, public, elected officials, government support agencies, or incident management. Data reporting provides the stakeholders with the information they need while ensuring the appropriate confidentiality for the victims and their families. Medicolegal authorities should work closely with other response agencies, the joint information center (JIC), and public information officers on a communication plan before reporting on DVI data.

4.1.8. Data Exchange

Data exchange addresses the policies and data format standards necessary for data compatibility to allow for the effective interchange of data between systems. The efficient and effective exchange of data facilitates the acquisition and comparison of data necessary for victim identification.

4.2. Data Management System Components

Much has been learned from the development of data management systems and their application following mass fatality incidents around the world. These lessons have led to the identification of specific capabilities that facilitate effective DVI data management. There is considerable overlap between DVI data and routine decedent case management data, although the same data may have different applications for DVI than for daily decedent case management. Commonly, when the DVI surge is over, unidentified remains may be incorporated into the daily

case management systems. DVI data should be managed in such a way that allows for communication with daily case management systems.

4.2.1. Antemortem DVI Data

Antemortem data management can be divided into the following subcategories:

- Unaccounted For Persons reporting.
- Unaccounted For Persons Manifest.
- Victim Information Center (VIC) operations.

The above subcategories are not listed in operational order, which may vary based on the incident characteristics (e.g., open versus closed population).

4.2.1.1. Unaccounted For Persons Reporting

Mass fatality incidents typically result in a surge of unaccounted for persons reports in the immediate hours following an incident. These initial reports provide the first opportunity to obtain antemortem data. The responsibility for maintaining this data may reside with law enforcement, the medicolegal authority, or another authorized entity. The data collected from these reports must be vetted to assess the likelihood of the individual being involved in the incident.

The method to gather antemortem data may differ across medicolegal jurisdictions based on incident characteristics and resource capabilities. Call centers, virtual and in-person interviews, and internet-based applications have been used to collect data in the immediate aftermath of an incident, and long term. These methods can function as stand-alone entities or be co-located within a Family Assistance Center once it is established.

Whether the data collection is conducted virtually or in person, it should be streamlined to capture the data. At a minimum, the following data should be collected:

- Name and contact information of the person making the report
- Demographic information of the unaccounted-for person
    - First and Last Name, Suffix
    - Biological Sex
    - Gender (Identifies As)
    - Race
    - Approximate Age
- Investigative contact data for the unaccounted-for person
    - Place of residence
    - Place of employment
    - Phone number(s)
    - Relationship to person making the report.
    - Social Media Handles
    - Date/Time of last contact
    - Location of last contact
    - Method of last contact

- A brief explanation of why they think the person was involved.

The process of collecting data on unaccounted-for persons should allow for internet-based reporting by family and friends. An effective internet-based reporting method should:

- Establish a centralized data collection process.
- Capture and distribute data points relevant to all involved agencies.
- Provide confirmation that the report has been received, including instructions for next steps.

Table 1 presents a list of the capabilities that constitute an unaccounted-for persons reporting function within a DVI data management system.

4.2.1.2. Unaccounted For Persons Manifest

Data collected from the call center, internet-based reporting functions, and investigative information from law enforcement should be incorporated into a single unaccounted-for persons manifest. The volume of data associated with large-scale mass fatality incidents may be difficult to manage, and efficient data management should include a strategy for effective data consolidation. For this reason, an effective DVI data management system will incorporate an unaccounted-for person manifest development function. This function will pare down unaccounted for persons data by detecting and resolving duplicate reports and verifying the status of persons reported unaccounted for. The unaccounted-for persons manifest development process requires data verification and consolidation, and the result of the process is a complete and verified electronic list of unaccounted for persons. Development of the unaccounted-for persons manifest should include list management, report verification, and VIC data management.

4.2.1.2.1. List Management Function

The list management function facilitates the detection and resolution of unaccounted-for person's data duplication. Data mining and report searching capabilities are important components of effective list management. The system should be able to accommodate these capabilities in a multi-jurisdictional, large-scale incident with multiple users and multiple locations. It should also be capable of sending automatic notifications of detailed unaccounted for person's data to all users, even in multi-jurisdictional contexts.

4.2.1.2.2. Report Verification Function

The report verification function involves the facilitated reconciliation of unaccounted for person's reports. This function should be capable of providing confirmation of unaccounted for persons status when system queries are made, information that cases can be marked as closed or completed as individuals are reported found or are identified, records searches by any data field or combination of fields, generation of unaccounted for persons statistics, and capable of converting and uploading data provided by air carriers and other entities that have a verified manifest.

Recommended specific functions within the unaccounted-for persons manifest development capability is listed in Table 2.

4.2.1.3. VIC Operations

VIC operations support DVI data management through the collection and efficient transfer of antemortem data to the medicolegal authority. This data is collected through the process of conducting antemortem interviews with family members. Utilizing the unaccounted-for persons manifest, the VIC can minimize the number of interviews being performed. VIC operations manage data collection by scheduling interviews, providing for the collection, and tracking of photos, radiographs, friction ridge prints, and dental and DNA specimens. Although the unaccounted-for persons manifest development process does not need to be completed before antemortem interviews begin, the development of the manifest drives the antemortem data collection process.

Recommended functions within the VIC/FAC component are listed in Table 3.

4.2.2. Postmortem DVI Data

Postmortem DVI data can be divided into the following subcategories:

- Scene Recovery data
- Morgue Operations data

The following are best practice recommendations for the data types that should be included under each of these headings.

4.2.2.1. Scene Recovery Data

Data from the scene of a mass fatality incident should be recorded in a format that facilitates comparison to both ante and postmortem data. A DVI data system should accommodate materials including site maps, text, photographs, video, and scanned documents. Data management strategies should include a processing for inventorying and tracking evidence, with proper chain of custody.
This process can be enhanced using barcodes or radio frequency identification devices (RFID). Ideally, the system should accommodate data from multiple:

- Recovery locations/scenes
- Concurrent incidents
- Jurisdictions with different case numbering systems

Table 4 lists recommended scene data management capabilities.

4.2.2.2. Morgue Operations Data

PM data collected in the morgue should be collected in a format that facilitates comparison to antemortem data. Ideally, a DVI data system should accommodate human remains (HR) intake,

accessioning, and processing of data collected by multiple jurisdictions. The system should be capable of generating a unique identifier that can be cross-referenced to multiple case numbering schemes. The morgue data function should also accommodate the exchange, storage, and protection of PM data, photographs, radiographs, friction ridge prints, dental, and DNA data.

Table 5 lists recommended morgue data management capabilities.

4.2.3. Victim Identification Data

The process of comparing AM, PM, and scene data to achieve identification is the core function of the DVI process. Effective data management should include reconciliation, and the ability to search fields, recognize body part duplication, and suggest exclusions. The system should accommodate data formats pertinent to scientific identification, including dental, friction ridge prints, radiographs, and DNA. The data management system should also be able to import, store, and export data from different systems.

Table 6 lists recommended identification capabilities related to data management.

4.2.4. Fatality Surveillance

Preliminary reporting of fatalities and operational progress provides metrics to gain situational awareness and develop response strategies. Reliable and efficient accounting of the preliminary number and circumstances of deaths is of particular importance in widespread multi-jurisdictional and/or protracted responses. Fatality surveillance facilitates the acquisition and consolidation of data from a variety of sources to generate estimates of incident-related fatalities. The system should have report generation capabilities for a variety of databases and jurisdictions.

Table 7 identifies the best practice capabilities of a fatality surveillance function.

4.3. DVI-Relevant Data Exchange Standards

There are existing data exchange standards that should be applied to DVI data management. The relevant exchange standards are defined below.

Tables 8 and 9 identify the appropriate ANSI/NIST-ITL standards for the various data types that are associated with a DVI investigation in tabular format.

4.3.1.1. ANSI/NIST-ITL 1-2011 500-290 Version (2015)

The document entitled ANSI/NIST Special Publication 500-290, *Data Format for the Interchange of Fingerprint, Facial and Other Biometric Information* specifically addresses the biometric data commonly used in DVI operations. The scope of this document is to define the content, format, and units of measurement for the electronic exchange of fingerprint, palm print, plantar, facial/mugshot, scar, mark and tattoo, iris, dental, DNA, and other biometric and forensic information used in the identification or verification process of an individual and is intended for use by criminal justice administrations or organizations that rely on biometric or forensic data for identification purposes.

4.3.1.2. NIEM

The National Information Exchange Model (NIEM) is designed to provide a common semantic approach for data transmission. DVI related biometric data are incorporated into the biometrics domain of NIEM, which is managed in coordination with ANSI/NIST-ITL. The NIEM Biometrics domain utilizes Extensible Markup Language (XML) Biometric Standards. It is closely linked with the ANSI/NIST-ITL organizational format and is fully conformant to the NIEM biometrics domain.

4.3.1.3. DICOM

Digital Imaging and Communications in Medicine (DICOM) is an accredited international standard published through the National Electrical Manufacturers Association (NEMA). In dental applications, medical images and associated data are both stored in the DICOM file format which can be transmitted by the ANSI/NIST-ITL standard for use in DVI operations. A DICOM reader is needed to view and interpret the data into a usable format.

4.4. Adherence to Existing Data Exchange Standards/Guidance

The best practice for medicolegal authorities or other agencies who intend to adopt or develop a DVI data management system is to abide by applicable existing data exchange standards. Adherence to these standards will facilitate compatibility between existing and future DVI solutions and allow for information sharing when applicable.

4.4.1. DVI-Relevant Data Collection Standards

Medicolegal authorities developing or acquiring a DVI data management system should be aware that relevant standards for data exchange exist, and systems should be conformed to ensure that the DVI process can effectively generate identifications. Organizations (such as the FBI or Interpol) that will receive data from a medicolegal authority require that the ANSI/NIST-ITL standard be used for data interchange.

4.4.2. Demographic Data

The demographic data collected during the unaccounted-for person report, antemortem interview, and PM examination processes should be handled using the ANSI/NIST-ITL Standard (typically in the Type 2 Record).

4.4.3. Friction Ridge Print Data

The fingerprint data collected during the antemortem interview and PM examination processes should be handled using the ANSI/NIST-ITL Standard (Types 4 and 14 Records). There are other record types in the ANSI/NIST-ITL standard to transmit other biometric data types such as palm and plantar prints (Types 15 and 19 Records).

4.4.4. Dental Data

The dental data collected during the antemortem interview and PM examination processes should be handled using the ANSI/NIST-ITL Standard (Type 12 Record).

4.4.5. Image Data

The image data, including images of the face, scars, marks, and tattoos (SMTs), and other body parts, non-dental photographs collected during the unaccounted-for person report, antemortem interview and PM examination processes should be handled using the ANSI/NIST-ITL Standard (Type 10 Record). The Type-10 record also includes the ability to transmit and describe images of suspected patterned injuries. Radiographic information and other non-visible light images are handled using the ANSI/NIST-ITL Standard (Type 22 Record).

4.4.6. DNA Data

The DNA data collected during the unaccounted-for person report, antemortem interview, and PM examination processes should be handled using the ANSI/NIST-ITL Standard (Type 18 Record).

4.4.7. Iris Collection Data

The ANSI/NIST-ITL standard includes the capability to transmit iris data when included in the biometric collection. (Type 17).

4.4.8. Non-biometric data

There are also additional records for non-biometric data, such as Type 21, that may be useful to medicolegal authorities. Type 21 includes the ability to transmit non-biometric associated images of personal effects and associated data for medical devices.

5. Tables

Table 1 – Unaccounted For Persons Reporting

Provide for publicly accessible reporting options
Standardized unaccounted for persons script for operators/staff
Just-in-time training for operators/staff
Capability to generate an unaccounted-for person's report
Accommodate a single reporter reporting multiple unaccounted for persons
Distribute data to appropriate law enforcement, medicolegal authority, and FAC
Foreign language translation
Receipt confirmation of report completion
Multi-jurisdictional data sharing
Internet based and mobile compatibility
User friendly interface
Handle multiple unaccounted for person reports
Accept reports from multiple locations during a single session
Capability to operate from multiple locations
Allow for the collection of multiple contact methods/means per case
Searchable fields including free text
Accommodate multiple incidents
All fields in database searchable
Quality assurance/Audit functions
Identify and display "like" cases (preliminary unaccounted for reconciliation)
Provide data field filtering and sorting
Data reporting functionality

Table 2 – Unaccounted for Persons Manifest Development

Data report analysis function
Ability to triage unaccounted for persons reports
Accommodate multiple concurrent users
Weighted report ranking
Data mining (searchable by specific report criteria)
Generate reports for any searchable criteria
Report consolidation
Workflow status indicator (e.g., unverified, in progress, complete)
Archival function
Convert and upload a verified manifest provided by air carriers or other entities

Table 3 – VIC Operations

Visitor management logs
Manage antemortem interview scheduling
Provide standardized antemortem interview questions to direct interview specifics
Accommodate scanned documents

Track outstanding antemortem data requests (lack of antemortem interview information; data requests from family members; data requests from external entities)
Track chains of custody
Utilize QR/ barcoding for tracking
Accommodate collection and tracking of photographs, radiographs, friction ridge prints, dental, and DNA data
Maintain log of NOK contacts
Track NOK notification preferences

Table 4 – Scene Data Function

Integrate with mapping data from other systems
Collect basic decedent location information
Accommodate the exchange/storage/protection of photography/video
Allow barcode/RFID compatible tags
Accommodate the exchange/storage/protection of biometric data
Manage multiple case number systems
HR description including handling (personnel), relocation, and transport
Site description
Manage evidence and personal effects chain of custody

Table 5 – Morgue Operations Data Function

Remains Intake/Accessioning/Tracking
Reporting of fatalities
Morgue caseload status reporting
Automated decedent identification status reporting
Capability to manage multiple remains collection points and morgue sites within a single incident
Automated tracking capability (i.e., barcode, RFID)
Generate unique morgue reference numbers
Cross reference field recovery, morgue, and MDI Authority case numbers
Case number data validation/verification
Accommodate exchange/storage/protection of PM photographs, radiographs, biometrics, DNA, dental data
Station-based morgue operations
Specimen tracking (toxicology, DNA etc.)
Support data entry for anthropology, PM examination, administrative data
Accommodate morgue tracker (escort) process
Funeral home data
Final disposition data

Table 6 – Identification Data Management Function

AM/PM Data Reconciliation
Rank-order possible matches based on available AM/PM data
Search based on any/all AM fields
Search based on any/all PM fields
Suggest exclusions based on available AM/PM data
Generate ID reports
Facilitate linking/unlinking HR by PM criteria (body part duplication etc.)
Exclusion list by identification modality
Compatibility with electronic death reporting systems (EDRS)

Table 7 – Fatality Surveillance

Data mining component that can identify deaths related to a particular incident
Data reconciliation component that eliminates duplicate and/or redundant death reports
Monitor EDRS to capture incident related deaths for temporal reporting and inclusion
Reporting capability for fatality metrics

Table 8 – Data Exchange Conformant with ANSI/NIST-ITL Standards

Facilitate Friction Ridge Print Data Exchange
Electronically collect friction ridge prints
Accommodate scanned copies of paper friction ridge prints
Transmit friction ridge print data to various databases automatically
Generate fingerprint comparison reports
Facilitate Radiographic Exchange
Accommodate digital skeletal and dental radiographs
Accommodate scanned radiograph films
Facilitate AM/PM radiograph comparison
Generate radiograph comparison reports
Facilitate DNA Data Exchange
Accommodate DNA data for various analysis types (autosomal STR, Y-STR, mitochondrial DNA, etc.)
Accommodate complex DNA matching results, including kinship analysis, generated by external software
Generate DNA matching reports

Table 9 – ANSI/NIST-ITL Standards for DVI Investigations

Type	***Applicable Standards***
Demographic data	ANSI/NIST-ITL Type 2 Record as specified in their application profiles (EBTS for FBI and DoD; INT-I for INTERPOL)
Fingerprint data	ANSI/NIST-ITL Type 4 or Type 14 records
Dental data	Dental Data ANSI/NIST-ITL record Type 12.

Dental radiographs	DICOM images transmitted through ANSI/NIST-ITL record Type 22 or scanned images directly through ANSI/NIST-ITL Type 22
Image data	Visible images and patterned injuries use ANSI/NIST-ITL Type 10; Radiographic information and other non-visible light images are handled using the ANSI/NIST-ITL Standard (Type 22 Record)
DNA data	CODIS & ANSI/NIST-ITL Type 18 record
Other biometric data	Palmprints: ANSI/NIST-ITL Type 15; footprints: ANSI/NIST-ITL Type 19; Scars/tattoos/injuries/deformities/piercings (images): ANSI/NIST-ITL Type 10
Non-biometric associated images	ANSI/NIST-ITL Type 21 for images of personal effects, and the type, make, model and serial number (if applicable) for any medical devices found in/on a person

452

Annex A
(Informative)

Bibliography

(1) Office of Research Integrity US Department of Health and Human Services. (2006). Guidelines for Responsible Data Management in Scientific Research.

(2) INTERPOL. (2009). Disaster Victim Identification Guide.

(3) U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (2005). Mass Fatality Incidents: A Guide for Human Forensic Identification.

(4) International Committee of the Red Cross. (2003). ICRC Report: The Missing and Their Families.

(5) International Committee of the Red Cross. (2009). Missing People, DNA Analysis and Identification of Human Remains: A Guide to Best Practice in Armed Conflicts and Other Situations of Armed Violence.

(6) United Nations. (1990). Guidelines for the regulation of computerized personal data files.

(7) The Organization for Economic Cooperation and Development. (1980). Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

(8) Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

(9) Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services. (2013). Electronic Biometric Transmission Specification.

(10) Department of Defense, Biometrics Identity Management Agency. (2011). Electronic Biometric Transmission Specification.

(11) National Information Exchange Model. (2009). NIEM 2.1.

(12) National Electrical Manufacturers Association, Medical Imaging and Technology Alliance, Digital Imaging and Communications in Medicine. (2011). The DICOM Standard.