PUBLIC HEALTH INFORMATION NETWORK (PHIN)

PHIN COMMUNICATION AND ALERTING (PCA) GUIDE

Version 1.3

April 27, 2010

VERSION HISTORY

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.0	Robb Chapman	08/21/2008			Version Release
1.1	Robb Chapman	03/17/2009			1, Cascade alerting is now a PHIN requirement, not an optional capability. 2. Add "PCG" value to alerting program attribute to support PHIN Certification testing. 3. Correct the encoding of *sendTime* attribute to be in accord with the current W3C standard. 4. Eliminate inconsistency in requirement (remove requirement) to populate *contact* attribute for severe alerts. 5. Resolve inconsistency re: encoding of *jurisdiction* attribute – ISO3166-1 vs. FIPS.
1.2	Robb Chapman, Tony Pruitt, Mark Jensen	10/30/2009			1. Resolve inconsistency with EDXLDistribution.distributionType element. Value will always be "Report" for cascade messages and "Ack" for cascade acknowledgement messages. 2. Removed the EDXLDistribution.distributionReference from Table 6.1.1 (Cascade Alert "Container"), the reference attribute will only be sent in CAP payload. 3. Added distributionIdentifier attribute to uniquely identify the EDXL distribution message. 4. Modified the example cascade message to incorporate the changes. 5. Modified the example cascade acknowledgement message to incorporate the changes. 6. Formatting changes to tables. 7. Revised audience specification description in Section 3.5.4. 8. Standardized date formats to CAP standard. 9. Removed the "Error" value for message type in Table 5.1 since it is not used by PCA. 10. Changed jurisdictionalLevel to jurisdictionLevel

Version #	Implemented By	Revision Date	Approved By	Approval Date	Reason
1.3	Robb Chapman, Tony Pruitt, Mark Jensen	1/10/2010			Change from PHIN Secure Message Transport (PHIN MS) standard to PHIN Exchange Standard. Affected sections of the document are: 1.1 3.6.1 3.6.1.3 6

TABLE OF CONTENTS

1   INTRODUCTION

The CDC Public Health Information Network (PHIN) is a national initiative to improve the capacity of public health to use and exchange information electronically by promoting the use of standards, defining functional and technical requirements. *PHIN Communication and Alerting* (PCA), one component of PHIN, is a specification of public health alerting capabilities, with an emphasis on interoperability of partners' systems. Alerting in this context means the functionality necessary to manage time-critical information about public health events, send it in real time to personnel and organizations that must respond to and mitigate the impact of these events, and verify and monitor delivery of this information. Systems that provide PCA functionality support these capabilities, integrate them with the organization's other public health information systems and processes, and support interoperability with partners' systems.

PCA is not identical to, or a replacement for, the Health Alert Network (HAN). PCA is a technical specification for alerting. HAN is a public health program that performs alerting. Most organizations with HAN systems are in the process of moving them toward compliance with the PCA specification.

1.1   OBJECTIVES

The objective of this *PHIN Partner Communication and Alerting Implementation Guide* is to provide a comprehensive description of the functional aspects of public health alerting. To perform alerting in a PHIN-compliant manner, systems must process, send, and manage alerts in a manner that conforms to the requirements of this guide.

This Implementation Guide defines functional and technical specifications for systems that support PHIN Communication and Alerting (PCA).

Among other things, this document defines how the following technical standards have been adopted for use by PCA:

- Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element
- Common Alerting Protocol (CAP) V 1.1
- Simple Object Access Protocol (SOAP)

This document is not intended as a tutorial for EDXL, CAP, XML, or SOAP. The reader is expected to have a basic conceptual understanding of messaging and XML in order to use this document.

1.2   AUDIENCE

This guide is designed to be used by analysts who require a better understanding of the business of PHIN Communication and Alerting, and by developers and implementers of PHIN-compliant alerting systems. Understanding and using this guide is a key factor in establishing PHIN compatibility.

1.3   DOCUMENT STRUCTURE

This document contains the following major sections.

- **Background and Problem Domain**: Describes the underlying business problem of cross-jurisdictional alerting. Explains the requirement for some uniformity in public health alerting systems.

- **Application Requirements**: Defines the standard functional behaviors and technical standards necessary to public health alerting systems.

- **PCA Alert Attributes**: Defines the set of alert attributes with which all PCA alerting systems must be semantically compatible, their vocabulary and semantics, and how alerting systems must populate, use, manage and process each attribute.

- **Vocabulary and Valid Value Sets**: Defines the vocabulary employed within the PCA domain and the values that PCA alert attributes can take.

- **PCA Cascade Alert Message Formats**: Defines the cascade alert message formats and the mapping of PCA alert attributes to these formats.

- **Appendices:** Define further the terminology used in this document and provide expanded examples of agency identifiers and audience specifications.

1.4 REFERENCES TO STANDARD ATTRIBUTES AND VOCABULARIES

Standard attributes, attribute names, attribute vocabularies (value sets), and vocabulary semantics for PCA are defined and referenced throughout this document. Public health alerting systems are *not* required to use these standard attribute names and vocabularies internally; they may use other, preferred local attribute names and vocabularies. However, whenever alerts and information about alerts must be conveyed across jurisdictional boundaries, the standard set of attributes and vocabularies must be used. Therefore, the alert information that a system manages must semantically correspond to, and be capable of translation into, the standard attributes and vocabularies. If the information used internally by an alerting system can be translated in this way, then the alerting system is said to "support" the standard attributes and vocabularies, and meets the PCA requirement for attributes and vocabularies.

Throughout this document, attribute names appear italicized. For example, the name of the *alertIdentifier* attribute is italicized in this sentence.

2   BACKGROUND AND PROBLEM DOMAIN

A working group of CDC and state health department representatives began developing components of the PCA standards during the spring and summer of 2003. Ongoing refinement and revision of this work continues under the direction of the CDC's National Center for Public Health Informatics (NCPHI) and new working groups.

2.1   DEFINITION: ALERT

For purposes of this document and for purposes of discussions about PHIN or PCA, the term "alert" means a real-time, one-way communication sent by a PHIN partner organization for legitimate business purposes, to a collection of people and organizations with which the partner has a business relationship, in order to notify them of an event or situation of some importance. The term is meant to include communications that are urgent as well as those that are routine.

A "health alert" is one category of the broader term "alerts." "Health alerts" are communications specifically about health events that are proactively distributed in order to mitigate the extent or severity of the event.

2.2   DEFINITION: PUBLIC HEALTH ALERTING SYSTEM

For purposes of this document and for purposes of discussions about PHIN or PCA, the terms "public health alerting system" and "alerting system" mean a system, or a collection of systems and processes, used by a PHIN partner organization to compose and manage alerts and deliver them to designated recipients in a manner consistent with the PCA requirements set forth here.

An alerting system delivers alerts to recipients using whatever methods of communication can be supported in practice by the system and by the organization, that are sufficient to meet functional and performance requirements, and that are appropriate to the event. The vocabulary and methods for conveying alert information to recipients can vary based upon circumstance, delivery method, and the capabilities of various communication device types, as will be detailed later in this document.

PCA functionality may be implemented using a combination of one or more information systems and manual business processes. The terms "public health alerting system" and "alerting system" within this document are intended to mean the combination of all of the systems and processes employed by a given PHIN partner to implement the PCA functionality. These terms do not imply any requirement for a single information system that performs all of the functions defined.

Further, there is no requirement that a PHIN partner organization own or operate its own alerting system. Under many circumstances it may be practical or preferable for organizations to share the use of a system. For example, a city health department might reasonably make use of an alerting system operated by the state health department within whose jurisdiction it lies, or a health department may make use of an alerting system operated by another government department. The requirement is that PHIN partner organizations have an alerting capability, through whatever arrangement, that meets the PCA specifications.

This document articulates the minimum functionality and operational processes necessary for PCA-compliant alerting systems, but does not preclude a system from incorporating additional functionality beyond what this document addresses.

2.3   OTHER DEFINITIONS

Definition of other terms used in this document are provided in <u>Appendix 1: Definition of Terms</u>.

2.4   REQUIREMENT FOR UNIFORMITY IN PARTNER COMMUNICATIONS AND ALERTING

A primary objective of PHIN is to establish the ability for public health organizations to communicate and work effectively with each other, especially during emergencies. It is important that public health alerting systems achieve a basic level of standardization with respect to functional capability, behavior, and terminology. Because many, if not most, public health events are cross-jurisdictional in scope, any individual working within any jurisdiction may be subject to receiving alerts originating from many different health departments or public health jurisdictions. In the event of an emergency or time-critical event, a certain degree of uniformity of alert message structure, vocabulary, semantics, and process is critical to clarity and accuracy in communications and to reducing the risk of communications being mismanaged or misunderstood across multiple organizations and jurisdictions. One objective of PCA, therefore, is that alerting systems be sufficiently consistent in the type of information sent to recipients, be semantically consistent with a standard set of attributes and vocabularies, be consistent as to how alerting terminology corresponds to system behaviors and human processes, and be consistent in the type of information stored for historical reporting and auditing purposes.

This PCA Implementation Guide therefore addresses:

- a common set of PCA attributes and vocabularies;

- the content of information in human-readable alerts;

- the correspondence of PCA attributes to system functionality;

- the requirements for persistent storage of information about alerting activities; and

- the composition and interpretation of system-to-system (Cascade) alert messages.

At the same time, another objective of PCA and PHIN in general is that each partner has the maximum possible leeway in choosing an alerting solution that works for their particular circumstance and environment.

3   APPLICATION REQUIREMENTS

3.1   ALERTING

A PHIN partner organization's alerting system must be able to create and manage alerts and send them to people and organizations that participate in public health activities within the organization's jurisdiction.

In particular, alerting systems must be able to send alerts on a 24/7/365 basis to those key personnel and organizations that are critical to the jurisdiction's emergency response plan. The identification of these "key personnel and organizations" is the responsibility of the jurisdiction.

Alerting systems must be able to "broadcast" alerts to all recipients within the scope of the system, but also target alerts to and limit distribution to specific audiences as circumstances require.

Alerting systems must support a variety of communication device types, in order that real-time communications with these people and organizations will be practical and effective, including emergency and after-hours communications.

Alerting systems must support the ability for alert recipients to confirm that they have received and acknowledge an alert. This acknowledgement must involve conscious deliberate action on the part of the recipient, such as pressing a specific key on a telephone (i.e. the fact that a phone went "off-hook" is not a confirmation that an intended recipient is aware of an alert). The alerting system must be able to record each recipient's acknowledgement and report it.

Alerting systems must be able to display or report delivery status information to the operator of the system, in near-real time, that includes the number of recipients targeted to receive an alert and the number that have received it, or, when confirmation is required, that have confirmed receipt.

3.2   SECURE COMMUNICATION

Alerting systems must provide a means of secure communication for delivery of alerts containing sensitive content. The term "secure communication." in the context of PCA, refers to methods used to ensure that the restricted information is delivered to and is available to only the intended recipients; it refers to the fact that a communications method is secured, but does not refer to the technology used to make the method secure.

Secure communication involves (1) the ability to restrict distribution of the alert and restrict access to the sensitive content, (2) the ability to authenticate the identity of a user before delivering the sensitive content, and (3) a message transport that is not easily open to unauthorized access. For example:

- Standard SMTP e-mail should not be used for secure communication because it is travels the public Internet in plain text and is notoriously easy to "sniff", does not protect against unauthorized access to message content, and does not reliably restrict access to only the intended recipients;
- Standard SMTP email entirely within a network and email system administered by the partner organization, coupled with security controls governing access to the email system, may be is suitable for secure communication;
- Fax transmission is unsuitable for secure communication because there is no recipient authentication or control over who might pick up the fax;

- Delivery by land-line and digital phone networks can be used in conjunction with a recipient authentication method, e.g. requiring entry of a PIN number.

Alerts with sensitive content must:
- be tagged as sensitive by having the *sensitive* attribute set to "Sensitive";
- be sent using a secure communication method.

Sensitive content may be defined as content whose inappropriate distribution or use could compromise the public health organization's effectiveness or reputation.

Alerting systems must be able to distinguish secure versus non-secure methods of communication.

3.3   ALERT ATTRIBUTES AND VOCABULARIES

Standard attributes and vocabularies for describing the parameters of an alert are critically important when exchanging alerting information across jurisdictions. PHIN Communication and Alerting, to the maximum extent possible, makes use of standard vocabularies and data structures already defined by standards development organizations.

Public health alerting systems must support, not necessarily use, the standard attribute names and vocabularies defined in this document (see section 1.4). The attributes that alerting systems must support are detailed in Table 4.2. The vocabularies that alerting systems must support are detailed in and Table 5.1.

3.4   ALERT FORMAT

A degree of standardization of alert format helps to ensure that public health organizations can communicate effectively within their jurisdictions and with other jurisdictions, especially during emergencies.

Each alert should address a single issue or health event, rather than combining multiple issues and events into one alert.

An alerting system should render alert content in a manner appropriate to the characteristics of the device on which the recipient will receive it. For purposes of discussion of PCA, the following content forms are defined:
- long text – content rendered in a form appropriate for email, fax, or web presentation;
- short text - content rendered in a form appropriate for SMS and pagers;
- voice text – content rendered in a form appropriate for voice delivery or automated voice delivery by phone.

Alert format requirements vary depending on the content form.

Generally, all alerts must include the following attributes:

• *alertIdentifier* - a unique message identifier;

• *agencyName* - the official name of the agency originating the alert; or where text size is constrained, *agencyAbbreviation* - an abbreviated representation of agency name;

• *sendTime* - the date and time the alert was initiated;

• *severity* - an indication of the severity of the event;

• *title* - the title or "subject line" of the alert;

• *message* - the message text.

Under some circumstances alerts must also include additional information:

• *sensitive* - if the alert contains sensitive content, this fact must be conveyed to recipients.

• *acknowledge* - if acknowledgement of receipt is required, this fact must be conveyed to recipients.

• *status* - if the alert is an exercise or test, this fact must be conveyed to recipients.

• *msgType* - If the alert is an update, cancellation, or error, this fact must be conveyed to recipients, along with the identifier of the referenced, previous alert.

Exceptions to these attribute requirements must be made for communication devices that have severe limitations on text size ("short text" devices). Details of these requirements and exceptions are provided in Table 4.2.

3.5   ALERT PROCESSING AND WORKFLOW

The following alert attributes and attribute values correspond to specific processing that an alerting system must execute.

3.5.1   sensitive

If the *sensitive* attribute of the alert is set to "Sensitive", then

- The alert must be sent using a secure communication method.
- The alert must inform recipients that the alert content is sensitive.

3.5.2   acknowledge

If the *acknowledge* attribute is set to "Yes", then:

- The alert must inform recipients that acknowledgement is required.
- The alerting system must attempt to obtain acknowledgement by trying alternate methods of reaching each recipient, for a reasonable period of time or until an acknowledgement is received.

3.5.3   deliveryTime

The *deliveryTime* attribute indicates the target timeframe for delivery of the alert to all recipients. If *acknowledge* is set to "Yes", then *deliveryTime* conveys the target time for both delivery of the alert and recipient acknowledgement

An alerting system must be operationally capable of delivering alerts within the timeframe specified in each alert's *deliveryTime* attribute. For example, to support the *deliveryTime* value of 60 (minutes), an alerting system will need to be operational nights and weekends. However, this is not intended to imply that an alerting system must always meet the target timeframes for delivery. It is understood that meeting these target timeframes is a question of operational capability, system capacity, and size of the target audience, and that organizations are unable to budget for capacity that they may need only very infrequently, or possibly never.   Rather, it is intended that PHIN partner organizations will be operationally ready to deliver alerts within the target timeframe, and will usually be able to meet target timeframes for at least the most critical recipients of any alert.

3.5.4   Audience Specification

Alerting systems must be able to "broadcast" alerts to all recipients within the scope of the system. Alerting systems must also be able to direct alerts only to specified people and

organizations, based for example on the nature of the event, urgency of delivery, type of response required, jurisdictions affected, severity of the event, and sensitivity of the content.

Public health alerting systems should have the capacity to target alerts to specific audiences, using:

- a list of values in the *role*, *jurisdiction*, and *jurisdictionLevel* attributes, that collectively describe a set of people;

- a list of values in the *recipients* attribute, each value identifying one individual person to be included in addition to the set of people described by *role*, *jurisdiction*, and *jurisdictionLevel* attributes.

- no value for any of the above attributes to target all recipients in your jurisdiction.

At least for purposes of sharing audience specifications across jurisdictional boundaries, alerting system must be able to express alert audience specifications in the manner described here.

The conceptual model underlying audience specification is:

A person plays one or more roles within (one or more) jurisdictions
    and/or
A person plays one or more roles within (one or more) organizations.
An organization has responsibility for (one or more) jurisdictions.
Therefore a person plays their roles within the corresponding jurisdictions.

A jurisdiction has a jurisdictional level (national, state, territorial, local).
Therefore, a person plays each of their roles at a jurisdictional level.

The intent of PCA is that a public health alerting system can specify a target audience using nothing more than a set of roles, a set of jurisdictions, and a set or jurisdictional levels. This is so that the organization initiating an alert need know very little about the people and the division of responsibility within other jurisdictions; it needs only to know the types of public health officials that should receive the alert and the set of jurisdictions – more or less, the geographic area - affected by the event. The set of jurisdictions can be mapped to a set of organizations, and the set of organizations and roles can be mapped to specific people.

Audience specification is intended to be straight-forward and interpretable using common sense:

- The lists for *role*, *jurisdiction*, and *jurisdictionLevel* work in tandem; the combination of values in these lists comprises an audience specification.
    - If all three of these lists are empty, it means that this method of audience specification is not being used to limit the audience; therefore all recipients are targeted.

- o If any one of these three lists is populated, it means that this method of audience specification is being used to limit the audience to specific types of recipients. When this is true, if any of the three lists is empty, it means that no value has been specified for the list, meaning that no constraint is being placed on that attribute, so all values of that attribute are selected. For example, if the *role* attribute contains the value "Health Officer" and the *jurisdiction* attribute is empty, then health officers in all jurisdictions are being targeted as recipients.
- If the list of *recipients* is empty, then no individual people are targeted. If the *recipients* list contains values, then the individuals listed are included in addition to the set of people specified by the *role*, *jurisdiction*, and *jurisdictionLevel* attributes.

More formally, the following pseudo-code details how to interpret an audience specification:

```
Send the alert to a person IF
{
        ( the person's identity has a value equal to any value in the recipients attribute )
}
OR
{
        ( at least one role, one jurisdiction, or one jurisdictionLevel has been specified )
        AND
        {
                ( the role attribute is empty )
                OR
                ( any role of the person has a value equal to any value in the role attribute) )
        }
        AND
        {
                ( the jurisdiction attribute is empty )
                OR
                 ( any jurisdiction in which the person plays a role specified above has a value equal
                to any value in the jurisdiction attribute )
        }
        AND
        {
                ( the jurisdictionLevel attribute is empty )
                OR
                ( any jurisdictional level at which the person plays a role specified above has a
                value equal to any value in the jurisdictionLevel attribute )
        }
}
```

For further clarification, the set of all possible permutations of audience specification attributes, populated with example values and accompanied by an interpretation, is found APPENDIX 2: AUDIENCE SPECIFICATION EXAMPLES.

These attributes – *recipients*, *role*, *jurisdiction*, and *jurisdictionLevel* - correspond directly to attributes in the Cascade Alert message format. Outside of Cascade Alerting, they serve currently simply as a conceptual framework for communicating an audience specification across jurisdictions. This communication can occur in a variety of ways; it would be straight-forward, for example, to convey an audience specification from one jurisdiction to another in a plain-text email using attribute-value pairs.

3.6 CROSS-JURISDICTIONAL ALERTING

Cross-jurisdictional alerting occurs when a public health organization must issue an alert to people and organizations outside of its own jurisdiction. Examples of cross-jurisdictional alerting include:

- A federal agency communicating to state or local health department workers, or to physicians, laboratories, etc. within a state's jurisdiction.
- A state health department communicating to local health department workers, or to federal agency workers.
- A local health department communicating to state or federal workers.
- A state health department communicating to workers in another state's health department.

PHIN partner organizations must be able to send alerts to and receive alerts from jurisdictions other than their own.

Management of alerts transmitted across public health jurisdictions poses a number of inter-organizational challenges stemming from the need for rapid and comprehensive distribution of alerts and information to public health workers in all affected jurisdictions, while at the same time respecting the autonomous authority of agency to control the flow of information within its jurisdiction.

The PCA standards at least partially address these challenges through clear specification of the following:

- Cross-jurisdictional alerting
- Direct alerting
- Cascade alerting
- Roles and responsibilities involved

Two possible methods exist for sending alerts across jurisdictional boundaries: <u>direct alerting</u> and <u>cascade alerting</u>.

<u>Direct alerting</u> is the normal process in which an alerting system delivers an alert to a human recipient. This is the normal mode of alerting when the recipient works within the organization or its jurisdiction. However, direct alerting can also be used to accomplish cross-jurisdictional alerting: an alerting system in one jurisdiction sending messages to recipients within another jurisdiction.

<u>Cascade alerting</u> is a process in which an alert is sent as a system-to-system message from one jurisdiction to another; the receiving system then distributes the alert to the appropriate recipients within the receiving jurisdiction. The message contains the alert along with parameters describing how and to whom the message should be delivered. Cascade alerting is the preferred method for sending cross-jurisdictional alerts because it allows PHIN partner organizations to better control public health alerting within their jurisdiction. The capability to send and receive cascade alerts is therefore a PHIN requirement.

Whenever alerts are sent to recipients in another jurisdiction the HAN Coordinator in the other jurisdiction must be included as a recipient. Whenever alerts are sent to recipients in a child jurisdiction of another jurisdiction, the HAN Coordinators in both the parent and the child jurisdiction (if any) must be included as recipients.

EXAMPLES:

• If an alert is sent to officials of a local health department in another state, then the HAN Coordinators in the state health department, and if one exists the HAN Coordinator in the local health department, must also receive the alert.

• If a state health department sends an alert to emergency room clinicians and local law enforcement agencies within the jurisdiction of one of its local health departments, then the HAN Coordinator for the local health department (if any) must also receive the alert.

Jurisdictions receiving an alert from another jurisdiction and distributing it within their own *may not alter the content* of an original alert, but may append new content to qualify the content or set an appropriate context. However, jurisdictions may delete the original point-of-contact information in a received alert and substitute contact information relevant to the receiving jurisdiction.

When a received alert is altered, the unique agency identifier of the organization that has altered the content should be appended to the original alert after the originator's unique agency identifier.

Alerting systems should have an audit trail capability that can capture all such edits and alterations.

3.6.1 Cascade Alerting

This section describes the functional requirements for cascade alerting.

Cascade-capable alerting systems must be able to identify which other PHIN partner organizations can receive cascade alerts (since not all PHIN partners will achieve this capability at the same time).

Whenever sending a cross-jurisdictional alert, all recipient partner organizations that are capable of receiving cascade alert messages must be sent a cascade alert. All other recipient partner organizations must be sent a direct alert.

Systems sending cascade alerts must convert information about an alert, in whatever form it is expressed internally, into the standard set of attributes and vocabulary used for cascade alerts.

Alerting systems receiving a cascade alert must parse, process and act upon the alert parameters contained in the cascade message to the best of their ability. The attributes and attribute values in a cascade alert message are directives set by the initiator of the alert regarding how the alert should be processed and handled. These attributes and values correspond directly with the PCA Attributes detailed in Table 4.2, which in turn correspond to desired behavior of an alerting system in processing the alert.

Systems receiving a cascade alert must transmit an acknowledgement message to the initiating system upon receipt of the alert.

Cascade alert messages and acknowledgement messages are implemented using standard message formats and a standard transport protocol. Cascade alert messages and acknowledgement messages must conform to the cascade alert message format specifications in section 6 of this implementation guide.

The message formats employ two XML message schemas that originate outside of PHIN, in the wider domain of emergency management interoperability:

(a) the Emergency Data Exchange Language (EDXL) Distribution Element

(b) the Common Alerting Protocol (CAP)

Cascade alert and acknowledgement messages must be transmitted using the PHIN Exchange, a secure SOAP web service hosted by CDC. Alerting systems my either produce their own XML files and send them using PHIN Exchange, or may instead opt to have the web service produce the XML in the background.

.

3.6.1.1 Emergency Data Exchange Language (EDXL) Distribution Element

The Emergency Data Exchange Language (EDXL) Distribution Element is an XML-based message developed by a consortium of emergency management organizations. EDXL is being widely adopted in the emergency management world and has been adopted for use in the message format for PCA Cascade Alerts. It facilitates emergency information sharing and data exchange across local, state, tribal, national and non-governmental organizations of different professions that provide emergency response and management services. The purpose of the Distribution Element is to route the emergency message to a set of recipients. The Distribution Element may be thought of as a "container" that provides the information needed to route "payload" messages (such as alerts) by including routing information such as distribution type, geography, incident, and sender/recipient.

3.6.1.2 Common Alerting Protocol (CAP)

The Common Alerting Protocol (CAP) is an XML-based specification for alerting and emergency communication messages. CAP was developed by a consortium of emergency management organizations in an effort to enable cross-organizational and cross-system exchange of emergency information. Like EDXL, CAP is being widely adopted in the emergency management world and has been adopted for use in the message format for PCA cascade alerts.   The CAP message may be thought of as the "payload" contained within the EDXL Distribution Element "container."

Because CAP and EDXL are general purpose emergency alerting protocols and are not specifically oriented toward addressing public health emergencies and events, it has been necessary to make adaptations for use in PCA. In these adaptations, only some of the EDXL and CAP attributes are employed, specific PCA-oriented attribute vocabularies are mandated, and a small number of PCA-specific attributes are appended. Since CAP and EDXL were designed to be extensible, these adaptations are easily accommodated.

3.6.1.3 Secure Message Transport

PHIN partners exchanging PCA Cascade Alerts messages are required to transmit and receive these messages using the PHIN Secure Web Services standard. Please refer to "Appendix A: PHIN Requirements – Standards" of the document "Public Health Information Network (PHIN) Requirements".

The alerting system must either:
- use the Cascade Exchange web service (provided as part of PHIN Exchange) to create PCA Cascade Messages and Acknowledgement Messages and route them to appropriate partner organizations, and to receive these messages from partners; or
- create PCA Cascade Messages and Acknowledgement Messages as EDXL/CAP XML files and use the File Exchange web service (provided as part of PHIN Exchange) to route them to appropriate partner organizations, and to receive these files from partners.

3.7 SYSTEM INTEGRATION AND DATA EXCHANGE

Alerting systems must be integrated with and supported by the jurisdiction's local instance of a public health directory. To support alerting functionality, the public health directory must contain contact information, roles, jurisdictions and communication devices for the people and organizations that the alerting system needs to reach, especially those that are critical to the organization's emergency response plan. For people who will be directly contacted by an alerting system, the directory must provide the attributes, or mapable equivalents, specified in the document "PHIN Directory Exchange Implementation Guide."

Recipients who are critical to the jurisdiction's emergency response plan, and those who are subject to receiving alerts with a *deliveryTime* attribute value corresponding to "within 15 minutes", "within 60 minutes" or "within 24 hours", must have communication devices listed in their directory entry that provide the ability to reach them on a 24/7/365 basis.

PHIN partner organizations must exchange public health directory information with other partner organizations using the standard PHIN directory data exchange formats and protocol in order to support partner communications. Their local instance of a public health directory must map to the attributes identified in the PHIN Directory Exchange Message Protocol in order to support data exchange. For additional information refer to the document "PHIN Directory Exchange Implementation Guide."

3.8 OPERATIONS

Personnel, roles, and responsibilities necessary to support alerting systems should be clearly defined.

Users of secure partner communications should receive regular security training, be required to agree to terms and conditions governing use of secure communications channels, and be subject to consequences including possible revocation of system access if they are found to violate these terms and conditions.

Organizations should quarterly validate the contact information, and must test the communication methods, of people that fill any roles considered vital to their emergency response plans or any other persons who are subject to receiving alerts with a Delivery Time attribute value corresponding to "within 15 minutes", "within 60 minutes" or "within 24 hours".

3.9 ARCHIVAL AND RETRIEVAL OF ALERT INFORMATION FOR HISTORICAL REPORTING

Alerting systems must be able to securely archive important information about all alerts that they process (i.e. that they initiate or cascade, and send), and retrieve and reconstruct alerts and alert information from this archive. This capability is critical to enabling PHIN partners to accurately determine the disposition of an alert that was sent across multiple jurisdictions. Information that is required to be stored as part of the alert archive is listed in Table 4.2: PCA Alert Attributes.

4   PCA ALERT ATTRIBUTES

"Table 4.2: PCA Alert Attributes" lists the attributes that are used for description and specification of a PCA alert.

Public health alerting systems are *not* required to use these attributes internally; they may use other local attributes and attribute names instead. Alerting systems may also bundle or combine information into attributes in a different manner than specified here. The attributes listed here, and their corresponding vocabularies, are for use when information about an alert must be conveyed between two or more PHIN partners. This is true when Cascade Alerting is used, but it is also true whenever partners need to coordinate alerting efforts using other automated or manual processes.

In order for an alerting system to be PHIN-compliant, the information about alerts that it uses and stores must have a semantic correspondence, and have the capacity to be translated, at least in principle, to the required attributes specified here and the corresponding vocabularies specified in Section 5. If the information about alerts managed within an alerting system can be translated in this way, then the alerting system meets PCA requirements with regard to attributes and vocabularies.

Example:
The table specifies that there is a *jurisdiction* attribute encoded using either a two-digit FIPS state code, or a five-digit FIPS state-plus-county code (two-digit state code followed by a three-digit county code). A particular public health alerting system could instead have an attribute named "Delivery Area" that is encoded as a string containing the two-letter postal abbreviation for state, optionally followed by a city or county name.

In principle, this information can be transformed into the PCA-standard encoding specified for *jurisdiction*. Therefore, this particular alerting system meets the attribute and vocabulary requirements pertaining to the *jurisdiction* attribute.

Table 4.2 defines how a PHIN-compatible public health alerting system is to support and use each attribute or its semantic equivalent. It defines:

- the vocabulary and semantics of the attribute values;
- whether, and how, the meaning of attribute values must be conveyed to alert recipients;
- whether, and how, each attribute's value affects or corresponds to a functional behavior of the alerting system;
- whether each attribute must be stored persistently as part of the archived information about an alert;
- whether, and how, each attribute corresponds to an EDXL and/or CAP element.

4.1   TABLE ELEMENTS

Table 4.2: PCA Alert Attributes (following) contains the following columns of information about each attribute.

Attribute Name
The PCA attribute name

Req

Indicates whether the attribute must be *supported* by alerting systems. *Support* of an attribute means that the system and/or its operators must be able to translate attributes and vocabularies used locally by an alerting system into the standard attribute and associated encoding, if any, specified here. If this column is set to "Y", then support for the attribute is required. If this column set to "N", then support for the attribute is optional. If this column contains "COND", then support for the attribute is required only under certain circumstances specified in the **Description** column.

Description
A general description of the attribute and its meaning.

EDXL v1.0 Attribute
Name, if any, of the corresponding attribute in the EDXL v1.0 Distribution Element, given as the EDXL Element and Sub-Element name. If this column is blank, there is no corresponding attribute in the EDXL v1.0 Distribution Element specification.
In a few cases, there is a corresponding attribute in *both* the EDXL and CAP message specification.

CAP v1.1 Attribute
Name, if any, of the corresponding attribute in the CAP v1.1 specification, given as the CAP Class and Attribute name. If this column is blank, there is no corresponding attribute in the CAP v1.1 specification.
In a few cases, there is a corresponding attribute in *both* the EDXL and CAP specification.

System Behavior
Specifies whether the attribute governs the alerting system behavior; that is, whether the value of the attribute corresponds to some aspect of how the system should function in delivering the alert. These attributes are of particular importance in cross-jurisdictional alerting, since they represent the intentions of the agency originating the message as to how the alert should be processed or managed. If this column is blank, the attribute has no effect on system behavior.

Convey To Recipient
Specifies whether there is a requirement that the information contained in the attribute be conveyed to human alert recipients, and the conditions under which there is a requirement, and the device types (long text, short text, voice) for which there is a requirement. Implementers of public health alerting systems should use their own judgment in how to convey the information on various device types.

Example:
It is important for an alert recipient to know whether the alert contains sensitive information. Therefore the table specifies that when the *sensitive* attribute is set to the value "Sensitive", this fact must be conveyed to alert recipients, on all device types. In a long text (email, fax, or web page) rendition, this might be conveyed using a text string such as "Caution: Sensitive Message" in bold text. In a short text (SMS or pager) rendition, this might be conveyed as "Sensitive!", to conserve characters. In a voice rendition, this might be conveyed as "This message is sensitive, please use caution." When the *sensitive* attribute is set to "NotSensitive", there is no requirement to explicitly convey this to recipients.

Archive

Specifies whether the attribute (or the semantically corresponding information) must be recorded by the alerting system when the alert is archived for logging and historical reporting purposes.

Encoding

Specifies the encoding that must be used for the attribute value, or the encoding into which the attribute value must be capable of being transformed.

4.2   TABLE 4.2: PCA ALERT ATTRIBUTES

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
agencyIdentifier	Y	Unique identifier of the agency originating the alert. The human-friendly rendering of this identifier is in the attribute: *agencyName*.	EDXLDistribution. senderID	alert. sender		N	Y(1)	Object Identifier (OID) of the agency originating the alert. See also: the vocabulary element "Originating Agency Identifier" in Section 5: Vocabulary.
agencyName	Y	Human readable name of the agency originating the alert. Corresponds to the human-unfriendly OID encoding in *agencyIdentifier*.		Info. senderName		Required: long, voice. For short, *agencyAbb reviation* is recommend ed instead.	N	Text string containing the full official name of the agency originating the alert.
agencyAbbreviatio n	Y	Human readable abbreviated name of the agency originating the alert. Corresponds to the human-unfriendly OID encoding in *agencyIdentifie*r.				Recommen ded: short.	N	Text string containing abbreviated name of the agency originating the alert, encoded as *Originating Agency Abbreviation*. Encoding for Originating Agency Abbreviation is specified in Section 5: Vocabulary.
agencyEmergency Contact	N	Emergency contact information for the person or office at the agency originating the alert that is responsible for providing follow-up and further information.		info. contact		Suggested: long, voice		Phone number and/or email address. May optionally include name or title of person.
sourceName	N(5)	Name of the official initiating the alert.				Suggested: long, voice		Text string
sourceTitle	N(5)	Title of the official initiating the alert.				Suggested: long, voice		Text string

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
alertProgram	Y	Identity of the alerting program.		info. event		Suggested: long, short, voice	Y	Enumeration values are listed in the Vocabulary element "Alerting Program" in Section 5: Vocabulary.
alertIdentifier	Y	Unique alert message identifier.		alert. identifier		Required: long	Y	Every alerting program must have a unique namespace and its own protocol for generating unique alert identifiers. These namespaces and protocols are beyond the scope of this document and of PCA.
sendTime	Y	Date and time the alert is sent	EDXLDistribution. dateTimeSent	alert. sent		Required: long, voice	Y	*datetime* format as specified in *W3C XML Schema Part 2: Datatypes Second Edition*. Ref: http://www.w3.org/TR/xmlschema-2/#dateTime. Times to be given always in Coordinated Universal Time (UTC, also known as Greenwich Mean Time (GMT)). Example: 2008-08-21T20:30:08.073+00:00 corresponds to August 21, 2008 at 3:30:08 (and 73/1000 seconds) PM EST.
severity	Y	Indication of the severity of the event.		info. severity		Required: long, short, voice	Y	Enumeration values: "Extreme", "Severe", "Moderate", "Minor", "Unknown". See the vocabulary element "Severity" in Section 5: Vocabulary.
acknowledge	Y	Indication of whether recipients are required to acknowledge receipt of alert.		info. parameter. acknowledge	Y	If value = "Yes", required: long, short, voice (4)	Y	Enumeration values: "Yes", "No". See the vocabulary element "Acknowledge" in Section 5: Vocabulary.

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
deliveryTime	Y	Target time frame during which alert must be delivered to all recipients. If acknowledge="Yes", target time frame during which alert must be delivered to all recipients and recipients must acknowledge receipt.		info. parameter. deliveryTime	Y	Suggested: long, voice	Y	Enumeration values: 15, 60, 1440, 4320. These correspond respectively to "15 minutes", "60 minutes", "24 hours", and "72 hours". See the vocabulary element "Delivery Time" in Section 5: Vocabulary.
sensitive	Y	Indication of whether the alert contains sensitive content.	EDXLDistribution. distributionType contentObject. confidentiality *and* EDXLDistribution. combinedConfidentiality		Y	If value = "Sensitive", required: long, short, voice (4)	Y	Enumeration values: "Sensitive", "NotSensitive". See the vocabulary element "Sensitive" in Section 5: Vocabulary.
status	Y	Indication of whether this is an actual alert, an exercise, or a test.	EDXLDistribution. distributionStatus	alert. status		If value = "Exercise" or "Test", required: long, short, voice	Y	Enumeration values: "Actual", "Execise", "Test". See the Vocabulary element "Status" in Section 5: Vocabulary.
msgType	Y	Indication of whether this is an original alert, an update to a previous alert, or a cancellation of a previous alert.		alert. msgType		If value = "Update" or "Cancel" required: long, short, voice	Y	Enumeration values: "Alert", "Update", "Cancel". See the Vocabulary element "Message Type" in Section 5: Vocabulary.

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
reference	COND	For alerts with a msgType of "Update" or "Cancel", this attribute must contain the unique identifier (that is, the value of the *alertIdentifier* attribute) of the original alert being updated or cancelled. If msgType = "Alert", then this attribute has no meaning and is not used.		alert. references		If value = "Update" or "Cancel" required: long, short, voice	Y	For PCA purposes, *reference* must contain the *alertIdentifier* of the referenced previous message. The CAP format requires that *reference* include *agencyIdentifier*, *alertIdentifier*, and *sendTime*, separated by commas.
recipients	COND	A list of unique identifiers corresponding to named individuals to whom this alert is to be sent. (3)	EDXLDistribution. explicitAddress. explicitAddressValue		Y (3)	Do *not* convey	Y	Comma separated list. When the list is cross-jurisdictional in scope or is to be shared across organizations, the unique identifiers must be email addresses. These email addresses are intended to function as identifiers for the people and not as delivery addresses. (3)
jurisdiction	COND	A list of public health jurisdictions in which this alert is to be distributed. (3)	EDXLDistribution. targetArea. locCodeUN		Y (3)		Y	Comma-separated list of Federal Information Processing Standards (FIPS) codes. See the vocabulary element "Jurisdiction" in Section 5: Vocabulary.
jurisdictionLevel	COND	A list of jurisdictional levels at which this alert is to be distributed. (3)		info. parameter. jurisdictionLevel	Y (3)		Y	Comma separated list. Enumeration values: "National", "State", "Territorial", "Local". See the Vocabulary element "Jurisdictional Level" in Section 5: Vocabulary.

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
role	COND	A list of public health roles to which this alert is to be distributed. (3)	EDXLDistribution. recipientRole. value		Y (3)	Suggested: long, voice	Y	Comma-separated list. Enumeration values for the role attribute are defined independently by each alerting program and are therefore beyond the scope of this document and of PCA. However, a listing of enumeration values for current alerting programs is provided in Appendix 4.
title	Y	Title or "Subject Line" of the alert		info. headline		Required: long, short (2), voice	Y	Text string
message	Y	The main message text.		info. description		Required: long, voice. For short, suggested that as much of message be included as possible.	Y	Text string
dissemination	N(5)	Instructions for sharing the information further.		info. instruction		Suggested: long, voice	N	Text string
followUpTime	N(5)	Estimated time for follow up.				Suggested: long, voice	N	Text string
approved	N(5)	Indicates whether alert content has been authoritatively approved, e.g. represents an official position or recommendation of the originating agency.				Suggested: long, voice	N	Enumeration values: "Yes", "No".

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
distributionIdentifier	Y	Unique EDXL distribution message identifier.	EDXLDistribution. distributionID				N	Every alerting program must have a unique namespace and its own protocol for generating unique EDXL identifiers. These namespaces and protocols are beyond the scope of this document and of PCA.
distributionType	Y	Required by EDXL	EDXLDistribution. distributionType			No	N	Standard enumeration values are listed in the EDXL v1.1 Distribution Element Data Dictionary. PCA cascade alert messages will always use the value "Report". PCA cascade acknowledgement messages will always use the value "Ack"
urgency	N(7)	Required by CAP but not by PCA.		info. urgency		No (6)	N	Standard CAP enumeration values are listed in the Element Name "urgency" in the Common Alerting Protocol Data Dictionary. A PHIN alerting system must use one of the standard CAP values.
scope	N(7)	A code required by CAP to indicate the intended distribution of the alert. PCA addresses this in other attributes.		alert. scope		No	N	CAP specifies several standard enumeration values which are listed in the Element Name "scope" in the Common Alerting Protocol Data Dictionary. Alerts sent by PHIN alerting systems should always use the value "Restricted", meaning "**for dissemination only to users with a known operational requirement.**"

Attribute Name	Req	Description	EDXL v1.0 Element	CAP v1.1 Element	System Behavior	Convey To Recipient	Archive	Encoding
category	N(8)	A code used by CAP to indicate the category of the event – e.g. meteorological, environmental, etc.		info. category		No	N	CAP specifies several standard enumeration values which are listed in the Element Name "category" in the Common Alerting Protocol Data Dictionary. Alerts sent by PHIN alerting systems should always use the value "Health" – meaning medical and public health.
certainty	N(7)	A code required by CAP to indicate the certainty or likelihood of the event described in the alert.		info. certainty		No	N	CAP specifies several standard enumeration values which are listed in the Element Name "certainty" in the Common Alerting Protocol Data Dictionary. PHIN alerting systems should most probably use the value "Very Likely", which means "Highly likely (p > ~ 85%) or certain".
programType	N(9)	A message type as defined by the alerting program and intended for display to alert recipients. E.g. the HAN program uses the values "Alert", "Update", etc.		Info. parameter valueName = "ProgramType"		Optional (9)	Y	Text string. Program specific vocabulary.

Exceptions and notes:

(1) *agencyIdentifier* needs to be stored persistently only if the alerting system is capable of receiving and processing cascade alerts. Otherwise, since *agencyIdentifier* logically can take on one value, the value for the agency operating this system, it is superfluous.

(2) In a short text rendition, *title* should be included to the extent that it fits, after other required attributes have been accommodated – e.g. it may be necessary to truncate *title*.

(3) The attributes "*role*", "*jurisdiction*", "*jurisdictionLevel*" and "*recipients*" work together to form an audience specification and may be empty in some circumstances. Refer to Section 3.5.4 Audience Specification

(4) If value = "No", does not have to be conveyed to recipients.

(5) Many of the optional attributes listed here are items of information that various workgroups over time have recommended for standard adoption in health alerts and other public health communications. Many were consequently listed in the PHIN Version 1.0 *Partner Communications and Alerting Functional Requirements* specification. These might better be

classified as *information that may be important to convey in an alert, and that particular alerting programs may choose to require,* rather than *attributes* that would be managed as such by an information system e.g. as database columns or message elements. In general, they are simply information elements that may be useful to include in the alert text. They are included here in the interest of completeness and consistency with previous documents, and because it is possible that some may become required attributes at some future time.

(6) It is up to each alerting program whether *urgency* must be conveyed to human alert recipients.

(7) These attributes are required in either the EDXL or the CAP message protocol but are of no value to PCA. Therefore, they are only of consequence to PHIN alerting systems that send Cascade Alert messages, in order to be able to construct a valid XML message, and to the extent that these EDXL/CAP messages may someday be received by systems in emergency response domains other that public health/PHIN. PHIN alerting systems that receive Cascade Alert messages can disregard these attributes.

(8) These attributes are optional in the EDXL and/or the CAP protocol, and are of no value to PCA, and are of consequence only to the extent that these EDXL/CAP messages may someday be received by systems in emergency response domains other that public health/PHIN, e.g. by police or emergency management systems.

(9) Programs such as HAN require the programType to represent the type of alert message (Alert, Notification, etc.). Each alerting program, if they use this attribute, will define their own enumeration values.

5   VOCABULARY AND VALID VALUE SETS

Public health alerting systems are *not* required to use these vocabularies internally; they may use other local vocabularies instead. The vocabularies listed here, and their corresponding attributes in Section 4, are for use when information about an alert must be conveyed between two or more PHIN partners. This is true when Cascade Alerting is used, but it is also true whenever partners need to coordinate alerting efforts using other automated or manual processes.

In order for an alerting system to be PHIN-compliant, the information about alerts that it uses and stores must have a semantic correspondence, and have the capacity to be translated, at least in principle, to the vocabularies specified here and the corresponding attributes specified in Section 4. If the information about alerts managed within an alerting system can be translated in this way, then the alerting system meets PCA requirements with regard to attributes and vocabularies.

Example:

The table specifies that there is a *jurisdiction* attribute encoded using either a two-digit FIPS state code, or a five-digit FIPS state-plus-county code (two-digit state code followed by a three-digit county code). A particular instance of a public health alerting system could instead have an attribute named "Delivery Area" that is encoded as a string containing the two-letter postal abbreviation for state, optionally followed by a city or county name.

In principle, this information can be transformed into the PCA-standard encoding specified for *jurisdiction*. Therefore, this instance of an alerting system meets the attribute and vocabulary requirements pertaining to the *jurisdiction* attribute.

5.1   TABLE 5.1: PCA VOCABULARIES AND VALID VALUE SETS

Vocabulary Element	Description	Valid values	Description of Valid Value
Originating Agency Identifier	A guaranteed-unique identifier for the agency originating the alert.		The OID of the agency originating the alert. Pending completion of an OID and ebXML registry for PHIN, these OIDs are currently managed by the PCA implementation team at CDC. Contact the PHIN for assistance (contact information given at the end of this document).
Originating Agency Abbreviation	An abbreviated, human-readable name of the agency originating the alert. It is used when space limitations prevent the use of the full, official name of the agency, for example, in SMS messages. It corresponds to the human-unfriendly OID encoding in "Originating Agency Identifier".		For national-level PHIN partners (which currently consist of only the CDC), the originating agency abbreviation is the commonly used agency acronym. For state public health partners, the originating agency abbreviation is the two character postal abbreviation for the state name. For county public health partners, the originating agency abbreviation 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 (-), and the word "COUNTY. For city public health partners, the originating agency abbreviation 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 (-); and the word "CITY" Examples are provided APPENDIX 3 –ORIGINATING AGENCY ABBREVIATIONS.
Alerting Program	Identifier of the alerting program sending this alert. An alerting program is a cross-jurisdictional public health function or program that engages in alerts and communications and uses PCA as a vehicle for their delivery.	HAN	Health Alert Network
		Epi-X	Epi-X
		PCG	"PHIN Certification Group": the workgroup performing PHIN Certification of PCA systems. This value may be used for cross-jurisdictional alerts sent during PHIN Certification testing in order not to interfere with production systems.

Vocabulary Element	Description	Valid values	Description of Valid Value
Severity	"Severity" indicates the level of significance of the event. The values used for this vocabulary element are equivalent to those used in the CAP protocol.	Extreme	Extraordinary threat to life or health; warrants immediate action or attention
		Severe	Significant threat to life or health; warrants immediate action or attention
		Moderate	Possible threat to life or health; may require immediate action
		Minor	Minimal or non-existent threat to life or health; unlikely to require immediate action
		Unknown	Unknown level of threat to life or health; may require immediate action
Delivery Time	"Delivery Time" indicates the target timeframe for delivery of the alert, and if acknowledgement is required, for delivery and acknowledgement of the alert.	15	no more than 15 minutes should elapse
		60	no more than 60 minutes should elapse
		1440	no more than 24 hours should elapse
		4320	no more than 72 hours should elapse
Acknowledge	"Acknowledge" indicates whether a manual acknowledgement on the part of the recipient is required to confirm that the alert was received. When the "Acknowledge" attribute has a value of "Yes", all appropriate defined device types for each recipient should be tried, and should be retried for a reasonable time period, in an attempt to obtain an personal acknowledgement. If possible, alternate contacts for recipients should be tried also.	Yes	indicates that the alert requires a manual acknowledgement from the recipient (e.g., "Press 9 to acknowledge"" on phoned alerts)
		No	indicates that the alert does not require a manual acknowledgement from the recipient.

Vocabulary Element	Description	Valid values	Description of Valid Value
Jurisdiction	"Jurisdiction" indicates the political jurisdictional entities (state, county, etc) affected by the public health event, and/or within which alert recipient(s) are targeted.	Federal Information Processing Standards (FIPS) codes for states and counties will be used to indicate the jurisdiction targeted by the alert. Partners may visit www.census.gov/geo/www/fips/fips.html, among other resources, for more information regarding FIPS codes. Each code can be (1) a 2 digit state FIPS code or (2) a 5 digit code consisting of a 2 digit state FIPS code followed by a 3 digit FIPS county code. It is acknowledged that the FIPS state and county codes are not adequate to describe cities, regions, and other jurisdiction entities used by some PHIN partners. The PCA working group has decided, however, that this vocabulary provides the best, most reasonable fit for the present, until a more comprehensive effort can be made to establish an optimal encoding.	
Jurisdictional Level	"Jurisdictional level" indicates whether role players in organizations serving at the national, state, territorial, or local level are targeted as alert recipients.	National	indicates national recipients
		State	indicates state recipients
		Territorial	indicates territorial recipients
		Local	indicates local recipients
Sensitive	"Sensitive" indicates whether the alert contains sensitive content. .	Sensitive	indicates the alert contains sensitive content
		NotSensitive	indicates non-sensitive content
Status	"Status" indicates whether the alert is related to an actual event or to a test scenario.	Actual	indicates that the alert refers to a live event
		Exercise	indicates that designated recipients must respond to the alert
		Test	Test - indicates that the alert is related to a technical, system test and should be disregarded
Message Type	"Message Type" indicates whether the alert is an original alert or is a follow-on to a prior alert.	Alert	indicates an original alert
		Update	indicates prior alert has been updated and superseded
		Cancel	indicates prior alert has been cancelled
Role	"Role" indicates a set of recipients targeted to receive an alert on the basis of the public health function for which they are responsible. Roles represent a combination of program functions and expertise.	Enumeration values for the role attribute are defined independently by each alerting program. These values are therefore beyond the scope of this document and of PCA. However, a listing of enumeration values for current alerting programs is provided in Appendix 4.	

6 PCA CASCADE ALERT MESSAGE FORMATS

This section of the document is pertinent only to alerting systems that use the File Exchange web service (provided as part of PHIN Exchange). These systems must be capable of creating and interpreting XML message files that conform to PHIN Communication and Alerting Cascade Alert Message Formats. Two message formats are defined.

1. PCA Cascade Alert – the format used for Cascade Alert messages.

2. PCA Cascade Acknowledgement – the format used to acknowledge receipt of a Cascade Alert.

Alerting systems that use the Cascade Exchange web service (provided as part of PHIN Exchange) do not need to actually produce messages in these formats; the web service handles all marshalling of XML messages. For purposes of such systems this section of the document is superfluous.

6.1 PCA CASCADE ALERT

The PCA Cascade Alert is formatted using two XML message formats:

- Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element
- Common Alerting Protocol (CAP) Version 1.1.

The EDXL Distribution Element may be thought of as a "container" or "envelope." It provides the information to route "payload" messages by including key routing information such as distribution type, sender, recipient, and geography. The CAP message may be thought of as the alert message "payload" contained within the EDXL Distribution Element "container."   Specifically, the CAP portion of the message is contained within the ContentObject.XMLContent.EmbeddedXMLContent element of the EDXLDistribution.

The Cascade Alert message format is defined in two tables below. The first table lists the elements of the EDXL Distribution Element that are used the message. The second table lists the elements of the CAP protocol that are used in the message.

Further information and complete specifications for these two XML message formats can be found at:

Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element:

        http://docs.oasis-open.org/emergency/edxl-de/v1.0/EDXL-DE_Spec_v1.0.pdf

Common Alerting Protocol (CAP) V 1.1:

        http://www.oasis-open.org/committees/download.php/15135/emergency-CAPv1.1-Corrected_DOM.pdf

6.1.1   Table 6.1.1: Cascade Alert "Container" using Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
EDXLDistribution		XML Structure	REQUIRED. Once.	The container of all of the elements related to the distribution of the content messages.	The <EDXLDistribution> element may include one or more <targetArea> and <contentObject> blocks.
distributionID	distribution Identifier	xsd:string	REQUIRED. Once.	The unique identifier of this distribution message.	MUST be a properly formed - escaped if necessary- XML string.
senderID	agencyIden tifier	xsd:string	REQUIRED. Once.	The unique identifier of the sender.	1. The identifier MUST be a properly formed -escaped if necessary- XML string. 2. The EDXL specification requires that senderID be unique and be in the form: actor@domain-name. The PCA specification uses Object Identifier (OID) as a unique identifier for the agency originating the alert. In order to meet the EDXL requirement, PCA Cascade Messages will adopt the form: agencyIdentifier@domain-name, where agencyIdentifier is the agency OID and domain-name is the agency's domain name. A valid domain name belonging to the agency should be used, however for PCA Cascade Messages it is only present to meet EDXL formatting requirements and is of no consequence to systems receiving the Cascade Alert.

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
dateTimeSent	sendTime	xsd:dateTime	REQUIRED. Once.	The date and time the distribution message was sent.	The date and time is represented in W3C format for the XML *dateTime* data type (e. g., "2008-08-21T20:30:08.073+00:00" corresponds to August 21, 2008 at 3:30:08 (and 73/1000 seconds) PM EST). Refer to *sendTime* attribute listing in Table 4.2: PCA Alert Attributes.
distributionStatus	status	xsd:string with restrictions	REQUIRED. Once	Indication of whether this is an actual alert, an exercise, or a test	Values: Actual, Exercise, Test. MUST be a properly formed - escaped if necessary- XML string.
distributionType	distributionType	xsd:string with restrictions	REQUIRED. Once.	The function of the message.	For PCA Cascade Messages, the value is "Report".
combindedConfidentiality	sensitive	xsd:string	REQUIRED. Once.	Confidentiality of the combined distribution message's content	Enumeration values: "Sensitive", "NotSensitive".

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments

recipientRole	role	List and Associated Value(s)	OPTIONAL. Multiple.	A list of public health roles to which this alert is to be distributed.	The list and associated value(s) is in the form:
					  \<recipientRole>
					    \<valueListUrn>valueListUrn\</valueListUrn>
					    \<value>value\</value>
					  \</recipientRole>
					Multiple instances of the \<value>, MAY occur with a single \<valueListUrn> within the \<recipientRole> container.
					
					The recipientRole container must have at least one \<value> element.
					
					Multiple instances of \<recipientRole> MAY occur within a single \<EDXLDistribution> container but is not recommended.

valueListUrn		xsd:string	REQUIRED. Once.	The Uniform Resource Name (URN) for PHIN roles.	The content of \<valueListUrn> is the Uniform Resource Name (URN) of a published list of values and definitions. For PCA Cascade Messages, the URN for recipientRole is "urn:phin:role".
value	role	xsd:string	REQUIRED. Multiple.	A string denoting a role.	The content of \<value> is a string denoting the role to which this alert is to be sent.

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
explicitAddress		XML Structure	OPTIONAL. Multiple.	A list of unique identifiers corresponding to named individuals to whom this alert is to be sent.	The explicit address of a recipient in the form: 　<explicitAddress> 　　< explicitAddressScheme > explicitAddressScheme </ explicitAddressScheme> 　　<explicitAddressValue> explicitAddressValue </ explicitAddressValue> 　</ explicitAddress > where the content of <explicitAddressScheme> is the distribution addressing scheme used, and the content of <explicitAddressValue> is a string denoting the addressees value. Multiple instances of the < explicitAddressValue >, MAY occur with a single < explicitAddressScheme > within the < explicitAddress > container. Multiple instances of < explicitAddress > MAY occur within a single <EDXLDistribution> container but is not recommended.
explicitAddressScheme		xsd:string	REQUIRED. Once.	The distribution addressing scheme used for the individuals.	For PCA Cascade Messages, the value is "email".
explicitAddressValue	recipients	xsd:string	REQUIRED. Multiple.	A string denoting the identifier for a named individual to whom this alert is to be sent.	Email address of an individual to whom this alert is to be sent. Note that this is intended to function as an identifier for the person and not necessarily a delivery address.

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
targetArea		XML Structure	OPTIONAL. Multiple.	The container element for location information	Multiple <targetArea> blocks may appear in a single <EDXLDistribution> element, in which case the target area for the current message is the union of all areas described in the various <targetArea> structures.
country		xsd:string	OPTIONAL. Multiple.	The code of the country.	The two-character ISO 3166-1 Country Code for the country concerned. More specific target location information can be defined in the <subdivision> elements. MUST be a properly formed - escaped if necessary- XML string.
locCodeUN	jurisdiction	xsd:string	OPTIONAL. Multiple.	A list of U.S. public health jurisdictions in which this alert is to be distributed.	Federal Information Processing Standards (FIPS) codes for states and counties will be used to indicate the jurisdiction targeted by the alert. Each code can be (1) a 2 digit state FIPS code or (2) a 5 digit code consisting of a 2 digit state FIPS code followed by a 3 digit FIPS county code. MUST be a properly formed - escaped if necessary- XML string.
contentObject		XML Structure	REQUIRED Once	The container element for message data and content.	
confidentiality	sensitive	xsd:string	REQUIRED Once	Indication of whether the alert contains sensitive content.	MUST be a properly formed - escaped if necessary- XML string. Enumeration values: "Sensitive", "NotSensitive".

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
xmlContent		XML Structure	REQUIRED Once		
embeddedXMLContent		xsd:string	REQUIRED Once	The <embeddedXMLContent> element is an open container for valid XML from an explicit namespaced XML Schema.	The content MUST be a separately-namespaced well-formed XML document. For PCA Cascade Messages, this element will contain the CAP message. The enclosed XML content MUST be explicitly namespaced as defined in the enclosing <embeddedXMLContent> tag. Enclosed XML content may be encrypted and/or signed within this element.

6.1.2   Table 6.1.2: PCA Cascade Alert "Payload" using Common Alerting Protocol (CAP) Version 1.1

Element	PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
Alert	**group**	**cap. alert. group**	REQUIRED	The container for allcomponent parts of the CAP alert message	(1) Surrounds CAP alert message subelements (2) MUST include the xmlns attribute referencing the CAP URN as the namespace, e.g.: <cap:alert xmlns:cap="urn:oasis:names:tc:emergency:cap:1.1"> [sub-elements] </cap:alert> (3) In addition to the specified subelements, MAY contain one or more <info> blocks.
identifier	**alertIdentifier**	**cap. alert. identifier**	REQUIRED	The identifier of the alert message	(1) A number or string uniquely identifying this message, assigned by the sender (2) MUST NOT include spaces, commas or restricted characters (< and &) (3) For PCA Cascade Messages, every alerting program must have a unique namespace and its own protocol for generating unique alert identifiers.
sender	agencyIdentifier	**cap. alert. sender. identifier**	REQUIRED	The identifier of the sender of the alert message	(1) Identifies the originator of this alert. Guaranteed by assigner to be unique globally. (2) MUST NOT include spaces, commas or restricted characters (< and &) (3) For PCA Cascade Messages, the OID of the organization originally generating and sending this alert.

Element	PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
sent	sendTime	**cap. alert. sent. time**	REQUIRED	The time and date of the origination of the alert message	(1) The date and time is represented in **W3C format for the XML *dateTime* data type** (e. g., "2008-08-21T20:30:08.073+00:00" cooresponds to August 21, 2008 at 3:30:08 (and 73/1000 seconds) PM EST. **Refer to *sendTime* attribute listing in Table 4.2: PCA Alert Attributes.** (2) Alphabetic timezone designators such as "Z" MUST NOT be used. The timezone for UTC MUST be represented as "-00:00" or "+00:00. (3) For PCA cascade messages, this is the date and time that the message was originally sent by the originating agency.
status	alert.status	**cap. alert. status. code**	REQUIRED	The code denoting the appropriate handling of the alert message	Code Values: "Actual" - Actionable by all targeted recipients "Exercise"- Actionable only by designated exercise participants; exercise identifier should appear in <note> "Test" - Technical testing only, all recipients disregard. PCA has no identified need for the additional values supported by CAP: "System" or "Draft".
msgType	msgType	**cap. alert. type. code**	REQUIRED	The code denoting the nature of the alert message	Code Values: "Alert" - Initial information requiring attention by targeted recipients "Update" - Updates and supersedes the earlier message(s) identified in <references> "Cancel" - Cancels the earlier message(s) identified in <references> PCA will not use the values "Ack" or "Error" at this time.

Element	PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
scope	scope	**cap. alert. scope. code**	REQUIRED	The code denoting the intended distribution of the alert message	Code Values: "Public" - For general dissemination to unrestricted audiences. "Restricted" - For dissemination only to users with a known operational requirement. "Private" - For dissemination only to specified addresses. PCA does not require or regard this element but must populate it when using the CAP. Therefore PCA will always use the value "Restricted" to indicate that dissemination should be limited to the PCA systems targeted.
references	reference	**cap. alert. references. group references. group**	CONDITIONAL	The group listing identifying earlier message(s) referenced by the alert message	(1) The extended message identifier(s) (in the form sender, identifier, sent) of an earlier CAP message or messages referenced by this one. (2) For PCA Cascade Messages, if *msgType* = "Update" or "Cancel" this attribute must contain a reference to the original alert. Due to the CAP format requirements, this reference must consist of agencyIdentifier, alertIdentifier, and sendTime, separated by commas. If *msgType* = "Alert", then this attribute is not used.
info		**cap. alertInfo. info. group**	For PCA Cascade Messages, REQUIRED	The container for all component parts of the info sub-element of the alert message	CAP allows for multiple occurrences within a single <alert>. However, at least currently, PCA Cascade Messages will contain a single <info> block.
category	category	**cap. alertInfo. category. code**	REQUIRED	The code denoting the category of the subject event of the alert message	PCA does not require or regard this element but must populate it when using the CAP. PHIN alerts will always set this attribute to "Health".

Element	PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
event	alertProgram	**cap. alertInfo. event. text**	REQUIRED	The text denoting the type of the subject event of the alert message	PCA uses this to indicate the alerting program (*alertProgram*), which may take the values: HAN, Epi-X. Other alerting programs may come into being in the future.
urgency	urgency	**cap. alertInfo. urgency. code**	REQUIRED	The code denoting the urgency of the subject event of the alert message	Code Values supported by CAP are: "Immediate" - Responsive action SHOULD be taken immediately "Expected" - Responsive action SHOULD be taken soon (within next hour) "Future" - Responsive action SHOULD be taken in the near future "Past" - Responsive action is no longer required "Unknown" - Urgency not known. PCA does not require this element but systems must populate it when using the CAP. PCA alerting systems should disregard this element when receiving a cascade alert message. In the event the message is being distributed to non-PCA systems (i.e. outside of public health), PCA alerting systems should set this to an appropriate value.
severity	severity	**cap. alertInfo. severity. code**	REQUIRED	The code denoting the certainty of the subject event of the alert message	Code Values: "Extreme" - Extraordinary threat to life or property "Severe" - Significant threat to life or property "Moderate" - Possible threat to life or property "Minor" - Minimal threat to life or property "Unknown" - Severity unknown

Element	PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
certainty	**certainty**	**cap. alertInfo. certainty. code**	REQUIRED	The code denoting the certainty of the subject event of the alert message	PCA does not require or regard this element but must populate it when using the CAP. Since most health alerts describe events known to be happening, PCA alerting systems should most probably use the value "Very Likely", which means "Highly likely (p > ~ 85%) or certain".
senderName	**agencyName**	**cap. alertInfo. sender. name**	For PCA Cascade Messages, REQUIRED	The text naming the originator of the alert message	Required for PCA. Must contain the full official name of the agency originating the alert.
headline	title	**cap. alertInfo. headline. text**	For PCA Cascade Messages, REQUIRED	The text headline of the alert message	The "subject:" or "title" of the alert.
description	message	**cap. alertInfo. description. text**	For PCA Cascade Messages, REQUIRED	The text describing the subject event of the alert message	The main alert text.
contact	agencyEmergencyContact	**cap. alertInfo. contact. text**	OPTIONAL	The text describing the contact for follow-up and confirmation of the alert message	Emergency contact information for the person or office at the agency originating the alert that is responsible for providing follow-up and further information. Phone number and/or email address. May optionally include name or title of person.
parameter		**cap. alertInfo. parameter. group**	For PCA Cascade Messages, REQUIRED	A system-specific additional parameter associated with the alert message	Required for PCA Cascade Alerting. PHIN Alerting uses this element to hold the following PHIN-specific attributes: *acknowledge* *deliveryTime* *jurisdictionLevel* *programType*

Element			PCA Attribute	Context. Class. Attribute Representation	Optionality	Definition	Notes, Value Domain, and PCA usage
		acknowledge	acknowledge		For PCA Cascade Messages, REQUIRED	A PCA-specific additional attribute indicating whether alert recipients are required to manually acknowledge receipt.	Enumeration values: "Yes", "No"
		deliveryTime	deliveryTime		For PCA Cascade Messages, REQUIRED	A PCA-specific additional attribute indicating, in minutes, how quickly the alert must be delivered to recipients (and acknowledged, when acknowledgement is required).	Enumeration values: 15, 60, 1440, 4320 These values in minutes translate to 15 minutes, 60 minutes, 24 hours, and 72 hours.
		jurisdictionLevel	jurisdictionLevel		For PCA Cascade Messages, CONDITIONAL	A PCA-specific additional attribute indicating the "jurisdictional level" to which the alert is to be distributed	Enumeration values: National, State, Territorial, Local
		programType	programType		For PCA Cascade Messages, CONDITIONAL	A PCA-specific additional attribute indicating the message type, as defined by the alerting program.	The values for the programType is unique for each program.

6.1.3   Sample PCA Cascade Alert Message

Following is a sample PCA Cascade Alert Message. This example is annotated to show the corresponding PCA Attribute for each element of the message. This example shows a test update to a HAN message from the CDC.

PCA Attribute	PCA Cascade Message Example
	`<?xml version="1.0" encoding="UTF-8" ?>`
	`<EDXLDistribution xmlns="`**`urn:oasis:names:tc:emergency:EDXL:DE:1.0`**`">`
distributionIdentifier	`<distributionID>`**`20060004115`**`</distributionID>`
agencyIdentifier	`<senderID>`**`2.16.840.1.114222.4.1.450@cdc.gov`**`</senderID>`
sendTime	`<dateTimeSent>`**`2006-11-07T21:25:16.5127+00:00`**`</dateTimeSent>`
status	`<distributionStatus>`**`Test`**`</distributionStatus>`
distributionType	`<distributionType>`**`Report`**`</distributionType>`
sensitive	`<combinedConfidentiality>`**`Sensitive`**`</combinedConfidentiality>`
role	`<recipientRole>`
	`<valueListUrn>`**`urn:phin:role`**`</valueListUrn>`
	`<value>`**`Health Officer`**` </value>`
	`<value>`**`Emergency Preparedness Coordinator`**`</value>`
	`<value>`**`Chief Epidemiologist`**`</value>`
	`<value>`**`Communicable/Infectious Disease Coordinators`**`</value>`
	`<value>`**`HAN Coordinator`**` </value>`
	`</recipientRole>`
recipients	`<explicitAddress>`
	`<explicitAddressScheme>`**`e-mail`**`</explicitAddressScheme>`

	<explicitAddressValue>**johnsmith@healthdept.gov**</explicitAddressValue>
	<explicitAddressValue>**maryjones@healthdept.gov**</explicitAddressValue>
	</explicitAddress>
jurisdiction	<targetArea>
(optional ->)	<country>**US**</country>
	<locCodeUN>**01091**</locCodeUN>
	<locCodeUN>**01003**</locCodeUN>
	</targetArea>
jurisdiction	<targetArea>
	<locCodeUN>**28059**</locCodeUN>
	<locCodeUN>**28047**</locCodeUN>
	<locCodeUN>**28045**</locCodeUN>
	</targetArea>
jurisdiction	<targetArea>
	<locCodeUN>**22071**</locCodeUN>
	<locCodeUN>**22087**</locCodeUN>
	<locCodeUN>**22075**</locCodeUN>
	<locCodeUN>**22051**</locCodeUN>
	</targetArea>
	<contentObject>
sensitive	<confidentiality>**Sensitive**</confidentiality>
	<xmlContent>
	<embeddedXMLContent>
	<ns1:alert xmlns:ns1="**urn:oasis:names:tc:emergency:cap:1.1**">
alertIdentifier	<ns1:identifier>**CDC-2006-183**</ns1:identifier>
agencyIdentifier	<ns1:sender>**2.16.840.1.114222.4.1.450**</ns1:sender>

sendTime	<ns1:sent>**2006-11-07T21:25:16.5127+00:00**</ns1:sent>
status	<ns1:status>**Test**</ns1:status>
msgType	<ns1:msgType>**Update**</ns1:msgType>
reference	<ns1:references>**2.16.840.1.114222.4.1.450,CDC-2006-182,2006-11-05T13:02:42.1219+00:00**</references>
scope	<ns1:scope>**Restricted**</ns1:scope>
	<ns1:info>
category	<ns1:category>**Health**</ns1:category>
alertProgram	<ns1:event>**HAN**</ns1:event>
urgency	<ns1:urgency>**Expected**</ns1:urgency>
severity	<ns1:severity>**Severe**</ns1:severity>
certainty	<ns1:certainty>**Very Likely**</ns1:certainty>
senderName	<ns1:senderName>**Centers for Disease Control and Prevention**</ns1:senderName>
title	<ns1:headline>**Cases of Vibrio vulnificus identified among Hurricane Katrina evacuees**</ns1:headline>
message	<ns1:description>**To date, seven people in the area effected by Hurricane Katrina have been reported ill from the bacterial disease Vibrio vulnificus.**</ns1:description>
dissemination	<ns1:instruction>**Please distribute to health providers and officials within your jurisdiction as deemed appropriate**</ns1:instruction>
	<ns1:parameter>
acknowledge	<ns1:valueName>**Acknowledge**</ns1:valueName>
	<ns1:value>**Yes**</ns1:value>
	</ns1:parameter>
	<ns1:parameter>
deliveryTime	<ns1:valueName>**DeliveryTime**</ns1:valueName>
	<ns1:value>**1440**</ns1:value>

```
                                    </ns1:parameter>
                                    <ns1:parameter>
jurisdictionLevel                       <ns1:valueName>jurisdictionLevel</ns1:valueName>
                                        <ns1:value>State</ns1:value>
                                    </ns1:parameter>
                                    <ns1:parameter>
programType                             <ns1:valueName>ProgramType</ns1:valueName>
                                        <ns1:value>Notification</ns1:value>
                                    </ns1:parameter>
                                </ns1:info>
                            </ns1:alert>
                        </embeddedXMLContent>
                    </xmlContent>
                </contentObject>
            </EDXLDistribution>
```

6.2   PCA CASCADE ALERT ACKNOWLEDGEMENT

The PCA Cascade Acknowledgement is formatted using the Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element . The message format is defined in the table below.

6.2.1   Table 6.2.1: PCA CASCADE ACKNOWLEDGEMENT Using Emergency Data Exchange Language (EDXL) V 1.0 Distribution Element

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
EDXLDistribution		**XML Structure**	**REQUIRED. Once.**	**The container of all of the elements related to the distribution of the content messages.**	**The <EDXLDistribution> element may include one or more <targetArea> and <contentObject> blocks.**
distributionID	distributionIdentifier	**xsd:string**	**REQUIRED. Once.**	**The unique identifier of this distribution message.**	**MUST be a properly formed - escaped if necessary- XML string. -**

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
senderID	agencyIdentifier	xsd:string	REQUIRED. Once.	The unique identifier of the sender.	For Cascade Ack Messages, use the *agencyIdentifier* of the organization that is acknowledging the alert. 1. The identifier MUST be a properly formed -escaped if necessary- XML string. 2. The EDXL specification requires that senderID be unique and be in the form: actor@domain-name. The PCA specification uses Object Identifier (OID) as a unique identifier for the agency originating the alert. In order to meet the EDXL requirement, PCA Cascade Messages will adopt the form: agencyIdentifier@domain-name, where agencyIdentifier is the agency OID and domain-name is the agency's domain name. A valid domain name belonging to the agency should be used, however for PCA Cascade Messages it is only present to meet EDXL formatting requirements and is of no consequence to systems receiving the Cascade Alert.

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
dateTimeSent		xsd:dateTime	REQUIRED. Once.	The date and time the distribution message was sent.	For Cascade Ack Messages, use the date & time of the acknowledgement message (not of the message being acknowledged). The date and time is represented in W3C format for the XML *dateTime* data type (e. g., "2008-08-21T20:30:08.073+00.00" corresponds to August 21, 2008 at 3:30:08 (and 73/1000 seconds) PM EST. Refer to *sendTime* attribute listing in Table 4.2: PCA Alert Attributes.
distributionStatus	status	xsd:string with restrictions	REQUIRED. Once	Indication of whether this is an actual alert, an exercise, or a test	Values: Actual, Exercise, Test. For Cascade Ack Messages use the same value used in the alert being acknowledged. MUST be a properly formed - escaped if necessary- XML string.
distributionType		xsd:string with restrictions	REQUIRED. Once.	The function of the message.	For Cascade Ack Messages, the value must be ""Ack". The type MUST be a properly formed -escaped if necessary- XML string.
combindedConfidentiality	sensitive	xsd:string	REQUIRED. Once.	Confidentiality of the combined distribution message's content	Enumeration values: "Sensitive", "NotSensitive". For Cascade Ack Messages use the same value used in the alert being acknowledged.

Element	PCA Alert Attribute	Type	Optionality/ Multiplicity	Definition	Comments
distributionReference	reference	xsd:string	CONDITIONAL. Multiple.	This attribute must contain a reference to the original alert being acknowledged.	The \<distributionID> and \<senderID> and \<dateTimeSent> of the referenced previous message, concatenated with a comma delimiter. This element must appear in a Cascade Acknowledgement Message. MUST be a properly formed - escaped if necessary- XML string

6.2.2   Sample PCA Cascade Acknowledgement Message

Following is a sample PCA Cascade Acknowledgement Message. This example is annotated to show the corresponding PCA Attribute for each element of the message. This example shows an acknowledgement to the example test update HAN message from the CDC shown in 6.1.3.

PCA Attribute	PCA Cascade Acknowledgement Example
	\<?xml version="1.0" encoding="UTF-8" ?>
	\<EDXLDistribution xmlns="**urn:oasis:names:tc:emergency:EDXL:DE:1.0**">
distributionIdentifier	\<distributionID>**1028457**\</distributionID>
agencyIdentifier	\<senderID>**2.16.840.1.114222.4.1.3456@state.healthdept.gov**\</senderID>
sendTime	\<dateTimeSent>**2006-11-07T21:29:42.8133+00:00**\</dateTimeSent>
status	\<distributionStatus>**Test**\</distributionStatus>
msgType	\<distributionType>**Ack**\</distributionType>
sensitive	\<combinedConfidentiality>**Sensitive**\</combinedConfidentiality>
reference	\<distributionReference>**20060004115,2.16.840.1.114222.4.1.450@cdc.gov,2006-11-07T21:25:16.5127+00.00**\</distributionReference>

```
</EDXLDistribution>
```

7 FOR FURTHER INFORMATION AND SUPPORT

For more information about this document, or for additional information and guidance about implementation of PHIN Partner Communication and Alerting, please contact:

PHIN Help Desk
National Center for Public Health Informatics
Phone: 1-800-532-9929 or 770-216-1299
Email: PHINTech@cdc.gov

APPENDIX 1 – DEFINITION OF TERMS

Definition of terms

The following terms are defined for purposes of this document and for purposes of discussion about PHIN, PHIN Communication and Alerting, and PHIN Directory Exchange.

Alert

An alert is a time-sensitive, one-way communication sent by a *PHIN partner organization* for legitimate business purposes, to a collection of people and *organizations* with whom the *partner* has a business relationship, in order to notify them of an event or situation of some importance. The term is meant to include communications that urgent as well as those that are more routine in nature.

Alert recipient

A person who receives or is intended to receive an *alert*.

Alerting

The processes, activities, and functionality necessary to manage time-critical information about events, send it in real time to personnel and *organizations* that must respond to and mitigate the impact of these events, and verify and monitor delivery of this information.

Alerting program

A public health program that employs *alerting* and that conforms to the *PCA* specification.

Alerting system – see *Public health alerting system.*

Cascade Alerting

The sending of *alerts* to *recipients* in another *jurisdiction* by means of a system-to-system message. The originating *alerting system* sends a message containing the *alert* text along with parameters describing the *alert* to the receiving *alerting system*, which then distributes the *alert* the appropriately within its corresponding *jurisdiction*.

Communication device

An instance of equipment or technological capability by means of which a *recipient* can receive *alerts*. Examples include: a telephone, email address, fax machine, PDA, pager, web site. Note that a single piece of physical equipment can count as two communication devices: i.e. a cell phone can function as a cell phone and as (a means of accessing) an email address. The primary unique characteristic of a communication device is its address: the phone number, email address, or URL through which it is reached. Thus an

email address is a single device although it can be accessed using any number of computers.

Cross-jurisdictional alerting

The sending of *alerts* from one *jurisdiction* to another.

Device

See *Communication device*.

Device type

A classification of *communication devices* according to their capabilities. Examples include land-line phones, cell phones, email addresses, fax machines, PDAs, pagers, SMS (text message) devices, and web sites. Note that a single piece of physical equipment can have more than one device type: e.g. a cell phone can also be an SMS device and (a means of accessing) an email address.

Direct Alerting

The sending of *alerts* from an *alerting system* to a *recipient*, in which the system delivers the *alert* to one or more of the *recipient*'s *communication devices*. This is the usual mode of alerting.

Health alert

A type of *alert* that is specifically about a public health event or situation. A Health Alert is a time-sensitive communication, issued by a local health department, state health department, federal health agency, or other organizational entity having a role in public health, that provides notice of a public health threat or an occurrence of an emerging significant public health event. It prompts recipients to come to a state of preparedness or to take action to mitigate a negative health impact.

Health Alert Network

The Health Alert Network (HAN) is a network of systems operated by local and state health departments in U.S. states and territories, and the CDC, to create, send, and manage *health alerts*. This network is unified by virtue of inter-agency coordination regarding processes and protocols, terminology and semantics, and technological capability, which are necessary due to the often cross-jurisdictional nature of health threats and the public health response to them.

Jurisdiction

A domain over which a *public health organization* exercises authority to manage and administer public health. This domain may variously be a geographic/political entity, such as a state, city, or county, an organizational domain, such as the U.S. military, or a cultural domain, such as a Native American tribe.

Long text – a manner of rendering *alert* content that is intended to be read, when there is no appreciable constraint on text size; e.g. rendering for email and web presentation;

Organization

A government agency or private business establishment.

Partner

See *PHIN partner organization*.

PHIN Communication and Alerting (PCA)

PHIN Communication and Alerting (PCA), one component of *PHIN*, is a specification of public health *alerting* capabilities, with an emphasis on interoperability of *partners*' systems. Systems that provide PCA functionality support these capabilities, integrate them with the *organization*'s other public health information systems and processes, and support interoperability with *partners*' systems.

PHIN partner

See *PHIN partner organization*.

PHIN partner organization

A *public health organization* that is endeavoring to participate in the *Public Helath Information Network* by meeting *PHIN* standards and requirements and implementing *PHIN*-compliant systems.

Program

A public health activity that has responsibility for addressing or managing a particular health, administrative, or communication problem, and that requires coordinated action at the federal and state, and optionally local, level. For purposes of this document and discussion of PCA, a program is of interest if it is an *alerting program*, that is, a discreet activity that is autonomously managed and makes use of public health alerting capabilities. Examples could include: Health Alert Network (HAN), quarantine management, environmental health emergency management, etc.

Public health alerting system

A system, or a set of systems and processes, used by a *PHIN partner organization* to compose and manage *alerts* and deliver them to designated *recipients* in a manner consistent with the *PCA* requirements.

Public Health Information Network (PHIN)

The CDC Public Health Information Network (PHIN) is a national initiative to improve the capacity of public health to use and exchange information electronically by promoting the use of standards, defining functional and technical requirements.

Public health organization

An *organization* that has legitimate authority within some *jurisdiction* to manage and administer public health.

Recipient

See *Alert recipient*.

Short text

A manner of rendering *alert* content that is intended to be read, when there is a significant constraint on text size; e.g. rendering for SMS (text messaging) *devices* and pagers;

Voice

See *Voice text*.

Voice text

A manner of rendering *alert* content that will be delivered verbally; e.g. rendering for automated voice (text-to-speech) delivery by telephone.

APPENDIX 2 – AUDIENCE SPECIFICATION EXAMPLES

Following is a set of all possible permutations of the audience specification lists, populated with example values and accompanied by an interpretation.

These are expressed here as simple attribute value pairs for readability.

EXAMPLE 1

recipients = {johnsmith@healthdept.gov, maryjones@healthdept.gov}

Interpretation: The individuals John Smith and Mary Jones.

EXAMPLE 2

role = {Health Officer, Public Health Administrator, Chief Epidemiologist}
jurisdictionLevel = {State, Local}
jurisdiction = {01, 12, 13191, 13127, 13039, 13049}

Interpretation: The Health Officers, Public Health Administrators, and Chief Epidemiologists working at the state and local health department level in Alabama, Florida, and four Georgia counties (McIntosh, Glynn, Camden and Charlton county).

EXAMPLE 3

role = {Chief Epidemiologist}
jurisdiction = {01, 12, 13}

Interpretation: The Chief Epidemiologists responsible for the states of Alabama, Florida, and Georgia. Since no *jurisdictionLevel* parameter is specified, the Chief Epidemiologists at all levels – local, territorial, state, and federal – are targeted.

EXAMPLE 4

jurisdiction = {01, 12, 13}
jurisdictionLevel = {State, Local}

Interpretation: All possible alert recipients who are located in, have an association with, or have responsibility within state and local level jurisdictions in Alabama, Florida, and Georgia.

EXAMPLE 5

role = {Chief Epidemiologist Health Officer}

jurisdictionLevel = {State, Local}

Interpretation: All local and state level Chief Epidemiologists and Health Officers, in all state and local jurisdictions.

EXAMPLE 6

jurisdiction = {01, 12, 13}

Interpretation: All possible alert recipients who are located in, have an association with, or have responsibility within state Alabama, Florida, and Georgia. Note that this would include federal level role players since no jurisdictional level was specified.

EXAMPLE 7

jurisdictionLevel = {State, Local}

Interpretation: All possible alert recipients who are located in, have an association with, or have responsibility within any state or local level jurisdiction.

EXAMPLE 8

role = {Chief Epidemiologist}

Interpretation: All chief epidemiologists, in every jurisdiction, and working at any jurisdictional level (local, territorial, state, federal).

EXAMPLE 9

recipients = {johnsmith@healthdept.gov, maryjones@healthdept.gov}

role = {Chief Epidemiologist}

jurisdictionLevel = {State, Local}

jurisdiction = {01, 12, 13}

Interpretation:: All Chief Epidemiologists working at the state and local health department level in Alabama, Florida, and Georgia, and John Smith and Mary Jones.

APPENDIX 3 –ORIGINATING AGENCY ABBREVIATIONS

For national PHIN partners (which currently consists of only the CDC), the originating agency abbreviation is the commonly used agency acronym.

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

For county public health partners, the originating agency abbreviation 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"

For city public health partners, the originating agency abbreviation 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"

Examples:

National partners

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

State partners

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

County partners

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

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

APPENDIX 4   PUBLIC HEALTH ROLES

The following table contains public health *roles* defined by some current public health alerting programs. This table is included in this document for informational purposes only, and to document the correspondence of role definitions across alerting programs. The information in this table is subject to change. The PCA specification itself does *not* require any particular value set for the *role* attribute, nor does it require that PHIN partners fill particular roles. Individual alerting programs, however, may require the use of particular values for the *role* attribute, and may require that PHIN partners fill particular roles. An "X" in an alerting programs' "Usage" column indicates that the program issues alerts to the role.

Table AP4 - Public Health Roles for Alerting

	Role	Also known as	Definition	Alerting Program Usage		
				HAN	Epi-X	Quarantine
1	Health Officer	Commonly referred to as the State or Territorial Public Health Officer.	Responsible for the direction and administration of the jurisdiction's Department of Health.	X	X	X
2	Emergency Preparedness Coordinator	Formerly known as the Terrorism Coordinator or BT Coordinator. Commonly referred to as the State Public Health Emergency Preparedness Coordinator/BT Coordinator.	Responsible for the administration of all Terrorism related activities within the jurisdiction.	X	X	X
3	HAN Coordinator	Formerly known as the Health Alert and Communications Coordinator	Responsible for the coordination, implementation, and maintenance of the public health alert and information network for the agency or jurisdiction.	X	X	X

	Role	Also known as	Definition	Alerting Program Usage		
				HAN	**Epi-X**	**Quarantine**
4	Laboratory Director	Commonly referred to as the State or Territorial Public Health Laboratory Director.	Responsible for the coordination of the laboratory testing and reporting for the agency or jurisdiction.	X	X	X
5	Public Health Administrator	Commonly referred to as the State Public Health Administrator.	Responsible for the management of the jurisdiction's Department of Public Health.			X
6	Emergency Management Coordinator	Commonly referred to as the State Emergency Management Coordinator.	Responsible for coordinating, facilitating and assisting in the planning, organization, control and implementation of emergency management and emergency operations center activities.			X
7	Chief Epidemiologist	Commonly referred to as the State or Territorial Epidemiologist.	Responsible for the coordination of the public health surveillance, investigation and response activities within the jurisdiction.	X	X	X
8	Public Information Officer	Commonly referred to as the State Public Health Information Officer.	Responsible for the coordination of public information and emergency risk communications for the jurisdiction.	X	X	X
9	Communicable/Infectious Disease Coordinator		Responsible for the coordination of all communicable and infectious disease surveillance and investigations and response within the jurisdiction.		X	X
10	Strategic National Stockpile Coordinator		Responsible for the coordination of the pharmaceutical stockpile planning for the agency or jurisdiction.			X
11	Environmental Health Director		Responsible for the coordination and direction of the jurisdiction's Environmental Health department.	X		X

	Role	Also known as	Definition	Alerting Program Usage		
				HAN	Epi-X	Quarantine
12	Chief Veterinarian	Commonly referred to as the State Veterinarian.	Responsible for animal health concerns of the state (not zoonotic diseases). Liaison with federal agencies regarding impending or existing disasters among the animal population.		X	
13	Chief Public Health Veterinarian	Commonly referred to as the State or Territorial Public Health Veterinarian.	Responsible for the coordination of preventing exposures to and controlling diseases that humans can get from animals and animal products.. Deals with zoonotic diseases.	X		X
14	Chief Veterinary Laboratory Director	Commonly referred to as the State Veterinary Laboratory Director.	Director of the State Animal Diagnostic Laboratory.		X	
15	Emergency Medical Services Coordinator	Previously referred to as the Emergency Medical Services Authority.	Coordinates all medical response activities. Coordinates with other agencies and jurisdictions and responds to medical emergencies.			X
16	Public Health Logistics Coordinator		Responsible for transportation, facility setup, personnel protective equipment, supplies and other logistical requirements in an emergency response situation.			X
17	Quarantine Officer		Individual responsible for quarantine enactment and coordination at the local level to include international and travel issues for a region. This role is sometimes performed by the Chief Epidemiologist.			X

	Role	Also known as	Definition	Alerting Program Usage		
				HAN	Epi-X	Quarantine
18	LRN Laboratory Director	Formerly referred to as the Laboratory BT, and is sometimes referred to as the LRN Coordinator.	Responsible for the administration of Bioterrorism laboratory testing within the jurisdiction.			
19	Medical Director		Responsible for medical/health services in the jurisdiction			X
20	Poison Control Center Director	Commonly referred to as the Poison Control Director.	Office responsible for handling poison injury calls in a region		X	X
21	Border Health Director		Responsible for cross-border health issues, coordination and communication.			X
22	Epidemiologist		Individual who performs analysis of communicable disease and/or BT information for their jurisdiction.			X
23	Emergency Operations Center Director	Formerly known as the Emergency Operations Center Coordinator.	Responsible for managing the EOC and for brining together the Individuals who participate as a members of the Emergency Operations Center.			X
24	Public Health Officer On-Call	Also known as: Public Health Officer of the Day, Emergency Operations Center	The public health officer currently on-call and responsible for fielding and managing time-critical events.	X		
25	Infection Control Practitioner		Responsible for nosocomial and infectious disease in a hospital.			X
26	FBI WMD/BT Agent		Responsible for FBI activities and response in a WMD/BT event.			X
27	Public Health Investigator/Contact Tracer	Sometimes referred to as DGMQ Traveler Notification Contact.	Individual charged with tracing contacts of infected or possibly infected travelers.		X	

	Role	Also known as	Definition	Alerting Program Usage		
				HAN	Epi-X	Quarantine
28	Refugee Coordinator					X
29	Immigrant TB Coordinator					X
30	HIV Coordinator					X
31	Yellow Fever Coordinator					X