(Numerical Designation)

This document has been accepted by the Academy Standards Board (ASB) for development as an American National Standard (ANS). For information about ASB and their process please refer to asb.aafs.org. This document is being made available at this stage of the process so that the forensic science community and interested stakeholders can be more fully aware of the efforts and work products of the Organization of Scientific Area Committees for Forensic Science (OSAC). The documents were prepared with input from OSAC Legal Resource Committee, Quality Infrastructure Committee, and Human Factors Committees, as well as the relevant Scientific Area Committee. The content of the documents listed below is subject to change during the standards development process within ASB, and may not represent the contents of the final published standard. All stakeholder groups or individuals, are strongly encouraged to submit technical comments on this draft document during the ASB's open comment period. Technical comments will not be accepted if submitted to the OSAC Scientific Area Committee or Subcommittees.

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

DRAFT DOCUMENT

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

1 Foreword

DVI is a complicated process that necessitates the management of multiple layers of data. Regardless of the DVI data format (i.e. paper versus digital) and incident scale and complexity, there are overarching data management principles that dictate appropriate and effective management of data. These general principles are outlined in this document. 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 the management of digital DVI data.

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

2 Acknowledgements

Editor: Jason Wiersema, Harris County Institute of Forensic Sciences

Drafting Working Group Members:
Kenneth W. Aschheim, New York City - Office of Chief Medical Examiner
Donald Bloom, Disaster Mortuary Operational Response Team
Franklin Damann, National Museum of Health and Medicine
Frank DePaolo, New York City - Office of Chief Medical Examiner
Shuala Drawdy, International Committee of the Red Cross
Elias Kontanis, National Transportation Safety Board
Rene Pape, Plass Data
Amanda Sozer, SNA International
Sharon Stanford, American Dental Association
Naeem Ullah, New York City - Office of Chief Medical Examiner
Brad Wing, National Institute of Standards and Technology
Allison Woody, Harris County Institute of Forensic Sciences

3 Table of Contents

4 Scope

This document identifies the individual *components* of effective DVI data management systems, and reconciles them with the most appropriate applicable, non-fatality management specific data management *standards*. The *components* identified in this document are best practice recommendations regarding the capabilities that a data management strategy should include given appropriate resources. DVI practitioners should adhere to the best practices identified in this document to the extent possible, practical, and appropriate. In the absence of specific guidelines for particular data types or methods of data exchange, storage, or protection, the principle, spirit, and intent of these guidelines should be met. Although the principles of data management are similar, a distinction should be made between the approach to data management for identifications made during normal daily medicolegal operations and the data management approach following a mass fatality incident. While the types of data that are managed are similar, the approach in recording and managing the data is different. Case management systems used in daily operations are primarily a repository for decedent data, whereas DVI data management systems are more involved as they also facilitate large scale and often evolving data comparisons in the interest of identification. While the general principals apply to all aspects of the data management strategy, the best practices described below apply to DVI data management information systems.

5 Terms and Definitions

Data management involves the systematic collection, organization, validation (including quality assurance and control), analysis, interpretation, protection, reporting and storing of data, to ensure that the data are reliable, accurate, and of high quality. The primary goal of DVI data management is to facilitate the efficient utilization of antemortem data, scene and recovery data, postmortem data, 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 (2):

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.

5.1
Data Collection

The strategy for the acquisition of data should involve protocols to ensure the integrity, reliability, and validity of the collected data. The local medicolegal authority should also develop a standard data format and collection protocol to maximize the efficient and effective use of data. These protocols will not involve the scientific content of DVI data but the data collection process and record format. These protocols should outline what data is collected and how it is collected and recorded. Data collection procedures should facilitate: later data reconstruction, reproduction of results, and the systematic evaluation of data reliability, integrity, and validity. It is beyond the scope of this document to address these issues, but this document will provide guidance specific to DVI data collection. The INTERPOL Disaster Victim Identification Guide (3) and the National

Institute of Justice "Mass Fatality Incidents: A Guide for Human Forensic Identification" (4) provide additional recommendations for mass fatality management and human remains identification.

5.2
Data Ownership

The appropriate repository and ownership for DVI data of all types must be determined in advance of a MFI response. Relevant questions include: who maintains legal rights to DVI data; who retains this data after a MFI response; and, who is provided access to the data and via what transmission protocols? DVI data are typically the responsibility of the local jurisdictions within which it is collected, and the responsible parties need to develop standard operating procedures to address data ownership.

5.3
Data Security/Confidentiality/Protection

Ensuring the security and confidentiality of sensitive antemortem and postmortem data collected during the DVI operations is critical to the integrity of the process. Appropriate measures should be taken to protect personal data collected and exchanged during a DVI response[1]. There are numerous sources of guidance for the protection of DVI data including the following documents:

International Committee of the Red Cross (ICRC) Report: The Missing and Their Families Section 26, 2003 (5)

ICRC Report: Missing People, DNA Analysis, and Identification of Human Remains: A Guide to Best Practice in Armed Conflicts and Other Situations of Armed Violence, Second Edition 2009 (6)

The United Nations Guidelines Concerning Computerized Personal Data Files, 1990 (7)

The Organization for Economic Cooperation and Development Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, 1980 (8)

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 1981 (9)

The guidance in these documents can be distilled to the following criteria. It is a best practice recommendation that the following criteria be included in the development and deployment of DVI data management solutions and systems:

"Personal data" means any information relating to an identified or identifiable individual, including documents collected or copied in view of contributing to the process of identification.

"Sensitive data" means data likely to give rise to unlawful or arbitrary discrimination based on racial or ethnic origin, nationality, religious or other beliefs, sexual behavior, criminal prosecutions and convictions, medical data or health information, including antemortem data, postmortem data, or DNA profiles.

Personal and sensitive data shall be collected and processed fairly and lawfully, with appropriate safeguards.

[1] The Health Insurance Portability and Accountability Act (HIPAA) restricts the disclosure of patient information and is not suspended due to an MFI. The Privacy Rule: Disclosures for Public Health Activities (45CFR 164.512(b)) (12) allows providers to share information (e.g., location, general condition or notification of death) during emergencies in order to identify, locate, and notify family members, guardians, or anyone else responsible for the individual's care. Providers are also permitted to share information to disaster relief organizations without obtaining the patient's permission if not doing so would interfere with the organization's ability to respond to the emergency. The disaster relief organizations are not covered by the HIPAA Privacy Rule and can therefore share patient information, if necessary.

The collection and processing of personal and sensitive data shall be limited to that which is necessary for the purpose identified at the time of collection, or beforehand.

Personal data should be accurate, complete, and updated as necessary for the purpose for which they are used.

Personal and sensitive data may not be used, disclosed, or transferred for purposes other than those for which they were collected without the consent of the person concerned, except if required by a substantial public interest or for the protection of the vital interests of the person concerned or of others.

Personal and sensitive data may only be transferred to third parties (as defined in the above listed documents) respecting personal data protection principles.

The de-identification of personal and sensitive data should be considered as soon as the purpose of their collection has been fulfilled. However, consideration should be given to a long term secured archiving of the data if it may be required for the benefit of the individuals, any unidentified victims, DVI organization handling the data, or if it may be essential or benefit the future performance of the relevant and appropriate tasks of the organization which collected the data.

Access to personal and sensitive data should be granted only to those individuals to whom the data relates. Provision should also be made for the right to challenge the accuracy and completeness of the data and to have them amended as appropriate.

5.4

Data Storage/Retention

A comprehensive data storage strategy is a critical component of DVI operations. Poor communication and lack of robust data sharing policies and procedures can often result in duplicate data as well as data silos that complicate the DVI process. Pertinent questions are: what is the appropriate amount of data to be stored to facilitate the appropriate reconstruction of data after the incident, and the efficient use of that data for comparison for identification. It is also important to maintain a strategy for length of time the data will be stored, and for the ultimate disposition and possible destruction of the data.

5.5

Data Protection

Protection of DVI data is critical to the integrity of any DVI operation. Medicolegal jurisdictions should maintain protocols to ensure data protection (in accordance with pertinent legal statutes) during data collection, analysis, exchange, storage, and release processes. These protocols should ensure that the data that will become public record should, when practical and possible, be communicated first to the decedent's next of kin, and that non-public records are securely maintained in accordance with a data storage/retention strategy.

5.6

Data Verification/Validation

The ability to make scientifically reliable identifications is dependent on the reliability of the data that is collected and maintained. Whenever possible, quality reviews should be performed to assess the accuracy and completeness of the data. If issues exist, they need to be addressed in order to prevent unrecognized erroneous data from having detrimental effects later in the process. Data verification is a systematic process for evaluating the performance and conformance of a set of data when compared to a set of standards to ascertain the data's completeness, correctness, and consistency using the methods and criteria defined in the project documentation. Data validation follows the data verification process and uses information from the project documentation to ascertain the usability of the data in light of its measurement quality objectives and to ensure that results obtained are scientifically defensible. Data verification and validation is used to evaluate

whether data has been generated according to specifications, to satisfy acceptance criteria, and to ensure data is appropriate and consistent with its intended use.

5.7
Data Compatibility

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

5.8
Data Centralization/Analysis

In order for the data to be useful, the data must be centralized so that the comparisons can be made. Data analysis includes the selection, evaluation, and interpretation of data as a means to develop conclusions. The appropriate analysis of DVI data, which includes the comparison and matching of the antemortem and postmortem data, is fundamental to a successful DVI operation. The SWGDVI Reconciliation and Quality Assurance guidelines address the comparison of antemortem and postmortem data in greater detail.

5.9
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 response participants, media and general public, elected officials, government support agencies, incident management, etc. It is important that DVI agencies have a strategy for data reporting that provides the stakeholders with the information they need while ensuring the appropriate confidentiality for the victims and their families.

5.10
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. This is an essential component of DVI data management, as the efficient and effective exchange of data facilitates the acquisition of data from various sources and the comparison of antemortem (AM) and postmortem (PM) data necessary for victim identification. The best practices and standards discussed in the remainder of this document will concentrate on the application of existing data exchange standards for software-based DVI data management systems.

6 Requirements

With appropriate resources, DVI data management systems can be an efficient and effective tool to facilitate the collection, validation, exchange, analysis, and reporting of DVI data. Non-DVI specific data standards have not historically been applied to DVI data, however, they are applicable to DVI data management systems. Current DVI data management standards are listed in Section 5.3 below. DVI data management systems that adhere to common standards: support individual jurisdictions' efforts to achieve identifications, support the globalization of DVI data compatibility which will benefit all medicolegal jurisdictions, and strengthen the accuracy and efficiency of identifications due to the compatibility and fidelity of recorded/reported antemortem and postmortem data to the actual antemortem and postmortem characteristics of the individual(s). The following are best practices for DVI data management.

6.1 Data Management System Components

Much has been learned from the development of data management systems[2] and their application following recent 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 daily decedent case management data, although the same data may have different applications for DVI than for decedent case management (and often when the DVI surge is over, the remaining cases, e.g. unidentified bodies and families who have not been repatriated with human remains may be incorporated with daily case management systems). As such, DVI data should be managed in such a way that allows for communication with decedent case management systems. A consensus list of the components that constitute an effective DVI data management system are outlined below. The list is divided broadly into antemortem, postmortem, victim identification, and fatality surveillance, with some main components further divided into relevant subcategories.

Antemortem DVI Data
- Disaster missing persons reporting
- Victim list development
- Victim Information Center/Family Assistance Center data management

Postmortem DVI Data
- Scene data management
- Morgue data management

Victim Identification Data

Fatality Surveillance

6.1.1 Antemortem DVI Data

Antemortem data management can be divided into the following subcategories:

Disaster missing persons reporting
Victim list development
Victim Information Center/Family Assistance Center (VIC/FAC) operations

The above listed subcategories are not listed in operational order, and the operational order may vary based on the incident characteristics (e.g. open versus closed population). The following are best practice recommendations for data that should be included under each of these headings.

6.1.1.1 Disaster Missing Persons Reporting

Mass fatality incidents typically result in a massive surge in the number of missing persons (MP) inquiries/reports in the immediate hours following an incident with which the local law enforcement and medicolegal authority must contend. These initial inquiries/reports provide the first potential access to the antemortem data required to identify decedents. Because many of these individuals may be temporarily displaced and not dead, mismanagement of this data may undermine the identification effort and create unnecessary frustration on the part of the families of the deceased and missing. For this reason an effective disaster missing persons reporting function is a critical component of a DVI data management system. The entire missing persons reporting and resolution process often involves multiple agencies and the responsibility for the maintenance of this component of DVI data management may reside with law enforcement, the medicolegal

[2] A separate document entitled "Data Management: Guidelines for Information Technologists" is planned for issuance by the SWGDV I based on guidance published in the 2013 Update to the American National Standard for Information Systems/National Institute of Standards and Technology-Information Technology Laboratory (ANSI/NIST-ITL) standard. This document will contain technical best practices for the development of a data management software application presented in a language intended for information technologists. The NIST will develop the aforementioned document in partnership with the Data Management Committee of the SWGDVI.

authority, or another authorized entity. Table 1 presents a list of the capabilities that constitute a robust disaster missing persons reporting function within a DVI data management system. The disaster missing persons reporting function is divided into Call Center/Data Collection Center and internet-based reporting functions.

6.1.1.1.1 Call Center/Data Collection Center

A Call Center/Data Collection Center involves a mechanism by which individuals are able to report a person missing. This reporting mechanism may be implemented through a call center, requiring a large phone bank and phone operators. The call center allows family and friends of missing persons to report MPs via phone to a phone bank operator who is trained to acquire the appropriate information. Alternatively, a data collection center can provide the same services when a call center is not available or practical. A data collection center is a physical location to which families of the missing can report to provide information about the MP. The data collection center may be collocated with the Family Assistance Center as needed. In both instances, reports may be collected by a party that is independent of the identification effort, who then forwards the MP information to the relevant authority for investigation. Whether the interviews are conducted by operators over the phone or by data collectors in person, they should be streamlined to effectively and efficiently capture only the following data:

Contact information from the person making the report (i.e. the reporter)
Investigative contact data for the missing person(s)
- Place of residence
- Place of employment
- Phone numbers
- Relationship to person making the report (e.g. caller primary next-of-kin, distant relative, or life partner)
- Identification type(s) and number(s) (i.e. Social Security Number, Driver's License Number)

Summary information regarding the circumstances surrounding the disappearance of the MP (ideally, this information should be recorded in such a fashion that the end users of the system would be able to obtain an assessment of the likelihood that the person reported missing was actually involved in the MFI)

The system should facilitate efficient data collection by:

Utilizing a single phone number/contact point for all MP inquiries
Providing confirmation to the reporter that a report has been received
Ensuring timely forwarding of the data pertaining to the MP and the reporter to the local law enforcement agency and medicolegal authority (these data will facilitate investigative processes and subsequent contact with next of kin [NOK])

6.1.1.1.2 Internet-based Reporting Functions

DVI data management systems ideally should also facilitate publicly accessible, internet-based reporting capabilities by the family and friends of missing persons. If possible, these systems should be compatible with mobile devices. An effective DVI data management system should:

Generate a MP report based on data collected from reporters
Allow for the recording of multiple contact methods and addresses for each reportee
Include the capability to provide a receipt verifying that a report has been filed remotely

The entire missing persons reporting and resolution process often involves multiple agencies and the responsibility for the maintenance of this component of DVI data management may reside with law enforcement, the medicolegal authority, or another authorized entity. Table 1 presents a list of the capabilities that constitute a robust disaster missing persons reporting function within a DVI data management system.

6.1.1.2 Victim List Development

The reported missing persons data collected from the Call Center/Data Collection Points, the internet-based reporting functions, the investigative information from law enforcement, and the postmortem information from the medicolegal authority should be incorporated into a single missing persons list. 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 a victim list development function. This function will pare down missing persons data by detecting and resolving duplicate reports and verifying the status of persons reported missing. The victim list development process requires data verification and consolidation, and the end result of the process is a complete and verified electronic list of missing persons. The victim list development function should include a list management function and report verification function.

6.1.1.2.1 List Management Function

The list management function facilitates the detection and resolution of missing persons data duplication. Data mining and report searching capabilities are important components of an effective list management function. 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 notification of detailed missing persons data to all users, even in multi-jurisdictional contexts.

6.1.1.2.2 Report Verification Function

The report verification function involves the facilitated reconciliation of missing persons reports. This function should be capable of providing confirmation of missing 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 missing 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 victim list development capability are listed in Table 2.

6.1.1.3 Victim Information Center/Family Assistance Center Data Management

A Family Assistance Center function is a recommended component of a DVI data management system. This component should facilitate the collection of antemortem data at the VIC as well as efficient transfer of this data to the medicolegal authority. The system should minimize the number of antemortem interviews conducted through the efficient application of the victim list process. There are two phases to this process: 1) victim list development and 2) antemortem data collection. The collection of antemortem data can only begin after the victim list development process has initiated. Although the victim list development process does not need to be completed before antemortem data collection can begin, the development of list drives the antemortem data collection process, and must be initiated first. Recommended functions within the VIC/FAC component are listed in Table 3.

6.1.2 Postmortem DVI Data

Postmortem DVI data can be divided into the following subcategories: scene data and morgue data. The following are best practice recommendations for the data types that should be included under each of these headings.

6.1.2.1 Scene Data Management

Mass fatality incident scene data is critical to the integrity of the victim identification process. It is crucial that the appropriate data are captured in a format that facilitates comparison to morgue and VIC/FAC data. A DVI data management system should accommodate all scene materials including site maps, text, photographs, video, and scanned documents. Data management strategies should include a tracking capability through systematic coding of cases for the maintenance of chain of custody for all evidence related to identification efforts and associated data. This process can be enhanced through the use of barcodes or radio frequency identification devices (RFID). Ideally, the system should have the ability to accommodate multiple recovery locations/scenes multiple concurrent incidents, multiple jurisdictions, as well as accommodate multiple jurisdictions' case number systems. Movement/transfer of possible human remains (PHR) should always be recorded. Table 4 lists recommended scene data management capabilities.

6.1.2.2 Morgue Data Management

Morgue data are also critical to the DVI process, and in the case also the appropriate data should be collected and captured in a format that facilitates comparison to antemortem data. Ideally, a DVI data management system should accommodate PHR intake, accessioning, and processing of data collection by multiple jurisdictions. The system should be capable of generating a unique identifier that can be cross-referenced to multiple case numbering schemes in cases where multiple jurisdictions are involved. The morgue data management function should also be able to accommodate the exchange, storage, and protection of postmortem photographs, radiographs, fingerprints, dental, and DNA data. Table 5 lists recommended morgue data management capabilities.

6.1.3 Victim Identification Data

The process of comparing antemortem, postmortem, scene, and contextual data to achieve identification is the core function of the DVI process. This document does not make recommendations regarding appropriate identification methods or appropriate thresholds for identification, but provides guidance regarding the applicable standards that apply to whatever method(s) a medicolegal jurisdiction employs. An effective data management system should have data reconciliation capabilities as well as allow the searching of any data fields. The system should be able to recognize body part duplication and suggest exclusions if sufficient triage data is present. The system should accommodate data formats pertinent to scientific identification, including dental, fingerprints, radiographs, and DNA. The data management system should also be able to import, store, and export these data from different systems. A DNA matching solution should be able to validate kinship. Table 6 lists recommended identification capabilities related data management.

6.1.4 Fatality Surveillance

Preliminary reporting of fatalities and operational progress are important components of a data management system as stakeholders often require metrics to gain situational awareness and to develop and maintain a response strategy. Reliable and efficient accounting of the preliminary number and circumstances of deaths related to a particular incident is an important component of mass fatality incident response planning. This is of particular importance in widespread multi-

jurisdictional and/or prolonged responses. An effective DVI data management system should incorporate a surveillance/ reporting component that facilitates the acquisition and consolidation of death reports from a variety of sources including hospitals, healthcare facilities, and law enforcement sources. This function should have a data mining capability that can utilize publicly available data to generate a tentative estimation of incident-related fatalities, and should be able to automatically detect duplications and redundancies as well as indicate whether or not a particular death is subject to the medicolegal authority's jurisdiction. The system should have automatic report generation capabilities for the medicolegal authority and should be able to identify the appropriate medicolegal geographic jurisdiction for the report. It should be able to generate fatality statistics rapidly. Table 7 identifies the best practice capabilities of a fatality surveillance function.

6.2 DVI-Relevant Data Exchange Standards

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

6.2.1 ANSI/NIST-ITL 1-2011 500-290 Version (2013)

The Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST) provides technical leadership and fosters collaborative research in a variety of technology contexts in the interest of overcoming barriers to usability, scalability, interoperability, and security in information and networks. 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 (1). 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.

Several profiles of this standard are in use by major agencies and organizations around the world (e.g. INTERPOL, NATO, Royal Canadian Mounted Police, European Union). For instance, in order to exchange fingerprint and facial data with the Federal Bureau of Investigation (FBI), the Electronic Biometric Transmission Specification (EBTS) defines which fields of the ANSI/NIST-ITL standard format are required (10). The US Department of Defense (DOD) has a slightly different version of EBTS (11). Several states, such as Florida and Texas, also have established their own profiles of the ANSI/NIST-ITL standard.

6.2.2 NIEM

The National Information Exchange Model (NIEM) is a partnership between the US Department of Justice and the Department of Homeland Security. 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 supports biometric-related services and mission-based activities, such as homeland security, national defense, border management, immigration benefits, and global law enforcement through the joint development and alignment of Extensible Markup Language (XML) Biometric Standards. In 2013, the NIEM biometrics domain was established to harmonize XML naming conventions for biometrics-related applications. It is closely linked with the ANSI/NIST-ITL organizational format and is fully conformant to the NIEM biometrics domain. (12)

6.2.3 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 information; free readers are available for this application. (13)

6.3 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. The paragraphs below identify the appropriate standards for the exchange of DVI data. Adherence to these standards will facilitate compatibility between existing and future DVI solutions.

Extensible Markup Language (XML) is the most appropriate markup language for the exchange of text based DVI data. Novel data management systems should be constructed with, or be compatible with XML. The ANSI/NIST-ITL standard is encoded in either Traditional (binary) or NIEM-conformant XML. Traditional format is what is most commonly in use, but newer systems are encouraged to switch to XML.

6.3.1 DVI-Relevant Data Collection Standards

Medicolegal authorities that are 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. The standard describes the interchange as "transactions" involving the exchange of "records"; "records" are described as defined sets of fields which may be specified by the standard to be either mandatory or optional that contain data as defined by the ANSI/NIST-ITL standard. Examples include data capture, storage, and transmission requirements such as: fingerprints shall not be captured, stored or transmitted at less than 500 pixels per inch (PPI), and that such 500 PPI images are stored in WSQ format.

Each record type in ANSI/NIST-ITL described below can contain a hash of the data contained in that record. ANSI/NIST-ITL Type 98 has additional data security for the entire transaction (objects associated with the individual). In addition, the ANSI/NIST-ITL Type 98 (Information Assurance) record provides guidance regarding data protection and security. The ANSI/NIST-ITL Type 98 record contains security information that assures the authenticity and/or integrity of a transaction. The Type 98 record applies to all non-Type 98 records.

6.3.1.1 Demographic data

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

6.3.1.2 Fingerprint data

The fingerprint data collected during the antemortem interview and postmortem examination processes should be handled using the ANSI/NIST-ITL Standard (Types 4 and 14 Records).

6.3.1.3 Dental data

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

6.3.1.4 Image data

The image data (including images of the face, scars, [needle] marks, and tattoos [SMT], and other body parts, non-dental photographs) collected during the missing person report, antemortem

interview and postmortem 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).

6.3.1.5 DNA data

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

6.3.1.6 Other biometric data

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). Although these are not commonly used there are some small databases that may be available to medicolegal authorities. The ANSI/NIST- ITL standard also includes the capability to transmit iris data (Type 17).

6.3.1.7 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.

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

7 Tables

Table 1 – Disaster Missing Persons Reporting Functions

Missing Persons Call Center/Data Collection Center
Data Collection Center facilities and/or structures (e.g. large phone bank)
Single phone number or location advertised to the public
Standardized missing persons script for operators/staff
Just-in-time training for operators/staff
Capability to generate a missing persons report for each missing person (consolidation of multiple reports for one individual)
Accommodate reports from multiple incidents
Coordinate reports from multiple locations
Accommodate a single reporter reporting multiple missing persons
Automatically forward MP data to appropriate law enforcement, medicolegal authority, and FAC
Foreign language translation capability
Allow for the collection of multiple contact methods/means per case
Provide relationship/kinship filtering (i.e. male callers only search for father, brother etc.)
Searchable fields including free text
Capability to score/grade MP reports for comparison to decedents
Receipt confirmation of report completion
Multi-jurisdictional data sharing capability
Missing Persons Internet-Based Reporting Functions
User friendly interface
Capability to handle multiple missing person reports, possibly involving incidents in multiple locations during a single session

Provide email/text confirmation of report receipt to the reporter
Accommodate up to thousands of users
Mobile device compatible

Missing Persons Database Functions

Receive data from call center, internet-based reporting, law enforcement, etc.
Capability to operate from multiple locations
Accommodate multiple incidents
All fields in database searchable
Generate activity log that records all changes to reports
Identify and display "like" cases (preliminary MP reconciliation)
Capacity to develop missing persons statistics (missing persons tallies etc.)
Ability to prioritize or triage missing persons reports

Table 2 – Victim List Development

List Management Functions

Data report analysis function

Capability to generate multi-jurisdictional fatality reports (automatic notification)
Generate possible matches to facilitate the reconciliation process
Accommodate multiple concurrent users
Weighted report ranking
Data mining capability (searchable by specific report criteria)
Generate reports for any searchable criteria
Report consolidation

Report Verification Functions

Provide confirmation of MP status
Delete records, but retains record in log format if missing person is found alive
Search any missing persons by any field
Generate missing persons statistics
Capability to convert and upload a verified manifest provided by air carriers or other entities

Table 3 – FAC Data Management

Antemortem Data Collection

Capability to search missing persons data from law enforcement agencies and hospitals (monitor patient tracking)
Provide credentialing for responders and families entering the VIC/FAC
Manage interview scheduling
Track NOK visits to VIC/FAC
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 chain of custody for items submitted by NOK
Provide standardized automated coding capability (with barcode auto-population of predetermined fields)
Facilitate mailing items to NOK
Accommodate multi-jurisdictional data transfer for large scale incidents

Accommodate collection/tracking of photographs, radiographs, fingerprints, dental, and DNA data

Antemortem Data Reporting

Generate simple reports

Report FAC interview statistics

Document the status of items submitted by NOK

Tracks NOK Notification Status/Preferences

Maintain log of NOK contacts

Track NOK notification of identification preferences (e.g. every time an identification is made, first time an identification is made, end of process, beginning and end, never)

Table 4 – Scene Data Management Function

Accommodates Scene Documentation

Integrate with mapping data or maps developed using other systems

Capability to collect basic decedent location information in multi-jurisdictional responses

Accommodate the exchange/storage/protection of scene photography/video

Include barcode/RFID compatible tags

Accommodate the exchange/storage/protection of fingerprint data

Manage multiple case number systems in case the MFI involves multiple jurisdictions

Documents Human Remains Site Information

PHR description

Site description

Manages PHR Storage at Collection Site

Document PHR handling (personnel)

Document PHR relocation

Document PHR transport

Manage unassociated evidence chain of custody

Accommodate the exchange/storage/protection of evidence photos

Tracks Personal Effects

Log associated personal effects and manages chain of custody

Log unassociated personal effects and manages chain of custody

Table 5 – Morgue Data Management Function

Automated Fatality Reporting Capability

Facilitate reporting of fatalities to multiple jurisdictions (for widespread incidents)

Facilitate general MFI status reporting to multiple jurisdictions

Facilitate automated decedent ID status reporting (notification of identification status)

Manages Human Remains Intake/Accessioning

Capability to manage multiple remains collection points or morgue locations associated with a single incident

Human remains tracking through morgue process

Automated tracking capability (i.e. barcode, RFID)

Possible Human Remains Case Numbering

Generate case numbers

Manage multiple case number systems

Identify/prevent possible case number discrepancies

Morgue Data Capability

Accommodate exchange/storage/protection of postmortem photographs

Accommodate exchange/storage/protection postmortem radiographs

Accommodate exchange/storage/protection of fingerprint data

Accommodate exchange/storage/protection of DNA sample collection information

Accommodate exchange/storage/protection of dental data

Station-Based Morgue Operations

Sample tracking (toxicology, DNA etc.)

Postmortem exam component

Supports Postmortem Exam Data Entry

Support anthropology exam data entry

Support dental postmortem exam data entry

Support pathology postmortem exam data entry

Record postmortem exam administrative data (who performed exam, etc)

Accommodate morgue tracker (escort) process

Records Final Disposition Data

Funeral home data

Disposition location (i.e. GPS coordinates)

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 antemortem fields

Search based on any/all postmortem fields

Suggest exclusions based on available AM/PM data

Facilitates ID Tracking

Generate ID reports

Accommodate exclusionary DNA samples

Facilitates Re-Association of HR Fragments

Facilitate linking/unlinking HR by PM criteria (body part duplication etc) Capability to enter in exclusions to prevent duplicate review of possible matches **Facilitates**

Fingerprint Data Exchange Conformant with ANSI/NIST-ITL Standards

Accommodate electronically gathered fingerprints in ANSI/NIST-ITL format

Accommodate scanned copies of paper fingerprints

Transmit fingerprint data to various databases automatically (if possible: e.g. FBI requires different information than INTERPOL. Even though they are both ANSI/NIST-ITL conformant, they have different 'profiles')

Generate fingerprint comparison reports

Facilitates Radiographic Exchange Conformant with ANSI/NIST-ITL Standards

Accommodate digital skeletal and dental radiographs

Accommodate scanned radiograph films

Facilitate AM/PM radiograph comparison

Generate radiograph comparison reports

Facilitates DNA Data Exchange Conformant with ANSI/NIST-ITL Standards

Capability to accommodate DNA data for various analysis types (autosomal STR, Y-STR, mitochondrial DNA, etc)

Capability to accommodate complex DNA matching results, including kinship analysis, generated by external software

Generates DNA matching reports

Facilitates Collection of Information Needed for Death Certificates

Cause and manner of death

Decedent information (e.g. name date, location, and time of death)

Table 7 – Fatality Surveillance

Data mining component that can utilize both official (hospitals and law enforcement) and publicly available (media) data to identify deaths related to a particular incident

Data reconciliation component that eliminates duplicate and/or redundant death reports

Identify medicolegal cases via detection of "official" vs. unofficial reports when possible

Generate automatic reports to all users

Rapid generation of fatality statistics

Forward reports to appropriate medicolegal jurisdiction

Generate reports regarding circumstances of death

Table 8 – 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

Annex A (informative)

Foundational Principle

DVI data management systems should be designed to facilitate the collection, storage, comparison, and reporting of missing person (antemortem) data and decedent (postmortem) data in order to achieve a scientifically reliable identification. A DVI data management strategy is a collection of processes that may include, but is not limited to, policies, procedures, data, and for most situations, the various DVI and supporting software required to support the operation. DVI data management strategies should be effective, reliable, scalable, usable, and interoperable. Ideally, this strategy should not be limited to mass fatality incident responses but should also be incorporated into daily operations. DVI data can take many forms, ranging from the use of paper records to highly complex digital data. The preferred means for managing DVI data is dependent on the scale and complexity of the incident. There exist data exchange standards that have not historically been applied to DVI data, but that are applicable and should be adhered to (e.g. National Institute of Standards and Technology [NIST] ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290 Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information)(1).

Annex B

(informative)

Bibliography

(1) National Institute of Standards and Technology. (2013). NIST Special Publication 500-290, Information Technology: American National Standard for Information Systems, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. Retrieved from http://biometrics.nist.gov/cs_links/standard/ansi_2012/ May-29-Version.pdf

(2) Office of Research Integrity US Department of Health and Human Services. (2006). Guidelines for Responsible Data Management in Scientific Research. Retrieved from http://ori.hhs.gov/education/products/clinicaltools/data.pdf

(3) INTERPOL. (2009). Disaster Victim Identification Guide. Retrieved from http://www.interpol.int/INTERPOL-expertise/Forensics/DVI-Pages/DVI-guide

(4) U.S. Department of Justice, Office of Justice Programs, National Institute of Justice. (2005). Mass Fatality Incidents: A Guide for Human Forensic Identification. Retrieved from https://www.ncjrs.gov/pdffiles1/nij/199758.pdf

(5) International Committee of the Red Cross. (2003). ICRC Report: The Missing and Their Families. Retrieved from http://www.icrc.org/eng/assets/files/other/icrc_themissing_012003_en_10.pdf

(6) 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. Retrieved from http://www.icrc.org/eng/assets/files/other/icrc_002_4010.pdf

(7) United Nations. (1990). Guidelines for the regulation of computerized personal data files. Retrieved from http://www.un.org/documents/ga/res/45/a45r095.htm

(8) The Organization for Economic Cooperation and Development. (1980). Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

(9) Council of Europe. (1981). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Retrieved from http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm

(10) Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services. (2013). Electronic Biometric Transmission Specification. Retrieved from https://www.fbibiospecs.org/docs/Master%20EBTS%20v10%20-%20FINAL%2020130702.pdf

(11) Department of Defense, Biometrics Identity Management Agency. (2011). Electronic Biometric Transmission Specification. Retrieved from http://www.biometrics.dod.mil/Files/Documents/Standards/DoD_EBTS_v3_0.pdf

(12) National Information Exchange Model. (2009). NIEM 2.1. Retrieved from https://www.niem.gov/technical/Pages/current-release.aspx

(13) National Electrical Manufacturers Association, Medical Imaging and Technology Alliance, Digital Imaging and Communications in Medicine. (2011). The DICOM Standard. Retrieved from http://medical.nema.org/standard.html