PHIN Preparedness

(DRAFT for discussion)

OUTBREAK MANAGEMENT FUNCTIONAL REQUIREMENTS AND PROCESS FLOWS

Version 0.1 Draft

05/19/2004

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1	Jennifer Johnson	05/19/2004	<name>	<mm/dd/yy>	Initial draft
2					
3					
4					
5					

TABLE OF CONTENTS

TABLE OF FIGURES

ERROR! NO TABLE OF FIGURES ENTRIES FOUND.

1 INTRODUCTION

This document describes functional requirements and general workflow for systems implemented to participate in Outbreak Management. Outbreak Management (OM) is the high-level activity intended to support the needs of investigation, monitoring, management, analysis, and reporting of a public health event or act of bioterrorism. A system supporting OM should aid in the collection and analysis of data in effort to identify and contain the outbreak. The system should be configurable to meet the needs of various outbreaks, and capture data related to cases, contacts, investigations, exposures, relationships, clinical and environmental specimens, laboratory results, vaccinations and treatments, travel history, and conveyance information. The application should also allow for new objects to be defined and created during the course of an investigation.

Central to the functionality of a system supporting OM is the ability to collect data related to possible cases and exposures and to create traceable links between all appropriate objects. By tracing the mechanism of transmission and identifying the source of the outbreak, the appropriate outbreak response staff can more adequately contain the event. Systems supporting OM should also be integrated with early event detection, countermeasure administration, laboratory, and surveillance systems to achieve the primary goal of managing the response to and containment of an outbreak.

This document provides minimum operational requirements necessary to support an outbreak management system and should in no way preclude a system from incorporating additional functionality beyond what has been covered in this document.

2 REQUIREMENTS

2.1 OUTBREAK MANAGEMENT FUNCTIONAL REQUIREMENTS

The following requirements describe baseline functionality for any system implemented to support Outbreak Management:

- *System Architecture*: Broad system-level needs, such as flexible configuration, should be addressed by systems supporting OM.
- *Data Input Sources:* Outbreak management systems must be robust enough to capture a wide range of data inputs, including manual entry, data feeds, and electronic messaging.
- *Data Requirements*: OM systems need a variety of data to support investigations, including data regarding demographics, cases, exposures, investigations, agents, contacts, specimen collection, laboratory tests, travel and conveyance, and containment.
- *Case Investigation*: Investigations are conducted through the development and use of event-specific questionnaires intended to capture the data needed to make a determination regarding the illness or exposure. Questionnaire data are supplemental to the required detailed demographic and investigation data.

- *Linking*: The most powerful ability a system supporting OM should provide is the ability to capture links between data objects (people, places, events, actions, etc.).
- *Contact Tracing*: In order to help contain future cases and to determine exposure transmission and risk factors, contacts should be traced.
- *Analysis, Visualization, and Report Generation*: An OM system should enable investigators to produce both aggregated and individual reports about affected entities and events.
- *System Integration and Data Exchange*: OM information must be exchangeable, based on established standards, between systems involved in the investigation, identification, confirmation, and reporting of an outbreak.
- *Operations*: Personnel, roles, activities, and responsibilities necessary to support OM systems should be clearly defined.
- *System Security and Availability*: Security (i.e., authentication, authorization, and access control) and availability (i.e., continuity of operations) requirements should be enforced across the OM system.

2.1.1 System Architecture

- Systems designed to support OM must offer configuration flexibility so that new data fields, entities, and relationships may be added for each incident in order to capture the unique information particular to each outbreak.
- The OM system should support structured data entry for common forms and fields to ensure data integrity, validity, and standardization. A standardized data structure will ensure that data mapping of common elements will only be necessary one time, rather than for each event.
- Systems supporting OM should support multiple deployment options (i.e., web based, client server, disconnected, etc.).
- The system must be able to electronically record and store data from remote devices that may be uploaded to an aggregating system.
- An OM system should be capable of utilizing configurable, domain-specific vocabulary.

2.1.2 Data Input Sources

- Manual, intuitive data entry must be supported.
- Systems supporting OM should have the ability to accept electronic imports or uploads of data in various formats (i.e., EpiInfo, SAS, GIS, MS Access, Crystal Reports, etc.).
- Scanned documents should be accepted as a valid data input source.
- Properly formatted messages and alerts (from laboratories or surveillance systems) should be supported as a means of data entry.

2.1.3 Data Requirements

The following high-level data requirements are necessary to ensure that the data being collected, analyzed, and reported to support OM are clearly defined.

2.1.3.1 Entity Data

An entity is any being or object involved in an outbreak. Entities may be classified as a person, organization, place, animal, or object, and each type of entity requires specific data to be collected.

- Demographic data must be collected about persons involved in an OM investigation, including: subject ID, name, address, date of birth, gender, phone number, race, ethnicity, country of citizenship, and other descriptive details.
- Data must be collected about organizations involved in an OM investigation, (i.e., a local health department, a university, a professional association, etc.).
- Data must be collected about places involved in an OM investigation, including: name (if applicable), type (floor, building, room, store, etc.), street address, country, GPS coordinates, and the more specific location of an place, (i.e., a specific building on a campus, a business branch location, a local chapter's meeting hall, etc.)
- Data must be collected about any animals involved in an OM investigation, including: type (dog, monkey, etc), age, gender, owner's name and address, color, weight, and species.
- Data must be collected for any object involved in an OM investigation, such as a letter, invoice, food item, or any object that cannot be classified as a "person, organization, place, or animal." Collected data may include: name of the object, type, physical descriptors, address, identification number (i.e. serial number, package slip number, etc.), and event dates and times (if applicable).

2.1.3.2 Outbreak Event Data

- When an event is investigated, it must be assigned an event identifier (ID) in the OM system.
- Data describing the event, including the reason for the investigation, the date the event began, the suspected agent, the geographic area impacted by the event, as well as the event status (i.e., open or closed), should be captured.

2.1.3.3 Travel History and Conveyance Data

- Systems supporting OM must collect an entity's travel history and conveyance data in order to support investigations of entities exposed or potentially exposed. Travel history provides specific information to indicate when, where, and how a person traveled to a location (or to multiple locations), and conveyance describes the vehicle in which the travel occurred.
- Travel history data should include information such as the method of transportation (i.e. bus, plane, boat, car, etc.), departure and arrival dates and times, and the origination and destination locations (city, state, and country).
- Travel history data to be collected for an animal or object should include shipping invoices, animal shelter delivery and adoption receipts, delivery schedules (including delivery vehicle and driver information), etc.
- Additional travel details, such as the initiation, investigation, and residence locations, should be collected. For example, if a person who lives in Georgia

travels to Seattle and becomes exposed to monkey pox, then visits a friend in Santa Fe, travel history and conveyance data should be noted accordingly for each place the exposed person traveled.

- Detailed conveyance data must be collected, including the carrier identifier (i.e. flight number and seat assignment), the type of conveyance (such as airline, bus, or train, among countless others), as well as the make, model, year, and identification number (i.e., VIN) of each vehicle with which the entity was in contact.

2.1.3.4 Case, Contact, Exposure, and Investigation Data

Cases and contacts can be persons, animals, or exposure settings, such as travel conveyance, place, or organization, and provide more detailed information beyond demographic data.

- All suspected, probable and confirmed exposures should be identified, investigated, and monitored.
- Case data about the entity should include a case ID that is unique within the jurisdiction being reported, the suspected agent, health status, and case status (i.e., suspected, confirmed, negative).
- Detailed contact data must be collected about the source of exposure as well as the exposed entity in order to support contact tracing. Exposure data related to both the potential source and the potential spread include the entity's type, subject ID, contact ID, contact's name and address, exposure dates, health status, and priority level.
- Exposure investigation data to be captured must include information related to exposure levels, type of exposure (intimate, social, household, environmental, etc.), length of time the entity was exposed, and the entity's distance to the source of exposure, for example.
- Epi data, including onset data of symptoms, risk factors, laboratory data, and survey question responses, must be collected to assist in the investigation of outbreaks.
- If applicable, other procedure data, such as x-rays, CT scans, or MRIs, should be captured.
- Investigation data should include the investigation dates, priority code, status code, case ID, symptom onset date, epi-link indicator, and health status code.
- Demographic information should be collected about the outbreak investigator, including their name, address, and contact information, so that the investigator may be contacted to answer questions or to provide additional information.

2.1.3.5 Specimen Collection and Laboratory Response Data

- Clinical or environmental specimen data must be collected and include a sample ID that is linked to test results, the collection date, specimen type, risk indicator (i.e., infectious, radioactive, corrosive, etc.), collector, location of collection, volume and quantity details, and the "parent" specimen's ID if the specimen was a sample taken from a larger source.

  - Clinical specimen data should include information about the body site from which the specimen was taken.
  - Environmental specimen data should include information about the location from which the specimen was taken.
- If specimens are transferred to test laboratories or other facilities, the batch shipment information should be collected, including the shipping number and the sender's contact information.
- Laboratory specimens must be collected and forwarded to participating laboratories for testing. These specimens can be collected from places, suspected cases and contacts, or environmental sources such as air, water, food, or soil.
- Laboratory result data that is provided must contain information about laboratory specimens collected by the case investigator or by other parties (i.e., health care providers, epidemiologists, emergency response team members, etc.). This data should include the specimen ID, test date, test type, organization data (i.e., testing laboratory name, location, contact information, etc.), laboratory results, and any relevant notes.

2.1.3.6 Containment Data

- Containment data should include information regarding monitoring of contacts quarantined and cases isolated. This data should include the date of onset of symptoms, health status, the recommended treatment, the number of recommended days of treatment follow-up, and the organization of that treatment.
- Containment data should be communicated to the quarantine or isolation site in order to monitor the case's health status.
- Quarantine and isolation data, including the type (voluntary or involuntary), location of the sites, restriction orders, contact information, and daily monitoring data should be captured.
- If samples taken from a location test positive for an agent, containment data to be collected should indicate when the location has been effectively decontaminated and deemed safe for occupation.

2.1.3.7 Prophylaxis and Treatment Data

- Prophylaxis and treatment data must include a description of the treatments, vaccinations, antidotes, or prophylaxis used to counteract the agent of an outbreak on exposed or possibly exposed entities.
- Administration and take response data must include the entity vaccinated; where and when the vaccination was administered; take response assessment (i.e., positive, negative, equivocal, etc.); where and when the take response was assessed; and the location on the entity's body where the vaccination was administered.
- Data should be collected to indicate what treatment is prescribed to an entity, as well as the recommended dosage and frequency of administration of the treatment.

- Contraindication information may also be collected to indicate why vaccinations, treatments, or antidotes may not have been administered or why the patient may not have complied with the prescribed treatments.

2.1.3.7.1 Adverse Event Data

- If an affected person suffers a negative reaction to administered vaccinations or prophylaxis, data should be collected to describe the characteristics of the reaction, as well as the amount of time lapsed between the entity receiving the vaccination and the onset of symptoms.
- If an affected person receives vaccination or prophylaxis to protect against the outbreak but shows no signs of benefit, this information should be captured.

2.1.3.8 Activity Logging Data

- An OM system should capture information such as the date of activity, activity type, who initiated the activity, and contact information in order to generate activity logs for management purposes.
- Activity logs should be tools that investigators use to work effectively. These logs may produce lists of phone numbers of affected persons so that the investigator may call to monitor their health status or schedule follow-up visits.
- Activity logs may also provide information needed to support communication with various jurisdictions in the event that the investigation crosses jurisdictional boundaries. For example, an investigation may be initiated by a local health department, but the outbreak spreads through conveyance and another health department manages the investigation.

2.1.4 System Functions and Behaviors

2.1.4.1 Case Investigation

- Electronic questionnaires should be developed, validated, and provide the capability to accept electronic signatures. They will be designed by investigators to collect common data elements (i.e., patient demographics, test results, and contacts), agent-specific data elements (i.e., specific laboratory test), and other customized data elements.
- The OM system must offer the ability to publish and control the configuration of investigation-specific questionnaires and implementation guides, and revisions to the same.
- Case investigation should be supported by reusable questionnaire libraries that use common terminology (where applicable) to maximize the efficiency of data exchange.

2.1.4.2 Linking

- Linkages allow investigators to create more meaningful analysis by characterizing the event and identify at-risk populations. Types of linkages include:
    - Entity-to-entity relationships (i.e., person-to-person, person-to-place, animal-to-person, object-to-place, etc.) must be dynamic in order to freely define an entity specific to an event.

  - Entity-to-action links describe the relationship between a person or animal to actions such as travel, exposures to cases, and relationship contacts.
  - Entity-to-epi data links will match the entity to their symptoms, survey questions, specimen collection, laboratory result data, and treatment data.
- Each new case must be linked to an assigned entity ID to an event ID within the scope of the investigation.
- An OM system must have the ability to capture information about possible cases and potential contacts from the identification process through the treatment and follow-up process, as supported by linkages of entities, events, and actions.
- Laboratory results must be linked to corresponding specimens, and cases or contacts when the participating laboratory returns the results. These linkages must unambiguously associate multiple entities to case and contact IDs.

2.1.4.3 Contact Tracing, Containment, Exposure, and Monitoring

- Each case ID may be associated with primary and secondary contacts, including unambiguous links to contacts in other jurisdictions.
- Primary and secondary contacts of exposed entities (i.e., people, animals, places, etc.) may be traced, investigated, and monitored.
- An OM system should be able to create new contacts from existing case records, and should also identify the contact type.
- Contact tracing must be supported by the OM system's ability to link one contact to multiple cases, and allow multiple contacts to be linked to a single case.
- Systems supporting OM should be able to produce contact work lists for each investigator to use, and should allow sorting by priority or geography.

2.1.5 Analysis, Visualization, and Report Generation

- Systems supporting OM should allow for analytical searches based upon multiple criteria.
- An OM system should have the ability to produce charts, maps, and graphs that illustrate outbreak data, such as epi-curves and the effect of vaccination or prophylaxis on the number of new cases (demonstrating the effectiveness to counteract the outbreak).
- An OM system should generate electronic data dictionaries (or other user-defined data descriptions to assist with effective data exchange), line lists, activity logs, aggregate data, and call-back lists to assist the emergency response group and investigators in responding to and containing an outbreak.
- Reports should clearly indicate the number of cases, the number of contacts per case, the number of cases with no known epi-link at the time of diagnosis, the laboratory results, and the number of vaccinations and/or treatments administered.
- Pre-formatted queries and reports should be supported by an OM system in order to allow faster and more accurate reporting, while still allowing the flexibility of ad-hoc reporting.
- The system should have the ability to produce individual reports for each emergency team member or investigator.

2.1.6 System Integration and Data Exchange

- An OM system must support sending, receiving, and storing outbreak data electronically.
- Systems supporting OM should be able to electronically accept data from surveillance and early event detection (EED) systems regarding the identification of possible clusters or outbreaks.
- Line lists, laboratory orders, specimen collection, and shipment data should be sent from an OM system to laboratories for evaluation in order to confirm or disprove the existence of cases. (Lab results can't confirm the existence of an outbreak. A public health authority must decide what constitutes an "outbreak").
- Upon analysis, participating laboratories should provide test results electronically to an OM system so that entities may be linked to the results.
- An OM system should integrate with countermeasure administration (CA) systems in order to provide line lists of contacts that need to be vaccinated. Subsequently, the OM system must accept vaccination administration confirmations from CA systems in order to link entities to their treatments.
- An OM system should integrate with incident management (IM) systems to provide information necessary for outbreak monitoring, such as the number of cases, number of persons under quarantine, and the number of vaccines administered. This information should also be passed to surveillance and EED source for their comprehensive data collection requirements.
- OM systems should also utilize IM data to identify the appropriate emergency response group staff to respond to the event, based upon their training, qualifications, and experience
- Because the OM systems are configurable to meet the individual needs of each event and therefore collect data specific to each event, mapping interfaces and data dictionaries must be clearly defined and included in data exchanges to indicate and describe both standard and supplemental fields.
- Messages should be grouped by observation type (i.e., laboratory, symptom, exposure, risk, treatment, etc) by the OM system.
- OM systems should support multiple file formats, such as databases, spreadsheets, messages, and text files, among others.
- Bi-directional, secure data exchange must be supported in order to enable a thorough knowledge transfer structure for public health investigations among multiple jurisdictions and reporting levels (i.e., local, state, and national).
- Industry standards supported by PHIN for messaging (such as HL7) and secure data transport (such as ebXML) should be used when exchanging information between organizations and systems.
- Secure data exchange is required and should include appropriate security and privacy considerations, including data obfuscation and both destination and source authentication.
- Data exchange should support analysis and information sharing of possible public health events at all levels of public health (national, state, and local).

2.1.7 Operations

- Operational requirements including processes, personnel, and responsibilities must provide clear instruction about supporting, maintaining, and testing OM systems.
- Policies and procedures for communicating information to appropriate stakeholders (i.e., state and federal emergency management organizations, FEMA, hazmat teams, public works facilities, intelligence organizations, the media, and the public) should be clearly defined.
- Operational processes must be defined in detail for successful data exchange (bundling, parsing, formatting, etc), data mapping, analysis, visualization, reporting, and alerting of public health events.
- Data back-up processes and policies for mission critical information must be clearly defined and communicated.
- Data sources should be monitored for compliance with the data collection, quality, consistency, and integrity standards.
- Interfaces with other systems must be monitored and managed by trained, qualified personnel to ensure the lines of communication remain constantly open and accessible.
- Personnel should be available to help resolve data exchange and connectivity issues, as well as to provide remote application support.

2.1.8 System Security and Availability

- The security layer must be managed for authentication, authorization, and access control.
    - Authentication is required to validate that the user is registered to access the system and has signed on with the appropriate user name and password or other identifiable key. Strong authentication mechanisms, such as X.509 certificates or secure token based technology, are required.
    - Authorization levels must be supported to manage access to system functions and data. Authorization levels can include user based, role based and/or context based authorization.
    - Access control rules must be implemented to enforce authorization levels and control user access to the system.
- The confidentiality and integrity of sensitive data must be constantly protected.
- Privacy concerns must be addressed in order to protect patients and organizations from fraudulent use of their information. Confidentiality agreements and data use and sharing agreements may be used as tools to address these concerns.
- Continuity of Operations (COOP) and Disaster Recovery plans must be clearly established to ensure the system will not suffer performance, availability, security, and validity failures during emergencies and destructive events.
- PHIN security standards can be viewed using the following link: www.cdc.gov/phin/architecture/automated_data_exchange.htm

3 PROCESS FLOWS

TBD

3.1 OVERVIEW