



PHIN Preparedness

PARTNER COMMUNICATIONS AND ALERTING FUNCTIONAL REQUIREMENTS

Version 1.0

04/26/2005

TABLE OF CONTENTS

1 INTRODUCTION..... 3

2 PARTNER COMMUNICATIONS AND ALERTING FUNCTIONAL REQUIREMENTS..... 3

 2.1 Alerting and Secure Partner Communications 4

 2.1.1 Alerting..... 4

 2.1.2 Secure Partner Communications 6

 2.2 Alert Format 6

 2.3 Vocabulary Standards 7

 2.3.1 Vocabulary Requirements 7

 2.3.2 Severity..... 7

 2.3.3 Delivery Time 8

 2.3.4 Acknowledge..... 8

 2.3.5 Jurisdiction 9

 2.3.6 Jurisdictional Level 9

 2.3.7 Role 9

 2.3.8 Sensitive 9

 2.3.9 Status 10

 2.3.10 Message Type 10

 2.4 Recipient Addressing 10

 2.5 Alerting Across Jurisdictions 11

 2.5.1 Cross-Jurisdictional Alerting..... 11

 2.5.2 Cascade Alerting 11

 2.6 System Integration and Data Exchange 12

 2.6.1 Directory Integration..... 12

 2.6.2 PHIN Common Alerting Protocol (CAP) Integration..... 13

 2.7 Operations 14

 2.8 System Security and Availability 15

 2.9 Privacy..... 15

APPENDIX A – ORIGINATING AGENCY IDENTIFIERS 16

APPENDIX B - PUBLIC HEALTH ROLES 18

APPENDIX C – DIRECTORY EXCHANGE ATTRIBUTES: PERSON 22

APPENDIX D – DIRECTORY EXCHANGE ATTRIBUTES: ORGANIZATION 24

APPENDIX E – DIRECTORY EXCHANGE ATTRIBUTES: COMMUNICATION DEVICE..... 26

1 INTRODUCTION

This document describes the Public Health Information Network (PHIN) functional requirements 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 health events. Systems supporting communication and alerting should support alerting protocols, remain constantly available, and integrate with directories for recipient addressing.

The PHIN functional area of Partner Communications and Alerting (PCA) encompasses disseminating information using public web sites, collaborating 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.

Throughout this document, the phrase “communications and alerts” refers to a broad spectrum of notifications, with different levels of significance of the content, among public health partners and potentially to the public. A “health alert” is one category of the broader “communications and alerts” referring specifically to communications about health events that are proactively distributed in order to mitigate an extent or severity of an event. The terms “call-down” and “blast” alerting are introduced in section 2.4 *Recipient Addressing* of this document. “Call-down” alerting refers to a type of message addressing that includes a very specific, defined set of recipients. Alternatively, “blast” alerting describes addressing that includes a very broad set of recipients.

Secure communications are used to ensure that restricted information is available to the intended recipients only. Depending on the sensitive nature of the content, communications and 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 communication” refers to whether the communication channel needs to be secured, not to the technology employed to make the channel secure.

The business processes, information requirements, controlled vocabularies, authority and role definitions, security requirements, system specifications, and technology services are needed to effectively support communications and alerting. This document provides minimum operational requirements necessary for systems supporting PCA 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(s) implemented to support PCA capabilities:

2.1 Alerting and Secure Partner Communications: The purpose of systems supporting PCA is to inform designated recipients about health events or emergencies using an appropriate method of communication for the event.

2.2 Alert Format: A well-defined format for communications and alerts provides for 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 standards organizations. Where they exist, systems supporting PCA should use them. As additional standards are defined, they should be accepted and implemented.

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

2.5 Alerting Across Jurisdictions: When communications or alerts must be sent across jurisdictional boundaries, different methods of delivery may be applied.

2.6 System Integration and Data Exchange: Systems supporting PCA should be able to exchange directory data with partners using standardized data exchange formats and protocols to support partner communications.

2.7 Operations: Personnel, roles, and responsibilities necessary to support systems supporting PCA should be clearly defined.

2.8 System Security and Availability: Security of systems supporting PCA includes the protection of data from corruption and access by unauthorized individuals, as well as the protection of systems supporting PCA from sabotage or other failure. A plan must be established for continuing activities when systems supporting PCA are unavailable.

2.9 Privacy: Patients, organizations, and personnel 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 Systems supporting PCA must have the ability to send, receive, manage, and disseminate communications and alerts to participants in public health.
- 2.1.1.2 Systems supporting PCA must securely exchange communications and alerts with other jurisdictions and organizations based on the communication capabilities of the receiving jurisdiction or organization. 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.
 - 2.1.1.2.a Direct alerting will always be used when communications or alerts are distributed within a single jurisdiction. This means that the organization initiating a communication or alert sends it directly to a specific list of recipients rather than first routing it through a recipient alerting system for dissemination.
 - 2.1.1.2.b When communications or alerts must be sent across jurisdictional boundaries, they may be sent either by direct or cascade alerting, or both. Cascade alerting is the process by which a communication or alert is sent to a system that in turn distributes it 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.

- 2.1.1.3 Public health partners must be able to send communications and alerts using direct alerting.
- 2.1.1.4 Public health partners must be able to send communications and alerts to and receive communications and alerts from jurisdictions other than their own.
- 2.1.1.5 Systems supporting PCA must be able to accept and register the confirmation of receipt that indicates a human user has received and acknowledged the communication or alert.
- 2.1.1.6 Initiating alerting systems must be able to identify which organizations or jurisdictions can receive cascade alerts.
 - 2.1.1.6.a If a jurisdiction or organization has been certified as meeting key performance measures for receiving and processing cascade alerts as defined in requirement 2.1.1.2 of this document, then the initiator will use cascade alerting.
 - 2.1.1.6.b If a jurisdiction or organization does not have the ability to receive and process cascade alerts, then the initiator will use direct alerting.
- 2.1.1.7 Systems supporting PCA should provide the ability for jurisdictions to append jurisdictionally specific information to original communications or alerts as long as the message delivery time requirements are met.
 - 2.1.1.7.a Jurisdictions may not alter the content of an original communication or alert, but may append new content to clarify jurisdictional action.
 - 2.1.1.7.b Jurisdictions may delete contact information included in an original communication or alert and substitute contact information relevant to the receiving jurisdiction.
- 2.1.1.8 Communications and alerts must support an audit trail for edits or alterations.
 - 2.1.1.8.a Communications and alerts that are edited or altered for jurisdictional clarification must be appended to the end of the original communications or alert.
 - 2.1.1.8.b When an original communication or alert is edited or altered, the editing jurisdiction's unique agency identifier must be appended to the original communication or alert after the originator's unique agency identifier.
- 2.1.1.9 Systems supporting PCA must generate a real-time delivery status report containing the number of recipients targeted to receive a communication or alert and the number who have confirmed receipt.
- 2.1.1.10 Systems supporting PCA must be able to securely archive communications and alerts that they send (e.g., initiate, forward, cascade).
- 2.1.1.11 Systems supporting PCA must be able to securely retrieve, reconstruct, and resend archived communications and alerts that they previously sent (e.g., initiated, forwarded, cascaded).

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 web sites that meet certification requirements may be used to satisfy secure delivery of sensitive information.

Epi-X is one example of a secure web site that partners may use. More information about Epi-X is available at <http://www.cdc.gov/epix>; however, Epi-X is not required as long as the partner has other means of providing secure communication.

- 2.1.2.3 Secure communications should support the ability for authorized users to post and receive content and to facilitate broader collaboration functions.
- 2.1.2.4 Sensitive communications and alerts require secure transport and restricted access and distribution.
 - 2.1.2.4.a When notification of a sensitive communication or alert cannot be sent using secure channels of communication, notification of content delivery in a secure channel may be sent over non-secure means (e.g., e-mail, fax) as long as the notification itself contains no sensitive content.
 - 2.1.2.4.b When notification of delivery is sent using non-secure channels of communication, the notification must include a reference to a secure web site where the sensitive information is accessible to authenticated users.
 - 2.1.2.4.c Secure systems supporting PCA must be able to authenticate the identity of a user before delivering sensitive information.
- 2.1.2.5 Secure web presentation over the Internet should be implemented using a secure encryption technology, such as Secure Sockets Layer (SSL).
- 2.1.2.6 Systems supporting PCA must be able to recognize secure versus non-secure channels of transmission. PHIN requirements related to secure transport should be reviewed in *PHIN Preparedness Cross Functional Components Requirements*, available at www.cdc.gov/phin.

2.2 ALERT FORMAT

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

- 2.2.1 Each communication or alert must address a single issue rather than combining multiple issues in one communication or alert.

- 2.2.2 To support downward compatibility, the content of a communication or alert must be translatable and sharable in simple text format for information delivered by devices that do not support graphics (e.g., Blackberry, pager, telephone).
- 2.2.3 All communications and alerts must include: a unique message identifier; a human readable, unique originating agency identifier; an indication of sensitivity; an indication of severity (as described in section 2.3.2 *Severity* of this document); an indication whether acknowledgment is required; and a succinct title. The data sets for these required attributes vary by delivery method. For these device-specific requirements, please refer to *PHIN Communication and Alerting Implementation Guide*, available at www.cdc.gov/phin.
- 2.2.3.1 The required unique, originating agency identifier must adhere to a specified format that recipients can interpret upon reading, as defined in *Appendix A* of this document.
- 2.2.4 For health alerts specifically, a specified, pre-defined unique message identifier format must be used. For this required message identifier formatting, please refer to *PHIN Communication and Alerting Implementation Guide*, available at www.cdc.gov/phin.
- 2.2.5 Communications and alerts may optionally include: issuing date and time; delivery time (as defined in section 2.3.3 *Delivery Time* of this document); intended audience; name, title, and contact information of the issuing partner; required actions; instructions for sharing the information; Public Health Agency's emergency contact information; estimated time for follow up; page numbers (if multiple pages); and approved content.

2.3 VOCABULARY STANDARDS

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

2.3.1 Vocabulary Requirements

- 2.3.1.1 Partner communications, direct messages, and cascade alerts must support and use the defined vocabulary structure defined in this section for the specific data elements and valid value sets.

2.3.2 Severity

- 2.3.2.1 Systems supporting PCA must include a "Severity" attribute to describe the level of significance to the recipients, using the values defined in the table below. The table below shows the values that must be used for this attribute, the default definitions for "Severity" as a CAP attribute, and the public health definition that must be used for all public health related communications and alerts.

Severity value	CAP Attribute definition	Public Health definition (to be used in communications and alerts)
Extreme	Extraordinary threat to life or property	Extraordinary threat to life or health; warrants immediate action or attention
Severe	Significant threat to life or property	Significant threat to life or health; warrants immediate action or attention
Moderate	Possible threat to life or property	Possible threat to life or health; may require immediate action
Minor	Minimal threat to life or property	Minimal or non-existent threat to life or health; unlikely to require immediate action
Unknown	Unknown threat to life or property	Unknown level of threat to life or health; may require immediate action

2.3.2.2 Systems supporting PCA that use an existing scale to indicate the significance of a communication or alert must use the “Severity” values defined in requirement 2.3.2.1 of this document, but may map existing values to those listed in requirement 2.3.2.1. For mapping guidelines, please refer to *PHIN Communication and Alerting Implementation Guide*, available at www.cdc.gov/phn.

2.3.2.2.a The “Severity” value appropriate to the significance of a communication or alert must be included as a required attribute in all communications and alerts, as described in requirement 2.2.3 of this document.

2.3.2.2.b Mapped, existing values may be included in communications and alerts as optional content, as described in requirement 2.2.5 of this document.

2.3.3 Delivery Time

2.3.3.1 Systems supporting PCA must include a “Delivery Time” attribute used to indicate how quickly the communication or alert must be delivered to the recipient (and acknowledged, when acknowledgement is required).

2.3.3.1.a *Within 15 minutes* – no more than 15 minutes should elapse

2.3.3.1.b *Within 60 minutes* – no more than 60 minutes should elapse

2.3.3.1.c *Within 24 hours* – no more than 24 hours should elapse

2.3.3.1.d *Within 72 hours* – no more than 72 hours should elapse

2.3.4 Acknowledge

2.3.4.1 An “Acknowledge” attribute must be used to indicate whether a return-receipt is required from the recipient to confirm the communication or alert was received.

2.3.4.1.a *Yes* - indicates that the communication or alert requires a return-receipt from the recipient (e.g., “sign and fax back” verbiage on faxed alerts)

- 2.3.4.1.b *No* – indicates that the communication or alert does not require a return-receipt from the recipient
- 2.3.4.2 When the “Acknowledge” attribute value is “Yes”, all defined contact methods for each recipient must be fully exhausted in an attempt to collect a return-receipt.
- 2.3.4.3 When the “Acknowledge” attribute value is “Yes”, systems supporting PCA must attempt delivery of communications or alerts to each recipient until the recipient personally confirms receipt.
- 2.3.4.4 When the “Acknowledge” attribute value is “Yes”, systems supporting PCA must attempt delivery using the sequential contact methods specified in each user’s communications profile and/or alternate contacts (as defined in section 2.6.1 *Directory Integration* of this document) for the recipient until the recipient personally confirms receipt of the communication or alert.

2.3.5 Jurisdiction

- 2.3.5.1 Communications and alerts must include an attribute for “Jurisdiction” to indicate the targeted recipient(s).

Federal Information Processing Standards (FIPS) codes will be used to indicate the jurisdiction targeted by the communication or alert. Partners may visit www.census.gov/geo/www/fips/fips.html, among other resources, for more information regarding FIPS codes.

2.3.6 Jurisdictional Level

- 2.3.6.1 Communications and alerts must include an attribute to indicate the targeted recipients’ jurisdictional level.
 - 2.3.6.1.a *National* – indicates national recipients
 - 2.3.6.1.b *State* – indicates state recipients
 - 2.3.6.1.c *Territorial* – indicates territorial recipients
 - 2.3.6.1.d *Local* – indicates local recipients

2.3.7 Role

- 2.3.7.1 If a communication or alert is directed by recipients’ roles, then one or more “Role” attributes must be included to describe the public health functions for which a person is responsible. Roles represent a combination of program functions and expertise. They are defined and should be reviewed in *Appendix B* of this document.

2.3.8 Sensitive

- 2.3.8.1 A communication or alert must include a “Sensitive” attribute to indicate whether it contains sensitive or non-sensitive content.
 - 2.3.8.1.a *Yes* – indicates sensitive content is included
 - 2.3.8.1.b *No* – indicates non-sensitive content is included

EXAMPLE

Answering “yes” to the following example guidelines may help determine whether content is considered to be “sensitive”:

- If the content of a communication or alert were used inappropriately, would it hamper the organization’s ability to operate?
- If the content of a communication or alert were used inappropriately, would it damage the organization’s reputation?

2.3.9 Status

2.3.9.1 A “Status” attribute must be used to indicate whether a communication or alert is related to a true event or to a test scenario.

2.3.9.1.a *Actual* - indicates that the communication or alert refers to a live event

2.3.9.1.b *Exercise* - indicates that designated recipients must respond to the communication or alert

2.3.9.1.c *Test* - indicates that the communication or alert is related to a technical, system test and should be disregarded

2.3.10 Message Type

2.3.10.1 A “Message Type” attribute must be included to categorize the communication or alert.

2.3.10.1.a *Alert* - indicates an original communication or alert

2.3.10.1.b *Update* – indicates prior communication or alert has been updated and superceded

2.3.10.1.c *Cancel* - indicates prior communication or alert has been cancelled

2.3.10.1.d *Error* - indicates prior communication or alert has been retracted

2.4 RECIPIENT ADDRESSING

2.4.1 Communication and alerting systems must send, receive, and manage “call-down” and “blast” communications and alerts on a 24/7/365 basis to key stakeholders. 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.

2.4.1.1 Communications and alerts may be directed either to a list of specific people or to a combination of parameter values including role, organization, organization type, jurisdictional level, or to some combination.

2.4.2 Systems supporting PCA must be able to direct communications and alerts to appropriate, targeted audiences based on the nature of the event, the delivery time, the type of response required, the jurisdictions affected, the severity of the event, and the sensitivity of the information.

- 2.4.2.1 Systems supporting PCA should be able to target and process a single communication or alert using different delivery times and/or acknowledge requirements for different recipients (e.g., Delivery Time attribute value is “60 minutes” and Acknowledge attribute value is “Yes” for some audiences; other audiences receive the same alert with Delivery Time attribute value of “24 hours” and Acknowledge attribute value of “No”).
- 2.4.3 Alerting systems should strive to ensure timely and comprehensive delivery to all required recipients while simultaneously minimizing communications and alerts that may be perceived as redundant or unnecessary.

2.5 ALERTING ACROSS JURISDICTIONS

When communications and 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 a communication or alert is sent across state lines, the initiating jurisdiction may also need to notify national health partners, depending upon the nature of the content.
- 2.5.1.1.a Communications and alerts that are interstate in nature warrant national level notification.
- 2.5.1.2 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.
- 2.5.1.3 When communications or alerts are sent to recipients such as front-line responders or sub-jurisdictions, the parent of the node must also be notified.

EXAMPLE

- If a communication or 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 a communication or alert, then the local health department should also be notified.

2.5.2 Cascade Alerting

Cascade alerting will be used for sending communications and alerts across jurisdictional boundaries when the receiving system has been certified as meeting key performance measures for receiving and processing cascade alerts.

- 2.5.2.1 Cascade communications and alerts must be transmitted via a secure transport protocol using an ebXML implementation that is compatible with PHIN Messaging Services (PHIN MS). For more information about secure transport and PHIN MS, please refer to *PHIN Preparedness Cross Functional Components Requirements*, available at www.cdc.gov/phn.

- 2.5.2.2 Systems receiving a cascade communication or alert must 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 communication or alert, not a return-receipt from a person on the intended recipient list.
- 2.5.2.3 For communications and alerts with a Delivery Time attribute value of “within 15 minutes” or “within 60 minutes”, the receiving system must transmit a delivery status report to the initiating system every 10 minutes, starting from the time of receipt of the cascade communication or alert and until the delivery is substantially complete.
 - 2.5.2.3.a A delivery status report must include the unique message identifier, the number of recipients targeted to receive the communication or alert, and the number who have confirmed receipt.
- 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 disseminate the communication or alert.
- 2.5.2.5 For communications and alerts with a Delivery Time attribute value of “within 24 hours” or “within 72 hours”, the receiving system must transmit an acknowledgement to the initiating system within one hour of commencement of normal business hours following receipt of the complete communication or alert.
 - 2.5.2.5.a An acknowledgement must include the unique message identifier, the number of recipients targeted to receive a communication or alert and the number to whom delivery has been made.

2.6 SYSTEM INTEGRATION AND DATA EXCHANGE

Systems integration requirements specific to systems supporting PCA are included in the section below and describe the types of data that PCA should be able to send and receive. This section is limited to describing the types of data exchange that PCA must support; not the requirements for transporting the data. Bi-directional, secure exchange of data with partner organizations support public health investigations across all levels of public health. 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.

2.6.1 Directory Integration

- 2.6.1.1 Systems supporting PCA must securely exchange public health directory information with public health partners. 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.
- 2.6.1.2 A local instance of a public health directory must contain contact information, roles, jurisdictions and communication devices for organizations and persons involved in public health.

- 2.6.1.2.a A local instance of a public health directory must map to the PHIN directory exchange schema v2.0 in order to support data exchange.
- 2.6.1.2.b A local instance of a public health directory must support people having multiple roles.
- 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 systems supporting PCA must provide specific attributes, or mapable equivalents, for persons who will be directly contacted. These attributes are in accordance with the PHIN directory exchange schema v2.0, and should be reviewed in *Appendix C*, *Appendix D*, and *Appendix E* of this document.
- 2.6.1.5 If an organization's or jurisdiction's emergency response plan includes communication with front-line responders (e.g., clinical care personnel, emergency rooms, paramedics, fire departments, law enforcement), 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 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 recipient's profile. For example, a contact may prefer to always be contacted about a health event first by cell phone, then by home phone number, then by e-mail 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 (e.g., a work phone number is usually available only during normal business hours).
- 2.6.1.8 Recipients who are required to receive communications and alerts with a Delivery Time attribute value of "within 15 minutes", "within 60 minutes" or "within 24 hours" must have access to one or more communication devices, providing the ability to reach the recipients on a 24/7/365 basis.
- 2.6.1.9 Systems supporting PCA must be able to contact all device types listed in a recipient's profile.

2.6.2 PHIN Common Alerting Protocol (CAP) Integration

- 2.6.2.1 Partners must be able to send cascade communications and alerts using the PHIN specification of the Common Alerting Protocol (CAP). For more detail about implementing the PHIN CAP, please reference *PHIN Communication and Alerting Implementation Guide* available at www.cdc.gov/phn.

- 2.6.2.2 Systems that can receive cascade communications and alerts must be able to parse and act upon the cascade communication or alert parameters from the CAP format as adopted by PHIN.
- 2.6.2.3 Systems that can receive cascade communications and alerts should be able to process the received communication or alert parameter in accordance with *PHIN Communication and Alerting Implementation Guide*, 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 communications and alerting and other PHIN functional areas. Operational requirements that span PHIN functional areas should be reviewed in “PHIN Preparedness Cross Functional Components Requirements”, available at www.cdc.gov/phin.

- 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 communications and alerts and the process(es) for approving the content, and should ensure that all communications and alerts sent are in compliance with these operating procedures.
- 2.7.3 Organizations should define and document the guidelines for assigning delivery times and appropriate alert transport mechanisms based upon the selected delivery time.
- 2.7.4 Organizations should define and document written protocols for describing processes and timelines when the Acknowledge attribute value is “yes”.
- 2.7.5 Jurisdictions should have written evidence of efforts made to establish agreements with sovereign jurisdictions (e.g., 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 or 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 systems function 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 B* of this document or any other persons who will receive communications and alerts with a Delivery Time attribute value of “within 15 minutes”, “within 1 hour” or “within 24 hours”.
- 2.7.9 People who occupy any of the roles named in *Appendix B* of this document or other persons who will receive communications and alerts with a Delivery Time attribute value of “within 15 minutes”, “within 1 hour” or “within 24 hours” must validate information in their communication profiles quarterly.

2.8 SYSTEM SECURITY AND AVAILABILITY

Systems and data supporting PCA 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/phn.

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 “PHIN Preparedness Cross Functional Components Requirements”, available at www.cdc.gov/phn.

APPENDIX A – ORIGINATING AGENCY IDENTIFIERS

The following examples illustrate the required format for originating agency identifiers, per section 2.2 Alert Format of this document.

- A.1 For national PHIN partners (currently just the CDC), the originating agency identifier is the commonly used agency acronym.

Example identifier – national partner

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

- A.2 For state public health partners, the originating agency identifier is the two character postal abbreviation for the state name.

Example identifier – state partner

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

- A.3 For county public health partners, the originating agency identifier is the concatenation of:

- The two character postal abbreviation for the state in which the agency is located
- A dash (-)
- The name of the county, excluding any special characters or embedded blanks (e.g., alpha-numeric characters only)
- A dash (-)
- The word “COUNTY”

Example identifier – county partner

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

- A.4 For city public health partners, the originating agency identifier is the concatenation of:

- The two character postal abbreviation for the state in which the agency is located
- A dash (-)

- The name of the city, excluding any special characters or embedded blanks (e.g., alpha-numeric characters only)
- A dash (-)
- The word “CITY”

Example identifier – county partner

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

APPENDIX B - PUBLIC HEALTH ROLES

The tables in this appendix define the 35 public health roles that support PCA. Table 1 includes roles that must be assigned within the jurisdictional levels indicated. Table 2 includes additional roles that a jurisdiction should assign.

Table 1 - Required Public Health Roles:

#	PRIMARY ROLE	NATIONAL, STATE, TERRITORIAL	COUNTY	DEFINITION
1	Health Officer	X	X	Responsible for the direction and administration of the jurisdiction's Department of Health.
2	Terrorism Coordinator	X	X	Responsible for the administration of all BioTerrorism related activities within the jurisdiction.
3	Health Alert Network Coordinator	X	X	Responsible for the coordination, implementation, and maintenance of the public health alert and information network for the agency or jurisdiction.
4	Laboratory Director	X	X	Responsible for the coordination of the laboratory testing and reporting for the agency or jurisdiction.
5	Public Health Administrator	X	X	Responsible for the management of the jurisdiction's Department of Public Health.
6	Emergency Management Coordinator	X	X	Responsible for the coordination of emergency response activities. Coordinates response activities with other agencies and jurisdictions.
7	Chief Epidemiologist	X	X	Responsible for the coordination of the public health surveillance, investigation and response activities within the jurisdiction.
8	Public Information Officer	X	X	Responsible for the coordination of public information and emergency risk communications for the jurisdiction.
9	Communicable/ Infectious Disease Coordinator	X	X	Responsible for the coordination of all communicable and infectious disease surveillance and investigations and response within the jurisdiction.

#	PRIMARY ROLE	NATIONAL, STATE, TERRITORIAL	COUNTY	DEFINITION
10	Strategic National Stockpile Coordinator	X	X	Responsible for the coordination of the pharmaceutical stockpile planning for the agency or jurisdiction.
11	Environmental Health Director	X	X	Responsible for the coordination and direction of the jurisdiction's Environmental Health department.
12	Chief Veterinarian	X	X	Responsible for the coordination of animal disease outbreak response activities for the agency.
13	Behavioral Health Director	X	X	Responsible for the coordination of the mental health services within the agency or jurisdiction.
14	Emergency Medical Services Authority	X	X	Coordinates all medical response activities. Coordinates with other agencies and jurisdictions and respond to medical emergencies.
15	Public Health Nursing Director	X	X	Responsible for coordinating the jurisdiction's public health nursing activities.
16	Public Health Logistics Coordinator			Responsible for transportation, facility setup, personnel protective equipment, supplies and other logistical requirements in an emergency response situation.

Table 2 - Optional Public Health Roles:

#	PRIMARY ROLE	NATIONAL, STATE, TERRITORIAL	COUNTY	DEFINITION
17	Immunization Director	X	X	Responsible for management of immunization services within the jurisdiction.
18	Emergency Training Coordinator	X	X	Responsible for the coordination of the WMD and other emergency training, education, and distance learning activities for the agency.
19	Quarantine Officer	X	X	Individual responsible for quarantine enactment and coordination at the local level to include international and travel issues for a region

#	PRIMARY ROLE	NATIONAL, STATE, TERRITORIAL	COUNTY	DEFINITION
20	Laboratory BT	X	X	Responsible for the administration of BioTerrorism laboratory testing within the jurisdiction.
21	Medical Director	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	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 bringing 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			Responsible for nosocomial and infectious disease in a hospital
31	Emergency Room Director			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

#	PRIMARY ROLE	NATIONAL, STATE, TERRITORIAL	COUNTY	DEFINITION
35	Animal Control Director		X	Responsible for animal bites and quarantine

APPENDIX C – DIRECTORY EXCHANGE ATTRIBUTES: PERSON

The following “Person” attributes or mapable equivalents noted as “Required” must be provided by a directory integrating with systems supporting PCA. Attributes noted as “Optional” may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	Description	Required/Optional
cn (commonName)	The person's common name, usually a first name followed by a surname.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
sn (surname)	The person's surname, or last name. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
externalUID	The person's Unique Identifier (UID) within the public health directory. This is a reference from the originating source of the data.	Optional
description	Text description of the person. This often includes their role or work assignment (e.g., Manager for the IT Services group).	Optional
displayName	Preferred name of a person, used when displaying directory entries. This is most often a concatenation of given name and surname.	Optional
givenName	The person's given, or first, name. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
mail	The person's primary e-mail address. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
preferredLanguage	A person's preferred written or spoken language.	Optional
title	The person's job title.	Required
roles	The role(s) a person has within their primary organization.	Required
county	The FIPS code of the person's county for alerting purposes. This is a required field.	Required

Attribute	Description	Required/ Optional
organizations	Distinguished Name (DN) of the primary organization for this person. The DN is the Directory Server name to uniquely distinguish an entry. To simplify implementation, initially only one organization per person will be supported.	Required

APPENDIX D – DIRECTORY EXCHANGE ATTRIBUTES: ORGANIZATION

The following “Organization” attributes or mapable equivalents noted as “Required” must be provided by a directory integrating with systems supporting PCA. Attributes noted as “Optional” may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	Description	Type and Multiplicity
cn (commonName)	Common name of the organization. Values for this attribute will come from the standardized vocabulary lists.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
externalUID	The organization’s Unique Identifier for the sending organization. Used to support record matching.	Optional
description	Text description of the organization.	Optional
fax (facsimileTelephoneNumber)	The organization's fax number.	Optional
l (localityName)	City or town in which the organization is located.	Required
postalAddress	The organization's mailing address.	Required
postalCode	The postal code for this address (e.g., United States ZIP code).	Required
st (stateOrProvinceName)	State or province in which the organization is located.	Required
street	Street address at which the organization is located.	Required
telephoneNumber	The organization's telephone number.	Required
county	The FIPS code of the county in which an organization is located.	Required
alertingJurisdictions	A list of the county FIPS codes which define an organization’s jurisdictional boundary for alerting.	Required

Attribute	Description	Type and Multiplicity
primaryOrganizationType	An organization's primary organization type. Values for this attribute will come from the standardized vocabulary lists.	Required

APPENDIX E – DIRECTORY EXCHANGE ATTRIBUTES: COMMUNICATION DEVICE

The following “Communication Device” attributes or mapable equivalents noted as “Required” must be provided by a directory integrating with systems supporting PCA. Attributes noted as “Optional” may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	Description	Type and Multiplicity
cn (commonName)	Common name of the communication device, such as email or telephone. This value needs to be unique within for a specific person.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
description	Text description of the communication device.	Optional
deviceName	This field contains the unique name for each device. This name will be used in most user interfaces (UI) to select the associated device.	Required
deviceType	This field contains the type of device (e.g., e-mail, telephone, fax, pager). Values for this attribute will come from the standardized vocabulary lists.	Required
coverage	This field contains the type of coverage for the device (e.g., Normal Business Hours, After Hours, 24/7/365). Values for this attribute will come from the standardized vocabulary lists.	Required
emailAddress	This field contains the e-mail address for the device. E-mail address is only valid for devices that support email addressing. Standard e-mail formatting applies.	Optional
areaCode	This field contains the area code for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional
exchange	This field contains the exchange for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional

Attribute	Description	Type and Multiplicity
line	This field contains the line for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional
rank	Rank defines the contact order for devices. When contacting people, this order will be followed until the person is reached. The rank is unique for all of a person's communication devices.	Optional
pin	This field contains the pin associated with a device. This field is only valid for devices that require pin numbers (e.g., pagers).	Optional
countryPrefix	This field contains the country prefix for foreign phone numbers. Values for this attribute will come from the standardized vocabulary lists.	Optional
internationalNumber	This field contains the phone number for international numbers. This field is only valid for international phone numbers. Non-international numbers should use the areaCode, exchange and line attributes previously defined.	Optional
emergencyUseInd	This field indicates if the device can be used for emergency contact. This is a Boolean field and should be set to "true" if selected. All other values will be interpreted as false.	Optional
homeInd	This field indicates if the device is associated with a person's home. This indicator should be used to protect the identity of the defined device that is associated with a person home. If the identity of this device needs to be protected, this indicator should be set. This is a Boolean field and should be set to "true" if selected. All other values will be interpreted as false.	Optional