PHIN Preparedness

OUTBREAK MANAGEMENT

FUNCTIONAL REQUIREMENTS

Version 1.0

4/26/2005

TABLE OF CONTENTS

1 INTRODUCTION

This document describes the Public Health Information Network (PHIN) functional requirements for systems implemented to participate in the management of outbreaks and other health events. Outbreak Management (OM) is the PHIN functional area intended to support the needs of investigation, monitoring, management, analysis, and reporting of a health event or act of bioterrorism. OM should aid in the collection and analysis of data to support identifying and containing the health event. OM systems should be configurable to meet the needs of different types of health events, and capture data related to cases, contacts, investigations, exposures, relationships, clinical and environmental specimens/samples, 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 cases and exposures and to create traceable links between all appropriate entities. By tracing the mechanism of transmission and identifying the source of the health event, the appropriate response staff can more effectively contain the event. Systems supporting OM should also be integrated with the systems supporting early event detection, countermeasure administration, laboratory, and surveillance to achieve the primary goal of managing the response to and mitigating the effects of an event.

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(s) 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/sample collection, laboratory tests, travel and conveyance, and restriction monitoring.

***2.3 System Functions and Behaviors*:** Systems supporting OM should support case investigation, maintain detailed and comprehensive linkages, trace contacts, and quarantine and isolation monitoring activities.

***2.4 Analysis, Visualization, and Report Generation*:** Systems supporting OM 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 a health event.

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

***2.7 Operations*:** Personnel, roles, activities, and responsibilities necessary to support all aspects of OM 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 the actual systems supporting OM from sabotage or other failure. A plan must be established for continuing activities when systems supporting OM are unavailable.

2.9 Privacy: Patients, organizations, and personnel 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, entity types and relationship types may be added to capture information unique to each particular health event.

2.1.2 Systems supporting 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 Systems supporting OM should support multiple deployment options (e.g., client server, disconnected, and potentially web based).

2.1.3.1 Systems supporting OM should provide the ability for computers in disconnected mode to reconnect to a server 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 Systems supporting OM should be able to electronically record and store data from remote devices that may be uploaded to an aggregating system.

2.1.5 Systems supporting OM should be capable of using configurable, domain-specific vocabulary.

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 a health event. Entities may be classified as a person, organization, location, animal, object, conveyance, event, or other organism. Each type of entity requires specific data to be collected.

2.2.1.1 Systems supporting OM must have the capability to capture demographic data about persons involved in an OM investigation, including: Subject ID, name, address, date of birth, gender, phone number, race, ethnicity, and country of citizenship.

2.2.1.1.a Other descriptive details may be captured, such as occupation and work history.

2.2.1.2 Systems supporting OM must have the capability to capture data about organizations (e.g., a local health department, a university, a professional association) involved in an OM investigation, including: organization name, location, and contact information.

2.2.1.3 Systems supporting OM must have the capability to capture data about locations involved in an OM investigation, including: name (if applicable), type (e.g., floor, building, room, store), street address, city, state, zip code, country, GPS coordinates, and other specific details (e.g., a specific building on a campus, a business branch location, a local chapter's meeting hall)

2.2.1.4 Systems supporting OM must have the capability to capture data 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. 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 Systems supporting OM must have the capability to capture data 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 (e.g. serial number, package slip number), and relevant dates and times (e.g., invoice date, shipping date, packaging date).

2.2.1.6 Systems supporting OM must have the capability to capture data about any conveyance involved in an OM investigation, including: type of conveyance, route taken (e.g., flight number), etc.

2.2.1.7 Systems supporting OM must have the capability to capture data about any public or private gathering of people (e.g., church social, ball game) involved in an OM investigation, including: time, location, nature of the event, etc.

2.2.1.8 Systems supporting OM must have the capability to capture data about any living things other than persons or animals that are involved in an OM investigation, including: type of living thing, and other customizable data collection questions.

2.2.1.9 Systems supporting OM must have the capability to capture an entity's travel history to support investigations of entities infected, exposed or potentially exposed.

2.2.2 Health Event Data

2.2.2.1 When a health event is investigated, it must be assigned an event identifier (i.e., Event ID) that is unique within the jurisdiction.

2.2.2.2 Data describing the health event should be captured, including the reason for the investigation, the category of event (e.g. environmental, infectious), the date the event began, the suspected agent (if known) or investigation focus, the geographic area impacted by the event, as well as the event status (e.g., open, closed).

2.2.2.3 Systems supporting OM should have the ability to record the case definition for a health event.

2.2.2.4 Systems supporting OM should have the ability to capture changes to the case definition that occur as the health event evolves.

2.2.3 Travel History and Conveyance Data

Travel history provides specific information to indicate when, where, and how subjects involved in an event traveled to a location (or to multiple locations), and conveyance data describes the vehicle in which the travel occurred. Examples of travel history include a person's local travel as a part of their daily activities as well as the shipment of animals or plants from one country to another.

2.2.3.1 Travel history data should include information such as the method of transportation (e.g. bus, plane, boat, car), flight number, departure and arrival dates and times, and the origination and destination locations (city, state, and country).

2.2.3.1.a Information about each leg of a trip, as well as the parent information about the trip, should be captured. 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.

2.2.3.2 Travel history data to be collected for an animal or object should include shipping invoices, animal shelter delivery and adoption receipts, and delivery schedules (including delivery vehicle and driver information).

2.2.3.3 Detailed conveyance data must be collected when relevant to the investigation, including the carrier identifier, the type of conveyance (such as airplane, bus, or train, among countless others), as well as the make, model, year, and identification number (e.g., VIN) of each vehicle with which the entity was in contact (if this information is 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 organisms, 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, systems supporting OM 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 identifier (i.e., Case ID) that is unique within the jurisdiction being reported, the suspected agent, case diagnosis, health status (e.g., no symptoms, acute illness), case status (e.g., confirmed, probable, suspect), investigation dates, clinical history, symptom onset date and time, epidemiological links to other cases, and priority (e.g., high, medium, low).

2.2.4.2.b There must be a means to update the case diagnosis either manually or automatically if the case definition changes during an event.

2.2.4.2.c Epidemiological (epi) data must be collected to assist in the case investigation of events. Standard epi data to be collected includes: onset date and time of symptoms, type of symptoms, risk factors, medical history data, laboratory data, procedure data, and questionnaire responses.

2.2.4.2.d Systems supporting OM must allow for dynamic, event-specific case investigation data to be captured.

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

2.2.4.2.f Demographic information should be collected about the investigator, including their name, address, and contact information, so that the investigator may be contacted to answer questions or to provide additional information.

2.2.4.2.g Both the jurisdiction investigating the event and the jurisdiction reporting the cases and associated investigations must be captured. 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 and investigated by the jurisdiction visited.

2.2.4.2.h Systems supporting OM should have the ability to classify entities associated with the investigation as investigation controls. For example, controls share demographic characteristics with the subject of the case, but are not infected with the agent that is the focus of the investigation.

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 (e.g., intimate, social, household, common conveyance), place of exposure, length of time the entity was exposed, frequency of exposure, 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 to support contact exposure 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 and times, health status, and priority code.

2.2.4.3.c Epi data must be collected to assist in the exposure investigation of health events. Standard epi data to be collected for exposure investigation parallels the data to be collected for case investigation and includes: onset date and time of symptoms, type of symptoms, risk factors, laboratory data, procedure data, and questionnaire responses.

2.2.4.3.d Systems supporting OM must support capturing dynamic, event-specific data that describes contact between two subjects.

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 health event. For more information about monitoring and follow-up data, please reference "PHIN Countermeasure/Response Administration Functional Requirements and Process Flows", available at www.cdc.gov/phin.

2.2.5.1 Systems supporting OM should support the monitoring and follow-up activities required when tracking the status of cases and exposed individuals.

2.2.5.1.a Monitoring data should be collected about cases and exposed individuals who are isolated or quarantined because of a health event.

2.2.5.1.b Follow-up data should be collected from subjects or their proxies to track symptoms and compliance with recommended treatment plans or prophylaxis.

2.2.5.1.c Follow-up data may be received from take response exams of persons who received a countermeasure that requires such an exam (i.e., smallpox vaccination).

2.2.6 Specimen/Sample Collection and Laboratory Response Data

Specimen/sample collection and laboratory response data supports the collection of clinical specimens, food samples, environmental samples, and other types of samples that will be tested for biological, chemical, and radiological agents. These specimens/samples can be collected from places, persons, animals, or environmental sources such as air, water, food, or soil.

2.2.6.1 Specimens/samples collected for laboratory testing must be assigned an identifier (i.e., Specimen ID) that is unique within the jurisdiction.

2.2.6.2 The subject of a specimen/sample collected for laboratory testing must be linked to the specimen/sample by an identifier (i.e., Subject ID) that is unique within the jurisdiction.

2.2.6.3 Systems supporting OM must be able to store data about the specimens/samples that are collected for laboratory testing. Examples of this data are: Specimen ID, Subject ID, purpose for test, collection date and time, subject type (e.g., human, plant, animal, food), specimen category, specimen type, suspected agent, risk indicator (e.g., infectious, radioactive, corrosive), person performing specimen/sample collection (including contact information), location of collection, and volume and quantity details.

2.2.6.3.a Clinical specimen data should include information about the specimen source/site from which the specimen was taken, symptom date of onset, and whether the sample is acute or convalescent.

2.2.6.3.b Environmental sample data should include information about the collection method, location (geocoded if possible) from which the sample was taken, source (e.g., rain or well for water, radiation release, asbestos, chair or desk in a specified location), nature of the sample (e.g., soil, water, air), quality control data, collection begin and end date and time for air samples, and original volume and volume of concentrate tested for water samples.

2.2.6.3.c Food sample data should include information about the lot number, batch number, manufacturer name, shipping invoice, temperature, sample type (e.g., dairy – milk, red meat, spice), and product storage condition.

2.2.6.3.d Bar-coding should be supported for the capture of detailed specimen/sample data to improve the quality and efficiency of data collection.

2.2.6.4 Chain of custody information for all specimens/samples should be captured.

2.2.6.5 Chain of custody information for forensic and select agent samples must be captured, including the person who collected the sample, the location of collection, all people who came into contact with the sample during the preparation for shipment to the laboratory, and the acceptance of the package by the shipper.

2.2.6.6 Systems supporting OM must be able to create a laboratory test request for a specimen/sample or group of specimens/samples. More information about creating laboratory test requests is found in section *2.5 System Integration and Data Exchange* of this document.

2.2.6.7 Information about batch shipments of specimens/samples that are transferred to test laboratories or other facilities must be collected, including the shipper (e.g., UPS, FedEx), shipment tracking number, and the sending organization's contact information.

2.2.6.8 Systems supporting OM should be able to support the inclusion of labeling, packaging and shipping instructions (e.g., container type, storage condition, preservative), and the shipping manifest with batch shipments of specimens/samples.

2.2.6.9 Systems supporting OM must be able to store laboratory result(s) and link the result(s) to the original laboratory test request. More information about receiving and linking laboratory test requests is found in section *2.5 System Integration and Data Exchange* of this document.

2.2.6.10 Systems supporting OM must store data about laboratory results. Examples of this data include the Specimen ID, Subject ID, test date and time, test type (LOINC), data for each organization involved in the testing of the specimen/sample (e.g., testing or reference laboratory name, location, contact information), laboratory results and result values (SNOMED), other data such as unit of measure for result value, overall interpretation, and any relevant notes.

2.2.6.10.a If the specimen/sample collection record exists, the laboratory result must be linked to the specimen collection record by the Specimen ID.

2.2.6.10.b If the specimen/sample collection record does not exist, the laboratory result must be linked to the subject by the Subject ID.

2.2.6.10.c All levels of granularity of results (e.g., specimen/sample level, assay level) must be supported.

2.2.7 Prophylaxis and Treatment Data

2.2.7.1 Systems supporting OM should capture or be linked to data regarding the prophylaxis or treatment to cases, exposed individuals, or at risk persons, including the person who ordered the prophylaxis or treatment, and the name, date, type, duration, and dosage of the treatment or prophylaxis given. For specific data requirements regarding the administration of prophylaxis and treatment, please reference *PHIN Preparedness Countermeasure/Response Administration Functional Requirements and Process Flows*, available at *www.cdc.gov/phin*.

2.2.7.2 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 interventions.

2.2.8 Adverse Event Data

2.2.8.1 If an affected person suffers a negative reaction to a vaccine or prophylaxis that was administered, adverse event data may be collected and used to determine the need for additional interventions or to determine if there is a problem with the pharmaceutical, batch, or the administering facility or person. For specific data requirements regarding adverse event data, please reference *PHIN Preparedness Countermeasure/Response Administration Functional Requirements and Process Flows*, available at *www.cdc.gov/phin*.

2.2.9 Activity Logging Data

2.2.9.1 Systems supporting OM should capture information such as the date and time of an activity, activity type, who initiated the activity, and contact information 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 must be developed and validated. They will be designed by investigators to collect common data elements (e.g., patient demographics, test results, exposure contacts), agent-specific data elements (e.g., specific laboratory test), and other customized data elements.

2.3.1.1.a Electronic questionnaires should provide the capability to accept digital signatures.

2.3.1.2 Systems supporting OM must provide the ability to control the configuration of and revisions to investigation-specific questionnaires.

2.3.1.3 Systems supporting OM must provide the ability to publish investigation-specific questionnaires and implementation guides.

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

2.3.1.5 Systems supporting OM should provide a manual or automatic means of updating the status of case records as the case definition changes.

2.3.1.6 Systems supporting OM should track the changes made to the status of case records as a result of changes in the case definition.

2.3.2 Linking

Linkages allow investigators to create meaningful analysis, characterize the event, and identify at-risk populations.

2.3.2.1 Systems supporting OM must support dynamically defined associations between entities for the purpose of defining relationships. For example, person-to-person (e.g., family relationship, exposure relationship), person-to-place (e.g., household, common place), animal-to-person, object-to-place, person-to-travel.

2.3.2.2 Entity-to-epi data links must match the entity to their symptoms, survey questions, specimens/samples collected, laboratory results, and prophylaxis and treatment data.

2.3.2.3 Each new case must be able to link an assigned Entity ID to an Event ID within the scope of the investigation.

2.3.2.4 Systems supporting OM require 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.

2.3.2.5 Laboratory results must be linked to corresponding specimens/samples including multiple results from one specimen/sample), and subjects when the participating laboratory returns the results. These linkages must unambiguously associate multiple laboratory results to case and contact identifiers.

2.3.2.5.a If the specimen/sample was created from another specimen/sample (e.g., aliquots, and new specimen types created from a source sample), laboratory results for the child specimens/samples must be linked to the corresponding parent specimen/sample.

2.3.3 Contact Exposure Tracing

2.3.3.1 Each investigation subject may be associated with exposure contacts, including unambiguous links to contacts in other jurisdictions.

2.3.3.2 Contacts of exposed entities (e.g., people, animals, places) may be traced, investigated, and monitored.

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

2.3.3.4 Systems supporting OM must support contact exposure tracing by allowing one contact to be linked to multiple cases, and allowing 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 Systems supporting OM should have the ability to produce charts, maps, and graphs that illustrate OM data, such as epi-curves and the effect of vaccination or prophylaxis on the number of new cases (demonstrating the effectiveness in containing the health event) or maps that illustrate the number of cases by zip code.

2.4.3 Systems supporting OM should generate electronic data dictionaries for dynamic data (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 a health event.

2.4.4 Reports generated by systems supporting OM 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 Systems supporting OM should have the ability to produce pre-formatted queries and reports to allow faster and more accurate reporting, while still allowing the flexibility of ad-hoc reporting.

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

2.4.7 Systems supporting OM should have the ability to compare characteristics of exposed and non-exposed (i.e., controls) persons.

2.4.8 Systems supporting OM should have the ability to produce lists of action items (e.g., to do lists).

2.4.9 Systems supporting OM must have the ability to print questionnaires for multiple uses, including taking to the field, use during phone interviews, etc.

2.4.10 Systems supporting OM must be able to aggregate data. Examples of aggregated data to be supported are: number of cases, number of contacts per case, and number of vaccinations and/or treatments administered.

2.4.11 Health event data should be aggregated into a centralized data store (i.e., data warehouse) designed specifically to support analysis of events over time.

2.4.12 Data should be accessible for use with commonly available analytical tools (e.g., SAS, SPSS, EPI-INFO, MS Access, MS Excel, Crystal Reports).

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. Bi-directional, secure exchange of data with partner organizations supports public health investigations across all levels of public health. Message construction and parsing, and secure data transport requirements that span PHIN functional areas are separately defined and should be reviewed in "PHIN Preparedness Cross Functional Components Requirements", available at www.cdc.gov/phin.

2.5.1 Contact information for key response partner organizations should be stored in a local instance of a public health directory for associating to a health event, as described in section *2.2.2 Health event Data* of this document.

2.5.2 Systems supporting OM must be able to accept data from other partner systems supporting OM.

2.5.3 Systems supporting OM must be able to create and send messages for laboratory test requests. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures,* available at *www.cdc.gov/phin*.

2.5.4 Systems supporting OM should be able to receive, parse and process messages for laboratory test request responses, in accordance with *PHIN Laboratory Test Order Response Message Implementation Guide*, available at *www.cdc.gov/phin.*

2.5.5 Systems supporting OM must be able to receive, parse and process messages for laboratory results. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures,* available at *www.cdc.gov/phin*.

2.5.5.1 Laboratory results should be linked to laboratory test requests, which are linked to subjects.

2.5.6 Systems supporting OM should be able to exchange messages for laboratory results with systems supporting surveillance, early event detection (EED), and other preparedness areas.

2.5.7 Systems supporting OM must be able to exchange messages for confirmed, probable and suspect cases, and the other case classifications that are noted in the PHIN message implementation guide, with systems supporting surveillance, early event detection (EED), and other preparedness areas. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures*, available at *www.cdc.gov/phin.*

2.5.8 Systems supporting OM must exchange messages for investigations and for exposure contacts. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures*, available at *www.cdc.gov/phin*.

2.5.9 Systems supporting OM must be able to receive, parse and process messages for countermeasures that have been administered. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures*, available at *www.cdc.gov/phin*.

2.5.9.1 Countermeasures that have been administered must be linked to the entity that was administered the countermeasures.

2.5.10 Systems supporting OM must be able to create and send messages for countermeasure administration requests. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures*, available at *www.cdc.gov/phin*.

2.5.11 Systems supporting OM must be able to exchange aggregated data. Examples of aggregated data to be supported are: number of cases, number of contacts per case, and number of vaccinations and/or treatments administered.

2.5.12 Systems supporting OM should be able to provide the aggregate data necessary for health event monitoring to systems that support response tracking, such as the number of suspect cases, number of persons under isolation or quarantine, and the number of patients receiving countermeasures.

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

2.5.14 Message components should be grouped by observation type (e.g., laboratory, symptom, exposure, risk, treatment) by systems supporting OM.

2.5.15 Systems supporting OM should support multiple file formats for import and export, such as databases, spreadsheets, messages, and text files, among others.

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

2.6 VOCABULARY STANDARDS

It is recommended that standards be used across systems supporting OM; however, it is required that vocabulary standards be used when exchanging data. Vocabulary requirements that span PHIN functional areas should be reviewed in "PHIN Preparedness Cross Functional Components Requirements", available at www.cdc.gov/phin.

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 "PHIN Preparedness Cross Functional Components Requirements", available at www.cdc.gov/phin.

2.7.1 Policies and procedures for communicating information to appropriate stakeholders (e.g., 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* of this document.

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 health event being investigated.

2.7.4 Policies and procedures should be in place for determining when follow up and isolation and quarantine monitoring should be done as a part of a focused countermeasure administration and response effort, rather than as a function of contact exposure tracing.

2.8 SYSTEM SECURITY AND AVAILABILITY

Systems and data supporting OM must be protected from sabotage, corruption and unauthorized access, and must be available subsequent to a catastrophic event. Security and Availability requirements that span PHIN functional areas should be reviewed in "PHIN Preparedness Cross Functional Components Requirements", available at www.cdc.gov/phin.

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 "PHIN Preparedness Cross Functional Components Requirements", available at www.cdc.gov/phin.