PHIN Preparedness

(DRAFT for discussion)

PARTNER COMMUNICATIONS AND ALERTING 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 workflows necessary to send and receive communications and alerts. Communication and alerting systems are intended to support, facilitate and integrate the processes necessary to compose, send, and acknowledge information among public health partners and the public regarding public health events. Systems supporting communication and alerting should provide real-time access to this information, establish alerting protocols, and remain constantly available.

Partner communications and alerting supports functionality such as information dissemination using public web sites, collaboration using secure web sites and e-mail, alerting partners about public health emergencies, sending informational notifications, and informing the media and the public at large. Communications and alerting involves message authorization, message content development and approval, target audience specification, message attributes specification, associated processing requirements (such as urgency and content sensitivity) determination, message delivery mechanisms, and delivery monitoring and reporting. Depending on the sensitive nature of the content, alerts may need to be sent over a secure communication channel. Communication channels refer to the mechanism used to send information among alerting partners. Throughout this document, secure communications refers to whether the communication channel needs to be secured, not to the technology employed to make the channel secure. Secure communications are used to ensure that restricted information is only available to the intended recipients.

An effective communication and alerting system incorporates the business processes, information requirements, controlled vocabularies, authority and role definitions, security requirements, system specifications, and technology services required to support these activities. This document provides minimum operational requirements necessary to support communication and alerting and should in no way preclude a system from incorporating additional functionality beyond what this document addresses.

2 PARTNER COMMUNICATIONS AND ALERTING FUNCTIONAL REQUIREMENTS

The following requirements describe baseline functionality for any system implemented to support communications and alerting capabilities:

2.1 Alerting and Secure Partner Communications**:** The purpose of systems supporting communications and alerting is to inform a designated recipient list about public health events or emergencies using various methods of communication.

2.2 Alert Format: A well-defined format for public health alerts provides for more efficient and standardized communication among public health partners during times of increased risk.

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

2.4 Recipient Addressing: Communications and alerts are forwarded to specified people, roles, organizations, or other groupings.

2.5 Alerting across Jurisdictions: When alerts must be communicated across jurisdictional boundaries, different methods of delivery may be applied.

2.6 System Integration and Data Exchange: To support partner communications, a communication and alerting system should be able to exchange directory data with partners using standardized data exchange formats and protocols.

2.7 Operations: Personnel, roles, and responsibilities necessary to support partner communication and alerting systems should be clearly defined.

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

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

2.1 ALERTING AND SECURE PARTNER COMMUNICATIONS

2.1.1 Alerting

2.1.1.1 An alerting system must have the ability to send, receive, manage, and disseminate information and public health alerts to public health partners using various delivery devices such as telephones, cell phones, faxes, pagers, email, PDAs, or other communication devices. 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*)

2.1.1.1.a Direct alerting will always be used when public health alerts are communicated within a single jurisdiction. This means that the organization initiating an alert sends it directly to a specific list of recipients rather than first routing it through a recipient alerting system to then be disseminated.

2.1.1.1.b When alerts must be sent across jurisdictional boundaries, they may be sent either by direct or cascade alerting or both. Cascade alerting is a process initiated by an originator sending an alert to an alerting system operated by other organizations. The recipient systems then deliver the alert to the appropriate recipients within their respective jurisdictions or organization. More details about cascade alerting are found in section *2.5.2 Cascade Alerting* of this document.

2.1.1.2 Public health partners must be able to send direct alerts.

2.1.1.3 Public health partners must be able to send alerts to and receive alerts from jurisdictions other than their own.

2.1.1.4 Initiating alerting systems must be able to identify which organizations or jurisdictions can receive cascade alerts.

2.1.1.4.a If a jurisdiction or organization has been certified as meeting key performance measures for receiving and processing cascade alerts, then the initiator will use cascade alerting.

2.1.1.4.b If a jurisdiction or organization does not have the ability to receive and process cascade alerts, the initiator will use direct alerting.

2.1.1.5 Professional and advocacy organizations (i.e., American Medical Association, American Public Health Laboratories, etc) that can further distribute alerts to their membership are viable channels of delivery that public health partners should use. The membership of these organizations will, in many cases, overlap with jurisdictions of partners' alerting systems. Standards-based exchange of directory data may help facilitate normalization of recipient lists and reduce duplicative message receipt.

2.1.1.6 An alerting system may support the ability for jurisdictions to append jurisdictionally specific information to original alerts if the message urgency timeliness requirements are met.

2.1.1.7 Alerting systems must generate a real-time message delivery status report containing the number of recipients targeted to receive a message and the number who have confirmed receipt. 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*)

2.1.1.8 Systems initiating alerts must be able to securely archive alerts and communications.

2.1.1.9 Systems initiating alerts must be able to securely retrieve, reconstruct, and resend archived alerts and communications.

2.1.2 Secure Partner Communications

Secure partner communications are used to ensure that restricted information is only available to the intended recipients. "Secure Partner Communications" refers to whether the communication channel needs to be secured, not to the technology used to make the channel secure. For example, standard SMTP e-mail should not be used for secure partner communications because it is neither a secure communication channel, nor does it restrict access to only the intended recipients.

2.1.2.1 A means of secure public health partner communication must be provided.

2.1.2.2 Secure communications should support the ability for appropriate users to post content as well as receive content and to facilitate broader collaboration functions.

2.1.2.3 Sensitive alerts require secure transport and restricted access and distribution.

2.1.2.4 Secure websites that meet certification requirements may be used to satisfy secure delivery of sensitive information.

2.1.2.5 Notification that a sensitive alert is pending delivery can be made using a non-secure communication channel, such as email or fax, as long as the notification itself contains no sensitive content but instead refers the recipient to a means for acquiring the content through a secure channel.

2.1.2.5.a A secure, alerting and communication system must be able to authenticate the identity of a user according to identified authentication requirements before delivering sensitive information.

2.1.2.6 In these cases, the alert may be sent over non-secure means but must include a reference to a secure web site where the sensitive information is available to authenticated users.

2.1.2.7 Secure web presentation over the Internet should be implemented using a secure technology encryption, such as Secure Sockets Layer (SSL).

> PHIN requires that partners have access to a secure web site. Epi-X is one example of a secure web site, and more information about Epi-X is available at *http://www.cdc.gov/epix*. Epi-X, however, is not required so long as the partner has access to a secure web site.

2.1.2.8 Systems supporting alerting must be able to recognize secure versus non-secure channels of transmission. PHIN requirements related to secure transport should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (*www.cdc.gov/phin/CFC.pdf*)

2.2 ALERT FORMAT

Public health alerts may be sent to a wide range of people and roles. A standardized alert format will help ensure that the alerting process works faster and more efficiently in times of urgency.

2.2.1 Alerts should address single issues rather than combining multiple issues in one message; each issue must have its own message.

2.2.2 To support downward compatibility, the content of an alert will be translatable and sharable in simple text format for information delivered by devices that do not support graphics, such as a Blackberry or pagers.

2.2.3 All alerts must contain a message header, body, and footer.

2.2.4 An alert header must include the appropriate level of urgency (as defined in section *2.3 Vocabulary Standards*), as well as the date and time the message was sent.

2.2.5 A title/subject must be included in the alert header, in addition to the sender's name and title.

2.2.6 Each alert header must include a unique identifier that is human readable and, for general reference and context, identifies both the agency originating the alert and the year in which the alert is sent. A standard method is established here to generate these identifiers. The alert identifiers will consist of a concatenation of:

- A two-or-more character agency identifier

- A dash (-)
- The four digit calendar year in which the alert is sent
- A dash (-)
- A three digit sequence number indicating the number of the alert sent by the agency in the year

2.2.6.1 Agency identifiers included in headers must adhere to a specified format that recipients can interpret upon reading.

2.2.6.1.a For federal PHIN partners (currently, just CDC), the agency identifier is the commonly used agency acronym.

Example identifier – federal partner

- CDC - Centers for Disease Control and Prevention
- FBI - Federal Bureau of Investigation

2.2.6.1.b For state health departments, the agency identifier is the two character postal abbreviation for the state name.

Example identifier – state health department

- AL – Alabama Department of Public Health
- AK – Alaska Division of Public Health

2.2.6.1.c For county health departments, the agency identifier is the concatenation of:

- the two character postal abbreviation for the state
- a dash (-)
- the name of the county stripped of any special characters and embedded blanks (i.e., alphabetic characters only)

Example identifier – county health department

- AL-AUTAUGA – Autauga County, Alabama
- LA-STJOHNTHEBAPTIST – St. John the Baptist County, Louisiana

2.2.6.1.d For city health departments, the agency identifier is the concatenation of:

- the two character postal abbreviation for the state
- a dash (-)
- the name of the city stripped of any special characters and embedded blanks (i.e., alphabetic characters only)

Example identifier - city health department

- NY-NEWYORKCITY – New York City, New York
- MO-STLOUIS – St. Louis, Missouri

Example communication and alert identifiers

- The third alert sent by CDC in 2005:
  - CDC-2005-003
- The hundred-and-first alert sent by South Carolina in 2005:
  - SC-2005-101
- The first alert sent by Los Angeles County, California in 2005:
  - CA-LOSANGELES-2005-001

2.2.6.2 Partner communications and alerts must include: a succinct and bold title or subject line; a unique message identifier; issuing date and time; level of urgency; intended audience; name, title, and contact information of the issuing partner; required actions; instructions for sharing the information; point of contact or website address to obtain more information; Public Health Agency's emergency contact information; estimated timeframe for follow up; page numbers (if multiple pages); and approved content.

2.3 VOCABULARY STANDARDS

It is recommended that standards be used across partner communication and alerting systems; however, vocabulary standards must be used when exchanging data. Vocabulary requirements specific to systems supporting alerting are included in the section below. Vocabulary 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)

2.3.1 Vocabulary Requirements

2.3.1.1 Partner communications and alerts must utilize the defined vocabulary structure below for specific data elements and their valid value sets to summarize the communication to the recipients.

2.3.1.2 Direct messages and cascade alerts must support the vocabularies in sections 2.3.2 – 2.3.7 of this document.

2.3.2 Urgency

2.3.2.1 An alerting system must be able to indicate an "Urgency" attribute according to the following guidelines in order to describe the significance of the communication to the recipients:

Urgency Level	Time between original transmission and receipt returned	Threat to life or property
* Emergency	Within 20 minutes	Significant - Extraordinary
* Alert	Within 2 hours	Possible – Significant
Advisory	Within 24 hours	Minimal – Possible
Notification	Within 72 hours	Not known - Minimal

** Note: These functional requirements are identified as a key performance measures for assessing preparedness. PHIN Key Performance Measures are described in the document. (www.cdc.gov/phin/KPM.pdf)*

2.3.2.2 All defined contact methods for each recipient must be fully exhausted in an attempt to collect a return receipt within the applicable Urgency Level timeframe.

2.3.2.3 Systems supporting partner communications and alerting must be able to deliver "Emergency" alerts on a 24 x 7 x 365 basis.

2.3.2.4 An alerting system should attempt delivery of "Emergency" alerts to each recipient until the recipient personally confirms receipt of the alert.

2.3.2.5 For alerts indicated as "Emergency", an alerting system will attempt delivery using the sequential contact methods specified in each user's communications profile and/or alternate contacts for the recipient until the recipient personally confirms receipt of the alert.

2.3.2.6 "Alerts," "Advisories," and "Notifications," are delivered during business hours, and may not require personal confirmation receipts.

2.3.2.7 Alerting systems must be able to accept and register the confirmation of receipt that indicates a human user has received and acknowledged the alert.

2.3.2.8 Systems which support alerting should be able to target and process a single alert using different urgency levels for different recipients (i.e., "Emergency" for some audiences and "Alerts" for others).

2.3.3 Jurisdiction

2.3.3.1 Partner communications and alerts must include an attribute for "Jurisdiction" to indicate the initiator and targeted recipient(s) of the alert.

2.3.4 Role

2.3.4.1 If an alert is directed by role, then one or more "Role" attributes must be included in alerts to describe the public health functions for which a person is responsible. Roles represent the combination of program functions and expertise. They are defined and should be reviewed in *Appendix A* of this document.

2.3.5 Sensitivity

2.3.5.1 An alert must include a "Sensitivity" attribute to indicate whether a message is sensitive or non-sensitive.

EXAMPLE

Answering "yes" to the following example guidelines may help determine that a message is considered to be "sensitive":

- If the information to be communicated were used inappropriately, would it hamper the organization's ability to operate?
- If the information to be communicated were used inappropriately, would it damage the organization's reputation?

2.3.6 Status

2.3.6.1 A "Status" attribute must be used to indicate whether a communication is related to a true event or to a test scenario.

2.3.6.1.a *Actual* - indicates that the alert refers to a live event

2.3.6.1.b *Exercise* - indicates that designated recipients must respond to the message

2.3.6.1.c *Test* - indicates that the message is related to a technical, system test and should be disregarded

2.3.7 Message Type

2.3.7.1 An attribute called "Type" must be included in alerts to identify the kind of a communication or alert.

2.3.7.1.a *Alert* - indicates to the recipient that attention is required

Please note that the "Alert" value of this Message Type attribute should not be confused with the "Alert" value of the Urgency attribute referenced in section *2.3.2 Urgency* above. The Message Type of "Alert" is used to indicate that this is the original message and that attention is required, rather than the message being an update, cancellation, or retraction.

2.3.7.1.b *Update* – indicates prior messages have been updated and superceded

2.3.7.1.c *Cancel* - indicates prior messages have been cancelled

2.3.7.1.d *Error* - indicates prior messages have been retracted

2.4 RECIPIENT ADDRESSING

2.4.1 An alerting system must be able to direct alerts to appropriate, targeted audiences on the bases of the nature of the event, the type of response required, the jurisdictions affected, the urgency of the event, and the sensitivity of the information.

2.4.2 Alerting systems should strive to ensure timely and comprehensive delivery to all required recipients while simultaneously minimizing alerts that may be perceived as redundant or unnecessary.

2.4.3 Alerts may be directed either to a list of specific people or to a combination of parameter values including role, organization, organization type, jurisdiction, or to some combination of both lists.

2.5 ALERTING ACROSS JURISDICTIONS

When alerts must be sent across jurisdictional boundaries, they may be sent either by cascade or direct alerting. Cross-jurisdictional alerting follows the same requirements previously set forth in this document, in addition to the specific requirements noted in this section.

2.5.1 Cross-Jurisdictional Alerting

2.5.1.1 When an alert is sent across state lines, the initiating jurisdiction must also notify federal health partners.

2.5.1.2 When alerts are sent to recipients such as front-line responders or sub-jurisdictions, the parent of the node must also be notified.

EXAMPLE

- If an alert is sent to a local health department, then the state health department must also be notified.
- If emergency room clinicians and local law enforcement agencies receive an alert, then the local health department should also be notified.

2.5.1.3 A notification tree to illustrate node-to-parent relationships must be defined by each state and made available to public health partners, preferably in a public health section of each state's web site.

2.5.2 Cascade Alerting

Cascade alerting will be used for communications sent across jurisdictional boundaries when the receiving system can accept them and meet requirements for delivery performance.

2.5.2.1 Cascade alerts must be transmitted via a secure transport protocol using an ebXML implementation that is compatible with PHIN Messaging Services (PHIN MS). 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*) For more information about secure transport and PHIN MS, please refer to *www.cdc.gov/phin/messaging/index.htm* as well as the *PHIN Preparedness Cross Functional Components Requirements* document. (*www.cdc.gov/phin/CFC.pdf*)

2.5.2.2 Alerting systems receiving a cascade alert should transmit an acknowledgement to the initiating system within 5 minutes of the end of transmission, network performance not withstanding. This receipt is a system-to-system acknowledgement of receipt of the cascade alert, rather than a receipt from a person on the intended recipient list. 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*)

2.5.2.3 For alerts with urgency levels of “Emergency” and “Alert,” systems receiving the cascade alert must transmit a delivery status report to the initiating system every 10 minutes, starting from the time of receipt of the cascade alert and until the delivery is substantially complete. This report indicates the message identifier, the number of recipients targeted to receive an alert and the number who have confirmed receipt, and is formatted in accordance with the PHIN Cascade Messaging Specification.

2.5.2.4 If a cascade alerting recipient system does not respond to the initiating system, then the initiating system will use direct alerting methods to communicate the alert.

2.5.2.5 For alerts with urgency levels of “Advisory” and “Notification,” systems receiving the cascade alert must transmit an acknowledgement to the initiating system within one hour of commencement of normal business hours following receipt of the complete alert. This report indicates the message identifier, the number of recipients targeted to receive an alert and the number to whom delivery has been made, and is formatted in accordance with the PHIN Cascade Messaging Specification.

2.6 SYSTEM INTEGRATION AND DATA EXCHANGE

Systems integration requirements specific to systems supporting partner communications and alerting are included in the section below and describe the types of data that alerting systems should be able to send and receive. This section is limited to describing the types of data exchange that partner communication and alerting 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)

2.6.1 Directory Integration

2.6.1.1 Bi-directional, secure exchange of data with partner organizations is required to support public health investigations across all levels of public health. 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*)

2.6.1.2 A local public health directory must contain contact information, roles, jurisdictions and communication devices for organizations and persons involved in public health. This information must map to the PHIN directory exchange schema to support data exchange.

2.6.1.3 Communication and alerting systems will integrate with a directory as a repository of people, roles, organizations, organization types, and jurisdictions.

2.6.1.4 Directories accessed by partner communication and alerting systems must provide specific attributes, or mapable equivalents, for persons who will be directly alerted. These attribute names are listed and should be reviewed in *Appendix B* of this document. These attributes are in accordance with the PHIN DIR schema v1.1.

2.6.1.5 If an organization's or jurisdiction's emergency response plan includes communication with front-line responders (i.e., clinical care personnel, emergency rooms, paramedics, fire departments, law enforcement, etc.), then the integrated directory must encompass these groups.

2.6.1.6 Directories supporting partner communication and alerting should allow for queries of person by name, role, organization, organization type, and jurisdiction.

2.6.1.7 Communication profiles should be defined to enable and prioritize the list of communication devices that may be used to contact a recipient.

2.6.1.7.a The preferred sequential priority of each communication device should be identified in a contact's profile. For example, a contact may prefer to always be contacted about a public health event first by cell phone, then by home phone number, then by email until successful contact is made.

2.6.1.7.b Each device in a recipient's communication profile should indicate whether it can be accessed during normal business hours or after normal business hours (i.e., a work phone number is usually available only during normal business hours).

2.6.1.7.c Recipients who are required to receive "Emergency" notifications must have access to at least one 24 x 7 x 365 communication device, which must be included in an instance of the directory.

2.6.2 PHIN Common Alerting Protocol (CAP) Integration

2.6.2.1 Systems supporting cascade alerting will use the PHIN specification of the Common Alerting Protocol (CAP) to send and/or receive cascade alerts. For more detail about implementing the PHIN CAP, please reference the PHIN CAP Implementation Guide. (*http://www.cdc.gov/phin/CAP/index.htm*)

2.6.2.1.a A cascading system must be able to parse and act upon the cascade alert parameters from the CAP format as adopted by PHIN.

2.6.2.1.b Alerting systems should be able to process the received alert parameter in accordance with the PHIN Cascade Messaging Specification.

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 communications and alerting and other PHIN functional areas. Operational requirements that span PHIN functional areas should be reviewed in the PHIN Preparedness Cross Functional Components Requirements document. (www.cdc.gov/phin/CFC.pdf)

2.7.1 Users of secure partner communications must agree to the terms and conditions of use of that secure communications channel, must receive regular security training, and may have their access revoked if they are found to have not met any of the requirements therein expressed.

2.7.2 Organizations should define and document the persons authorized to send alerts and the process(es) for approving the content, and should assure that all alerts sent are in compliance with these operating procedures.

2.7.3 Organizations should define and document the guidelines for assigning urgency levels and appropriate alert transport mechanisms based upon the selected urgency level.

2.7.4 Organizations should define and document written protocols for describing processes and timelines for acknowledging receipt of messages based upon the assigned urgency level.

2.7.5 Jurisdictions should have written evidence of efforts made to establish agreements with sovereign jurisdictions (i.e., tribal, international, or military installation borders) to jointly participate in quarterly disaster planning meetings, exchange public health communications and alerts, exchange surveillance data, support mutual aid efforts, and collaboratively participate in at least one drill or exercise per year.

2.7.6 Organizations should execute at least 2 drills/exercises per quarter to ensure that the systems, processes, and personnel supporting communications and alerting activities are successful.

2.7.7 Organizations should test alerting systems at least once per month to ensure that the system functions properly.

2.7.8 Organizations must test their communication methods to ensure they work properly for people hired to fill vacancies in any of the roles named in *Appendix A* of this document or any other persons who will receive "Emergency" alerts,.

2.7.9 People who occupy any of the roles named in *Appendix A* of this document or other persons who will receive "Emergency" alerts must validate information in their communication profiles quarterly.

2.8 SYSTEM SECURITY AND AVAILABILITY

Systems supporting partner communications and alerting 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 accessible to unauthorized users. 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.

APPENDIX A – PUBLIC HEALTH ROLES

The following table defines the public health roles that support partner communications and alerting. Roles that are minimally applicable for a jurisdiction are indicated.

	PRIMARY ROLES	State	County	Hosp	DEFINITION
1	BioTerrorism Coordinator	X	X	X	Responsible for the administration of all BioTerrorism related activities within the jurisdiction.
2	Communicable/ Infectious Disease Coordinator	X	X	X	Responsible for the coordination of all communicable and infectious disease surveillance and investigations and response within the jurisdiction.
3	Health Alert and Communications Coordinator	X	X	X	Responsible for the coordination, implementation, and maintenance of the public health alert and information network for the agency or jurisdiction.
4	Environmental Health Director	X	X		Responsible for the coordination and direction of the jurisdiction's Environmental Health department.
5	Health Officer	X	X		Responsible for the direction and administration of the jurisdiction's Department of Health.
6	Immunization Director	X	X	X	Responsible for management of immunization services within the jurisdiction.
7	Laboratory Director	X	X	X	Responsible for the coordination of the laboratory testing and reporting for the agency or jurisdiction.
8	Public Health Administrator	X	X	X	Responsible for the management of the jurisdiction's Department of Public Health.
9	Chief Epidemiologist	X	X		Responsible for the coordination of the public health surveillance, investigation and response activities within the jurisdiction..
10	Public Information Officer	X	X	X	Responsible for the coordination of public information and emergency risk communications for the jurisdiction.
11	Emergency Management Coordinator	X	X	X	Responsible for the coordination of emergency response activities. Coordinates response activities with other agencies and jurisdictions.
12	Behavioral Health Director	X	X	X	Responsible for the coordination of the mental health services within the agency or jurisdiction.
13	Emergency Medical Services Authority	X	X	X	Coordinates all medical response activities. Coordinates with other agencies and jurisdictions and respond to medical emergencies.
14	Strategic National Stockpile Coordinator	X	X		Responsible for the coordination of the pharmaceutical stockpile planning for the agency or jurisdiction.

15	Emergency Training Coordinator	X	X	X	Responsible for the coordination of the WMD and other emergency training, education, and distance learning activities for the agency.
16	Chief Veterinarian	X	X		Responsible for the coordination of animal disease outbreak response activities for the agency.
17	Weapons of Mass Destruction Coordinator	X	X	X	Responsible for the coordination of all WMD related activities for the agency.
18	Public Health Nursing Director	X	X		Responsible for coordinating the jurisdiction's public health nursing activities.
19	Quarantine Officer	X	X	X	Individual responsible for quarantine enactment and coordination at the local level to include international and travel issues for a region
	Other Roles	**State**	**County**	**Hosp**	**Definition**
20	Laboratory BT	X	X		Responsible for the administration of BioTerrorism laboratory testing within the jurisdiction.
21	Medical Director	X	X	X	Responsible for medical/health services in the jurisdiction
22	Medical Examiner/Coroner		X		Responsible for performing autopsies in the jurisdiction
23	Poison Control Center	X			Office responsible for handling poison injury calls in a region
24	Border Health Director	X			Responsible for cross-border health issues, coordination and communication
25	Microbiologist	X	X		A laboratorian that specializes in performing microbial testing for the jurisdiction.
26	Epidemiologist	X	X	X	Individual who performs analysis of communicable disease and/or BT information for their jurisdiction.
27	Technical Training Liaison	X	X		Coordinates training on the use of technical systems including those for IT//communication
28	Emergency Operations Center Coordinator	X	X		Responsible for managing the EOC and for brining together the Individuals who participate as a members of the Emergency Operations Center
29	Medical Society	X	X		Organization responsible for maintaining directory information and communications with the physician community
30	Infection Control Practitioner			X	Responsible for nosocomial and infectious disease in a hospital
31	Emergency Room Director			X	Responsible for running the hospital emergency room
32	School District Nurse		X		Responsible for school health in a school district

33	FBI WMD/BT Agent	X			Responsible for FBI activities and response in a WMD/BT event
34	Public Health Investigator/Contact Tracer	X	X		Individual skilled at tracking down contacts to TB, HIV or STD cases
35	Animal Control Director		X		Responsible for animal bites and quarantine

APPENDIX B – DIRECTORY ATTRIBUTES

The following attributes or mapable equivalents noted as "Required" must be provided by a directory supporting partner communications and alerting systems. Attributes noted as "Optional" may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN DIR schema v1.1.

Attribute	Description	Required/ Optional	Sensitive
Cn (commonName)	Person's common name (first name followed by a surname)	Required	
phindirUID	The person's Unique Identifier within the public health directory (UID).	Required	
sn (surname)	Person's surname, or last name.	Required	
givenName	The person's given, or first, name.	Required	
displayName	Preferred name of a person to be displayed	Optional	
st (stateOrProvinceName)	State or province in which the person is located.	Required	
l (localityName)	City or town in which the person is located.	Required	
phindirCounty	The county in which a person is located.	Required	
Title	The person's job title.	Required	
preferredLanguage	A person's preferred written or spoken language.	Optional[2]	
phindirHighestDegree	Highest academic degree achieved.	Optional	
phindirOtherDegree	Other academic degrees achieved.	Optional	
phindirProfessionalLicense	Identifiers of professional licenses held per jurisdiction.	Optional	
phindirPrimaryExpertise	DN of the person's primary area of expertise.	Optional	
phindirSecondaryExpertise	DNs of other areas of expertise.	Optional	
phindirPrimaryOrganizationRole	DN of the person's primary organizational role affiliation with regard to public health.	Required	
phindirAssociatedOrgRole	DNs of organization / roles that a person is associated with.	Optional	
phindirPublicHealthCommission.	Person's public health commission.	Optional	
preferredDeliveryMethod	The person's preferred method of contact or delivery. This attribute should contain	Required	

	values such as "email" or "work phone".		
telephoneNumber	The person's work telephone number.	Required	
Mail	The person's email address.	Required	
Fax (facsimileTelephoneNumber)	The person's fax number.	Optional	
phindirDirectPhone	Phone number of the direct line to a person's office	Optional	*Sensitive*
Pager	The person's pager number	Required[1]	*Sensitive*
phindirAlphaPager	Number of the person's alphanumeric pager	Required[1]	*Sensitive*
Mobile	The person's mobile phone number	Required[1]	*Sensitive*
phindirSatellitePhone	The person's satellite phone number	Required[1]	*Sensitive*
phindirHomeMail	The person's home email address	Required[1]	*Sensitive*
homeTelephoneNumber	The person's home telephone number	Required[1]	*Sensitive*

[1] These are after-hours and 24 x 7 x 365 contact methods. For persons who might be receiving Level 1 or Level 2 alerts, at least one of these contact methods must be listed in the directory.

[2] English is assumed to be the primary language; this attribute is required only if alerts will be issued in languages other than English.