PHIN Preparedness

(DRAFT for discussion)

OUTBREAK MANAGEMENT FUNCTIONAL REQUIREMENTS AND PROCESS FLOWS

Version 1.0 Draft

10/12/2004

TABLE OF CONTENTS

1 INTRODUCTION

This document describes the Public Health Information Network (PHIN) functional requirements and general workflow for systems implemented to participate in Outbreak Management. Outbreak Management (OM) is the PHIN functional area intended to support the needs of investigation, monitoring, management, analysis, and reporting of a public health event or act of bioterrorism. OM should aid in the collection and analysis of data to support identifying and containing the outbreak. OM systems should be configurable to meet the needs of different types of 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 entities. By tracing the mechanism of transmission and identifying the source of the outbreak, the appropriate outbreak response staff can more effectively 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 mitigating the effects 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 OUTBREAK MANAGEMENT FUNCTIONAL REQUIREMENTS

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

***2.1 System Architecture*:** Broad system-level needs, such as flexible configuration, should be addressed by systems supporting OM.

***2.2 Data Requirements*:** Systems supporting OM 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 restriction monitoring.

***2.3 System Functions and Behaviors*:** An OM system should support case investigation, maintain detailed and comprehensive linkages, trace contacts, and outbreak restriction monitoring activities.

***2.4 Analysis, Visualization, and Report Generation*:** An OM system should enable investigators to produce both aggregated and individual reports about affected entities and events.

***2.5 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.

2.6 Vocabulary Standards: Standard vocabulary lists and data structures have been defined by various organizations. Where they exist, OM systems should utilize them. As additional standards are defined, they should be accepted and implemented

***2.7 Operations*:** Personnel, roles, activities, and responsibilities necessary to support an OM system should be clearly defined.

***2.8 System Security and Availability*:** Security of OM data includes the protection of data from corruption and access by unauthorized individuals, as well as the protection of an OM system itself from sabotage or other failure. There must be a backup plan for continuing activities when OM systems are unavailable.

2.9 Privacy: Patients and organizations must be protected from fraudulent and unauthorized use of their information.

2.1 SYSTEM ARCHITECTURE

2.1.1 Systems designed to support OM must offer configuration flexibility so that new data fields, entities, and relationships may be added to capture information unique to each particular outbreak.

2.1.2 OM must support structured data entry for common forms and fields to ensure data integrity, validity, and standardization. A standardized data structure ensures that data mapping of common elements will only be necessary one time, rather than for each event.

2.1.3 OM should support multiple deployment options (i.e., client server, disconnected, and potentially web based.).

2.1.3.1 OM systems should provide the ability for computers in disconnected mode to reconnect to a server in order to share OM data among other computers that operate in disconnected mode.

2.1.3.2 OM data should be synchronized so that all instances of OM applications working from the same server are able to share and use the same data..

2.1.4 OM systems must be able to electronically record and store data from remote devices that may be uploaded to an aggregating system.

2.1.5 An OM system should be capable of utilizing configurable, domain-specific vocabulary.

2.1.6 Manual, intuitive data entry must be supported.

2.2 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.

2.2.1 Entity Data

An entity is any being or object involved in an outbreak. Entities may be classified as a person, organization, location, animal, object, conveyance, event, and other organisms. Each type of entity requires specific data to be collected.

2.2.1.1 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.

2.2.1.2 Data must be collected about organizations involved in an OM investigation, (i.e., a local health department, a university, a professional association, etc.).

2.2.1.3 Data must be collected about locations involved in an OM investigation, including: name (if applicable), type (floor, building, room, store, etc.), street address, country, GPS coordinates, and other specific details (i.e., a specific building on a campus, a business branch location, a local chapter's meeting hall, etc.)

2.2.1.4 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. A subject ID should also be collected for animals in an OM investigation; however, it may be a challenge to ensure unambiguous identification because demographic details of an animal are not easily identified; therefore, animals involved in investigations may need to be tagged.

2.2.1.5 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).

2.2.1.6 Data must be collected about any conveyance involved in an OM investigation, including: type of conveyance, route taken, seat number, etc.

2.2.1.7 Data must be collected about any event involved in an OM investigation, including: time, location, nature of the event, etc.

2.2.1.8 Data must be collected about any organisms other than those named above that are involved in an OM investigation, including: indicator whether the organism is bacterial or viral, or other customizable data collection questions.

2.2.2 Outbreak Event Data

2.2.2.1 When an event is investigated, it must be assigned an event identifier (ID) that is unique to the jurisdiction in the OM system.

2.2.2.2 Data describing the event, including the reason for the investigation, the date the outbreak began, the suspected agent (if known), the geographic area impacted by the event, as well as the event status (i.e., open or closed), should be captured.

2.2.3 Travel History and Conveyance Data

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.

2.2.3.1 Systems supporting OM must collect an entity's travel history and conveyance data in order to support investigations of entities infected, exposed or potentially exposed.

2.2.3.2 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).

2.2.3.3 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.

2.2.3.4 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.

2.2.3.5 Detailed conveyance data must be collected when relevant to the investigation, including the carrier identifier (i.e. flight number and seat assignment), the type of conveyance (such as airplane, 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 (if this information us relevant to the investigation).

2.2.4 Case Investigation and Exposure Contact Data

Case and exposure data provide more detailed information beyond demographic data. Cases can be persons or animals, and exposure contacts can be persons, animals, other organism, or exposure settings, such as travel conveyance, location, organization, object, or event.

2.2.4.1 Because attributes of both case and exposure data may describe the same entity, an OM system must have the ability to avoid capturing redundant entity demographic information.

2.2.4.2 Public Health Case Data

2.2.4.2.a Case data about the entity should include: a case ID that is unique within the jurisdiction being reported, the suspected agent, health status, case status (i.e., suspected, confirmed, negative), investigation dates, priority code, status code, case ID, symptom onset date, epidemiological links to other cases, and health status code.

2.2.4.2.b Epidemiological (epi) data must be collected to assist in the case investigation of outbreaks. Standard epi data to be collected includes: onset date of symptoms, risk factors, laboratory data, procedure data, and survey question responses.

2.2.4.2.c OM systems should allow for more dynamic, outbreak-specific case investigation data to be captured.

2.2.4.2.d In the context of a case, all entities exposed to a case must be recorded and linked to the case.

2.2.4.2.e 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.

2.2.4.3 Exposure Contact Data

2.2.4.3.a 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 proximity to the source of exposure.

2.2.4.3.b Detailed 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.

2.2.4.3.c Epi data must be collected to assist in the exposure investigation of outbreaks. Standard epi data to be collected for exposure investigation parallels the data to be collected for case investigation and includes: risk factors, laboratory data, procedure data, and survey question responses.

2.2.4.3.d OM systems should allow for more dynamic, outbreak-specific exposure contact data to be captured.

2.2.5 Monitoring and Follow-up Data

Monitoring and follow-up data is used to track the progress and treatment of subjects who were exposed or potentially exposed to a public health event. More detailed information about this data should be reviewed in the PHIN Countermeasure and Response Administration Functional Requirements and Process Flow document. (www.cdc.gov/phin/CRA.pdf)

2.2.5.1 An OM system should support the monitoring and follow-up activities required when tracking the status of exposed or possible cases.

2.2.5.1.a Monitoring data should be collected regarding the restriction of subjects involved in a public health event.

2.2.5.1.b Follow-up data should be collected from daily calls placed to exposed or possible cases to track the status of their symptoms and whether the cases are complying with recommended treatment plans or prophylaxis.

2.2.6 Specimen Collection and Laboratory Response Data

2.2.6.1 Clinical or environmental specimen data must be collected and include a specimen ID that is linked to test results, the test name, the date of testing, 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. Please reference section 2.5 Object Identifiers in the *PHIN Preparedness Cross Functional Components Functional Requirements and Process Flows* document (*www.cdc.gov/phin/CFC.pdf*) for more detail regarding specimen identifiers.

2.2.6.1.a Clinical specimen data should include information about the specimen source/site from which the specimen was taken (when appropriate), as well as the specimen type.

2.2.6.1.b Environmental samples (i.e., specimen) data should include information about the collection method, location from which the sample was taken, source, type, and nature of the sample, such as soil, water, or air.

2.2.6.2 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.

2.2.6.3 Laboratory specimens identified with a unique subject ID 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. Please reference section 2.5 Object Identifiers in the *PHIN Preparedness Cross Functional Components Functional Requirements and Process Flows* document (*www.cdc.gov/phin/CFC.pdf)* for more detail regarding subject identifiers.

2.2.6.4 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.). Examples of this data include the specimen ID, collection date, test date, test type, organization data (i.e., testing laboratory name, location, contact information, etc.), laboratory results, and any relevant notes. Please reference section 2.5 Object Identifiers in the *PHIN Preparedness Cross Functional Components Functional Requirements and Process Flows* document (*www.cdc.gov/phin/CFC.pdf)* for more detail regarding subject identifiers.

2.2.7 Prophylaxis and Treatment Data

2.2.7.1 An outbreak management system should capture or be linked to data regarding the prophylaxis or treatment to affected or possibly affected subjects, including the name, date, type, and dosage of the treatment or prophylaxis given.

2.2.7.2 For specific data requirements regarding the administration of prophylaxis and treatment, please reference the PHIN Preparedness Countermeasure and Response Administration Functional Requirements and Process Flows document. (*www.cdc.gov/phin/CRA.pdf*)

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

2.2.8 Adverse Event Data

2.2.8.1 If an affected person suffers a negative reaction to administered vaccinations or prophylaxis, adverse event data may be collected and used to determine the need for additional treatment or whether there is a problem with the pharmaceuticals, batches, treatment facility, or treatment administrator.

2.2.8.2 For specific data requirements regarding adverse event data, please reference the PHIN Preparedness Countermeasure and Response Administration Functional Requirements and Process Flows document. (*www.cdc.gov/phin/CRA.pdf*)

2.2.9 Activity Logging Data

2.2.9.1 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.

2.2.9.2 Activity logs, which are tools for investigators to track their actions during a case, should be supported. For example, investigators may log calls made to monitor symptoms or calls made to schedule follow-up visits.

2.2.9.3 Activity logs may also provide information needed to support communication with various jurisdictions in the event that the investigation crosses jurisdictional boundaries. For example, if a person becomes ill during travel in one jurisdiction but is the resident of another, the illness will be reported by the state (jurisdiction) of residence, rather than by the jurisdiction visited.

2.3 SYSTEM FUNCTIONS AND BEHAVIORS

2.3.1 Case Investigation

2.3.1.1 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 exposure contacts), agent-specific data elements (i.e., specific laboratory test), and other customized data elements.

2.3.1.2 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.

2.3.1.3 Case investigation should be supported by reusable questionnaire libraries that use common terminology (where available) to maximize the efficiency of data exchange.

2.3.2 Linking

Linkages allow investigators to create more meaningful analysis by characterizing the event and identifying at-risk populations.

2.3.2.1 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.

2.3.2.2 Entity-to-action links describe the relationship between a person or animal to actions such as travel, exposures to cases, and relationship contacts.

2.3.2.3 Entity-to-epi data links will match the entity to their symptoms, survey questions, specimen collection, laboratory result data, and treatment data.

2.3.2.4 Each new case must be able to link an assigned entity ID to an event ID within the scope of the investigation.

2.3.2.5 OM requires 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 among entities, events, and actions.

2.3.2.6 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 laboratory results to case and contact IDs.

2.3.3 Contact Tracing, Containment, Exposure, and Monitoring

2.3.3.1 Each case ID may be associated with primary and secondary contacts, including unambiguous links to contacts in other jurisdictions.

2.3.3.2 Primary and secondary contacts of exposed entities (i.e., people, animals, places, etc.) may be traced, investigated, and monitored.

2.3.3.3 An OM system should be able to create new contacts from existing case records, and should also identify the contact type.

2.3.3.4 Contact tracing must be supported by an OM system's ability to link one contact to multiple cases, and allow multiple contacts to be linked to a single case.

2.3.3.5 Systems supporting OM should be able to produce contact work lists for each investigator to use, and should allow sorting by priority or geography.

2.4 ANALYSIS, VISUALIZATION, AND REPORT GENERATION

2.4.1 Systems supporting OM should allow for analytical searches based upon multiple criteria.

2.4.2 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).

2.4.3 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.

2.4.4 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.

2.4.5 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.

2.4.6 An OM system should have the ability to produce individual reports for each emergency team member or investigator.

2.5 SYSTEM INTEGRATION AND DATA EXCHANGE

Systems integration requirements specific to systems supporting OM are included in the section below and describe the types of data that OM should be able to send and receive. This section is limited to describing the types of data exchange that OM must support; not the requirements for transporting the data. Secure data transport requirements that

span PHIN functional areas are separately defined and should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (www.cdc.gov/phin/CFC.pdf)

2.5.1 Bi-directional, secure exchange of data with partner organizations is required to support public health investigations across all levels of public health. Some of the system integration and data exchange requirements described in this section have been identified as key performance measures. These measures should be reviewed in the *PHIN Key Performance Measures* document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.2 If samples taken from a location test positive for an agent, data about the location should be forwarded to the Environmental Protection Agency (EPA) for action. The EPA is responsible for decontaminating a location and deeming it safe for occupation.

2.5.3 An OM system must support sending, receiving, and storing outbreak data electronically.

2.5.4 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.).

2.5.5 An OM system must be able to accept data from other partner systems supporting OM.

2.5.6 To confirm or disprove the existence of cases, OM must be able to create and send laboratory test order messages for tests that have been requested. This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.7 OM must be able to receive, parse and process laboratory test results messages for tests that have been performed. Laboratory results should be linked to specimen orders, which are linked to subjects. This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.8 Properly formatted messages from traditional surveillance systems (i.e., case messages), early event detection systems, or laboratories (i.e., laboratory results messages) should be supported as a means of data entry.

2.5.9 OM must be able to receive, parse and process "possible case" messages from surveillance and early event detection (EED) systems. This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.10 OM must be able to create and send "possible case" messages to other preparedness systems. This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document (*www.cdc.gov/phin/KPM.pdf*)

2.5.11 Systems supporting OM should be able to electronically send case messages back to surveillance systems.

2.5.12 OM must also be able to receive, parse and process data messages for individual and aggregate "countermeasures that have been administered" and link them to the treated entity. This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.13 OM must be able to create and send data messages for "countermeasures that are requested". This functional requirement is identified as a key performance measure for assessing preparedness. PHIN Key Performance Measures are described in the document. (*www.cdc.gov/phin/KPM.pdf*)

2.5.14 An OM system should integrate with emergency management (EM) systems to provide aggregate data necessary for outbreak monitoring, such as the number of cases, number of persons under restriction monitoring, and the number of patients receiving countermeasures. This information should also be passed in line listed format to surveillance and EED sources for their comprehensive data collection requirements.

2.5.15 OM systems should use characteristics from EM data to recommend training and prophylaxis required for potential response team members.

2.5.16 Mapping interfaces and data dictionaries must be clearly defined and included in data exchanges to indicate and describe both standard and supplemental fields because OM systems are configurable to meet the individual needs of each event and therefore collect data specific to each event.

2.5.17 Messages should be grouped by observation type (i.e., laboratory, symptom, exposure, risk, treatment, etc) by an OM system.

2.5.18 OM systems should support multiple file formats, such as databases, spreadsheets, messages, and text files, among others.

2.5.19 Bi-directional, secure data exchange must be supported in order to enable a thorough knowledge transfer structure for public health investigations among all levels of public health.

2.5.20 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.

2.5.21 Secure data exchange is required and should include appropriate security and privacy considerations, including data obfuscation and both destination and source authentication.

2.5.22 Data exchange should support analysis and information sharing of possible public health events at all levels of public health (national, state, and local).

2.6 VOCABULARY STANDARDS

It is recommended that standards be used across OM systems; however, vocabulary standards must be used when exchanging data. Vocabulary requirements that span

PHIN functional areas should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (***www.cdc.gov/phin/CFC.pdf***)

2.7 OPERATIONS

Operational requirements, such as system backup policies and procedures, continuity of operations, system monitoring, and employee training ensure that public health partners can effectively support activities in OM and other PHIN functional areas. Operational requirements specific to OM are defined below. Operational requirements that span PHIN functional areas are separately defined and should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (www.cdc.gov/phin/CFC.pdf)

2.7.1 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.

2.7.2 Polices regarding data synchronization should be defined to support multiple deployment options as discussed in section *2.1 System Architecture* above.

2.7.3 Configuration management protocols and personnel should be identified to support multiple deployment options.

2.7.3.1 Protocols and personnel should be identified to support the set-up and configuration of laptops and other field devices used in OM investigations.

2.7.3.2 Processes and personnel should be identified to support agent-specific deployment packages, including syndromic grouping libraries and vocabulary sub-sets, which will be used to efficiently collect data specific to the particular outbreak being investigated.

2.7.4 Data sources should be monitored for compliance with the data collection, quality, consistency, and integrity standards.

2.8 SYSTEM SECURITY AND AVAILABILITY

Systems supporting OM must be protected from sabotage or other system corruption. Security requirements that span PHIN functional areas should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (www.cdc.gov/phin/CFC.pdf)

2.9 PRIVACY

Privacy requirements ensure that sensitive information is not accessibly to unauthorized uses. Privacy requirements are broadly defined because they span all PHIN functional areas. These requirements should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (www.cdc.gov/phin/CFC.pdf)

3 PROCESS FLOWS

Process Flows are currently under development.