Public Health Information Network

Partner Communications and Alerting

Functional Requirements

PUBLIC HEALTH INFORMATION NETWORK

May 11, 2005

SAFER • HEALTHIER • PEOPLE

Agenda

The Vision Thing

Definitions

Current State of PCA and Directory

Review of Functional Requirements

- Alerting and secure partner communications
- Alert format
- Vocabulary standards
- Recipient addressing
- Alerting across jurisdictions
- Cascade Alerting
  - PHIN Specification of CAP protocol
- Integration of PCA and Directory

Partner Communications and Alerting
The vision thing

Every public health jurisdiction can send to health partners information critical for response to public health events and emergencies

- Rapidly
- Reliably
- Securely
- 24X7

Partner Communications and Alerting
The vision thing

- "Blast" alerts – large, general distribution
- "Call-down" alerts – targeted to key personnel based on their role or expertise
- Alerts to *affiliates* – hospitals, ERs, labs, clinicians, emergency management, first responders…
- Alerts to other jurisdictions

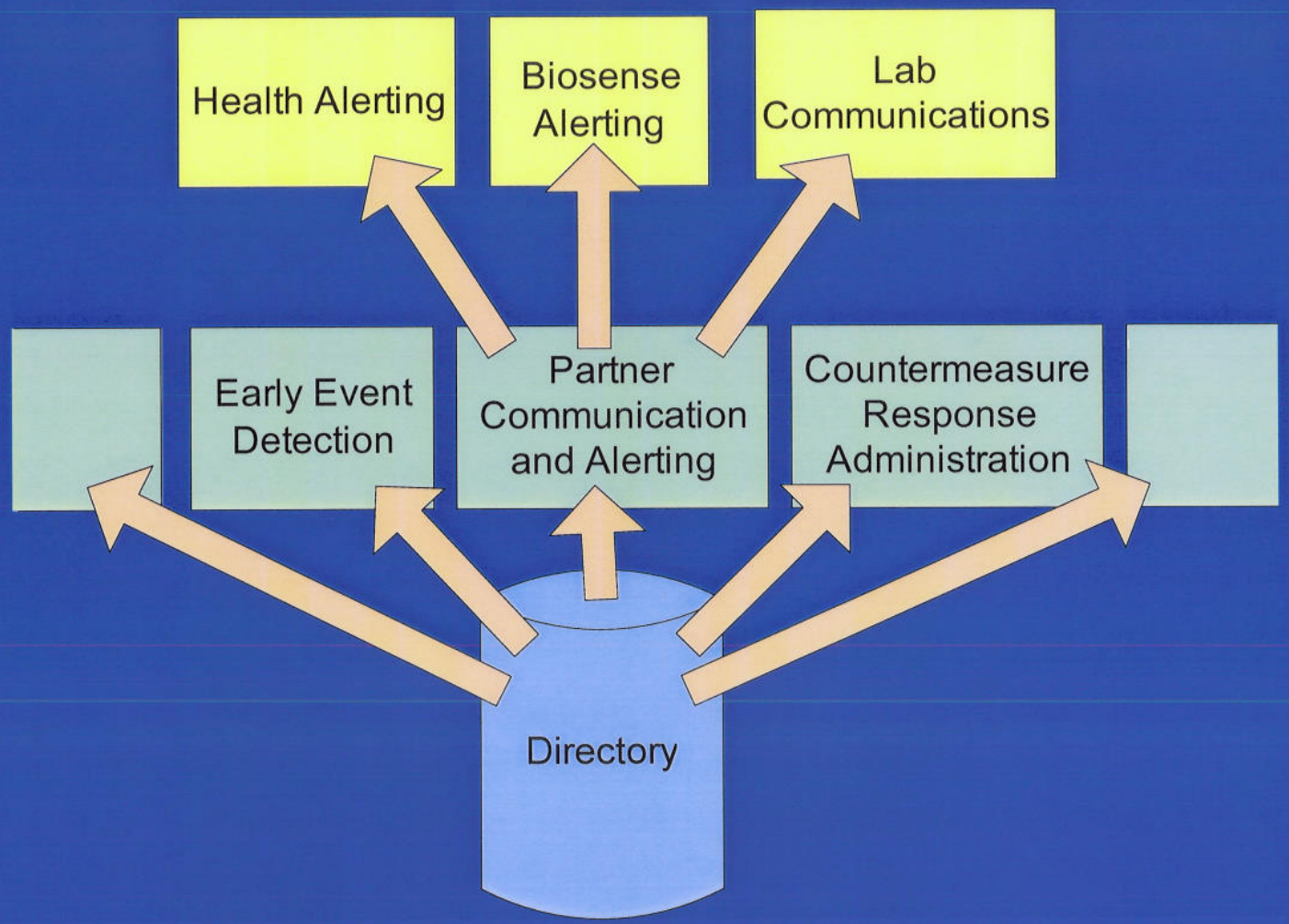
Definitions

for purposes of this presentation

- Alert
- Alerting System
- Jurisdiction
- Partner
- Affiliate
- PHIN Partner Communication and Alerting ("PCA")

PCA ≠ HAN

Directory supports PCA
PCA supports HAN



Current State of PHIN Alerting and Directory

• PCA Functional Requirements	complete
• Directory Functional Requirement	complete
• PCA Implementation Guide	June 05
• Directory Implementation Guide	June 05

CDC services to support partners

• Alerting solution for partners	August 05
– CAP capable	December 05
• Call center for partners	August 05
• CDC directory lookup	
• CDC directory data feed	
• Physician directory feed (State Medical Boards)	
• Laboratory directory data feed	

Current State of PHIN Alerting and Directory

Tasks ahead

- Business protocols
- Migration to PHIN PCA compliance

Alerting and Secure Partner Communications

Review of Functional Requirements

Alerting and Secure Partner Communications

Alerting systems must send, receive, manage, and disseminate alerts to *health partners*

- Within jurisdiction & sub-jurisdictions:
  - Health officials
  - Affiliates:

    Hospitals, ERs, docs, labs, 1st responders…

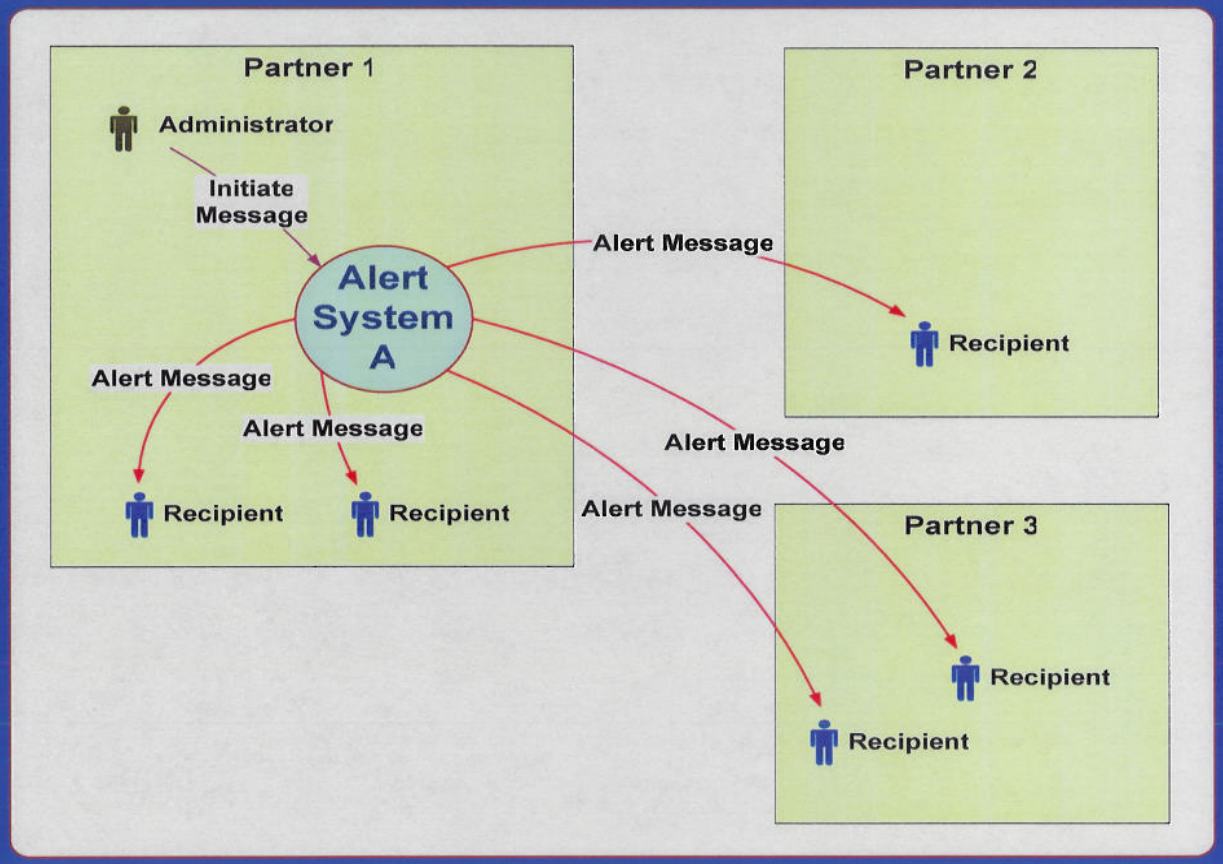
    …anyone involved in emergency response plan
- In other jurisdictions:
  - Health officials
  - *Request* delivery to affiliates

Alerting and Secure Partner Communications

- Partners must be able to send alerts to and receive alert from other jurisdictions & organizations
- Alerts across jurisdictions: direct or cascade
  - If receiving partner is certified as meeting KPMs for cascade alerts, the sending partner *must* use cascade alerting
  - If not, the sending partner will use direct alerting
  - Partners must be able to identify which other partners can receive cascade alerts

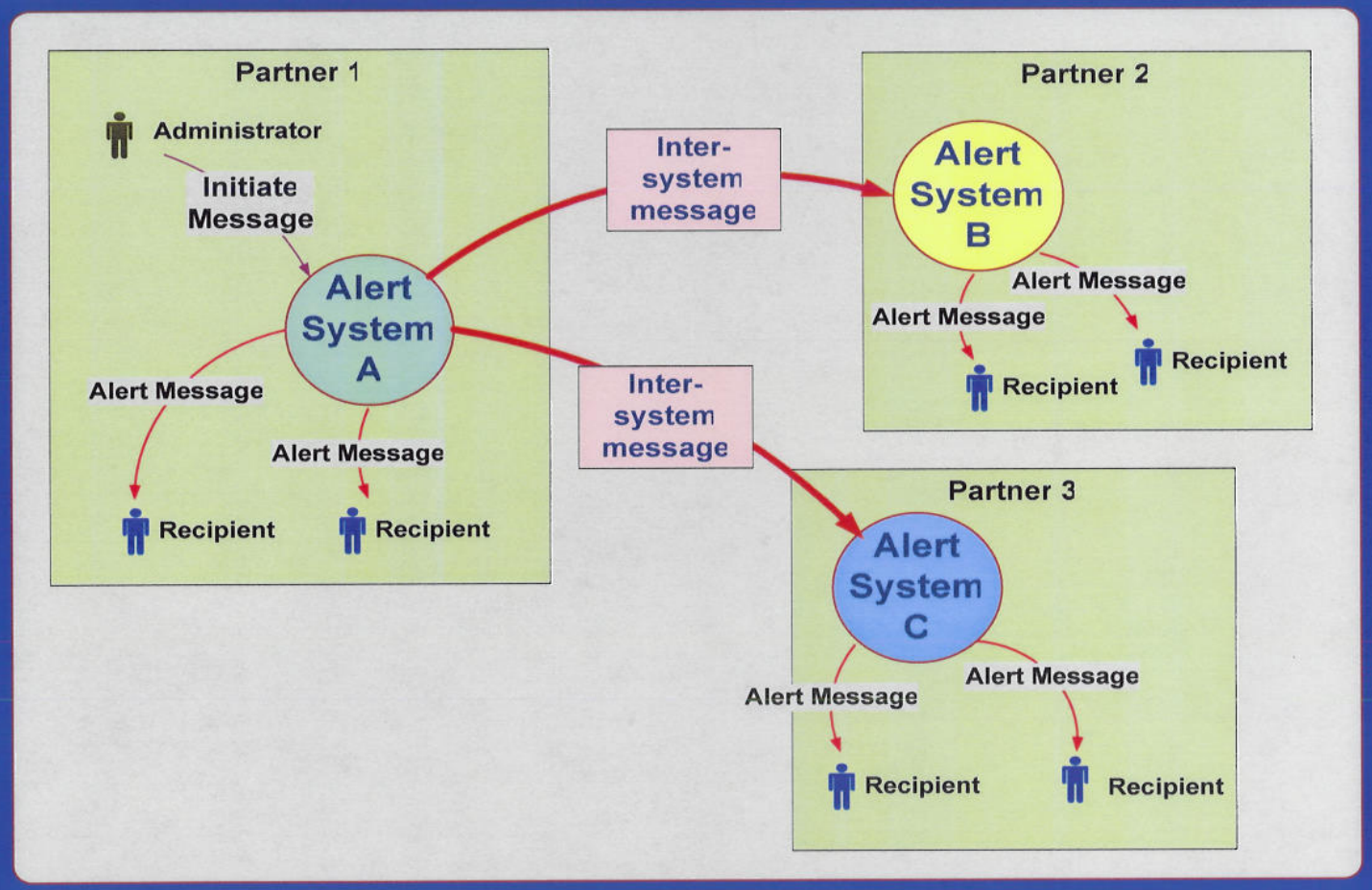
  Implication: every PHIN partner must become capable of sending cascade alerts

Direct Alerting
across jurisdictions



Cascade Alerting

across jurisdictions



Alerting and Secure Partner Communications

- A receiving partner may append jurisdiction-specific information to original alert
  - As long as message delivery time requirement is met
  - May not alter original content
    - …Except may delete/substitute contact information
  - May append new content to clarify jurisdictional action
  - Edits & alterations must be audit trailed

Alerting and Secure Partner Communications

- Alerting systems must support manual confirmation
  - Indicates human user receipt & acknowledgement
  - System must accept & record confirmation
- Alerting system must report status of delivery/confirmation
  - number of recipients targeted
  - number who have received/confirmed

Alerting and Secure Partner Communications

Alerting systems:

- Must be able to securely archive their alerts
- Must be able to securely retrieve, reconstruct, and resend archived alerts and communications

Alerting and Secure Partner Communications

Secure Communications

- A means of secure partner communication must be provided
  - Deliver of sensitive message content
  - Support collaboration – e.g. discussion boards
- Secure channel must provide:
  - Authentication
  - Restricted access and distribution
  - Secure transport

Secure websites that meet certification requirements may be used for secure information delivery

Alerting and Secure Partner Communications

Secure Communications

- Notification *about* sensitive alerts can be made over non-secure channel
  - Notification contains no sensitive content
  - Notification refers recipient to secure channel

    e.g. Notification via email → content on secure web site
- Alerting systems must recognize secure versus non-secure channels of transmission

Alerting and Secure Partner Communications

Secure Communications

- Secure web presentation should use secure technology encryption
  - e.g. Secure Sockets Layer (SSL)
- PHIN partners must have access to a secure web site
  - e.g. Epi-X (as one example)

Alert Format

Alert Format

Alerts may be sent to a wide range of people and roles.

A standardized format will help ensure that alerting works efficiently during an emergency.

- Alerts must address single issues
- Content must be presentable in simple text format for text-only devices

…Blackberrys, pagers, …

Alert Format

- All alerts must contain
  - Agency identifier (specific format)
  - Unique message identifier (program dependant)
  - Sensitivity indicator (specific vocabulary)
  - Severity indicator (specific vocabulary)
  - Acknowledgement required indicator
  - Succinct title

Device-specific data requirements in
PHIN Public Health Alert Implementation Guide

Alert Format

Standard format for *Agency Identifier:*

- Federal PHIN partners: use common agency acronym

  "CDC" "FBI"

- State health departments: use two character postal abbreviation for state

  "AL" "AK"

- County or city health departments: use concatenation of state abbreviation, dash (-), county or city name, dash (-), and the word "COUNTY" or "CITY"

  "AL-AUTAUGA-COUNTY"
  "MO-STLOUIS-CITY"

Vocabulary Standards

Vocabulary Standards

- Standardized attributes and value sets
  - Severity
  - Sensitivity
  - Delivery Time
  - Role
  - Sensitivity
  - Status
  - Message type
- Recommended that alerting systems use
- *Require* that systems use for data exchange

Vocabulary Standards

- Severity

Severity	Public Health Definition
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 or attention

Vocabulary Standards

- Sensitivity

Sensitive
Yes
No

Is it sensitive?
…If the information were used inappropriately:
- would it hamper the organization's ability to operate?
- would it damage the organization's reputation?

If yes:
- Must use secure method of delivery

Vocabulary Standards

- Delivery Time

  Interval of time between sending of alert and receipt (and acknowledgement if required)

Delivery Time
15 minutes
60 minutes
24 hours
72 hours

Vocabulary Standards

- Acknowledge

  Indicates whether human acknowledgement of receipt required

Acknowledge
Yes
No

  - If yes:
    - Exhaust all contact methods for each recipient
    - Try alternate contacts
    - Retry

    ….until acknowledgement received
  - Systems must register acknowledgement

Vocabulary Standards

- Role: public health function(s) of target recipients

Role	Definition
Health Officer	Responsible for the direction and administration of the jurisdiction's Department of Health.
Chief Epidemiologist	Responsible for the coordination of the public health surveillance, investigation and response activities within the jurisdiction.
Laboratory Director	Responsible for the coordination of the laboratory testing and reporting for the agency or jurisdiction.

...etc...

See Appendix A of *Partner Communications And Alerting Functional Requirements*

Vocabulary Standards

- Jurisdiction:

  of target recipients

FIPS codes

- Jurisdiction Level:

  of target recipients

Jurisdiction Level
National
State
Regional
Local

Vocabulary Standards

- Status: indicates whether alert is "real"

Status	
Actual	an actual event
Exercise	not actual event, but designated recipients must respond
Test	technical/system test message; disregard

- Message Type: identifies follow-ups to an alert

Message Type	
Alert	original message
Update	prior message(s) updated and superceded
Cancel	prior message(s) cancelled
Error	prior message(s) retracted

Recipient Addressing

Recipient Addressing

Alerting systems:

- May address alerts to
  - Specific people
  - A combination of attributes
    (e.g. role, jurisdiction, jurisdiction level)
  - Both
- Must be able to target alerts based on the nature of event
- Should be able to target one alert differently to different groups
- Should ensure delivery to all required recipients
- Should minimize redundant/unnecessary alerts

Recipient Addressing

Example

Recipient addressing based on attributes:

Attribute	Value
Role	Chief Epidemiologist Communicable/Infectious Disease Coordinator
Jurisdiction	13 (Georgia) 01 (Alabama) 12 (Florida)
Jurisdiction Level	State Local

Translation: Alert is addressed to Chief Epis and Infectious Disease Coordinators at state and local health departments in Georgia, Alabama and Florida

Cross-Jurisdictional Alerting

Cross-Jurisdictional Alerting

- When alerts are sent across state lines, the initiating jurisdiction may need to notify national health partners
  - If event is interstate in nature
- When alerts are sent to affiliates or sub-jurisdictions, the parent jurisdiction must be notified.
- Each state must develop a notification tree showing their parent/child hierarchy for alerting
  - Available to partners, preferably in public health section of state's web site.

Cross-Jurisdictional Alerting

Cascade Alerting

- If receiving partner is certified as meeting KPMs for cascade alerts, the sending partner *must* use cascade alerting
  - Partners must be able to identify which other partners can receive cascade alerts

Implication: every PHIN partner must become capable of sending cascade alerts

Cascade Alerting

Cascade alerts

- Must use the PHIN specification of Common Alerting Protocol (CAP)
- Must be transmitted using secure transport protocol
  - ebXML implementation compatible with PHIN Messaging Services (PHIN MS)

Cascade Alerting

Receiving system:

- Must be able to parse and act on alert parameters in the CAP message
- Must process parameters in accord with the PHIN Public Health Implementation Guide
- Must transmit acknowledgement of CAP message within 5 minutes

Cascade Alerting

Receiving system:

- Must return delivery status report to initiating system:
  - For Delivery Time = 15 minutes or 60 minutes:

    Report every 10 minutes
  - For Delivery Time = 24 hours or 72 hours:

    Report within one hour (during normal business hours
- Report includes message identifier, number of recipients targeted, and number reached
- Failure to report: sender reverts to direct alerting

Cascade Alerting

PHIN PCA Specification of CAP Protocol

Element Name	CAP Definition	PHIN Usage
identifier	Unique ID of alert message. Req'd.	"Program" specific protocol for unique identifier. E.g. (for HAN), "CDC-2005-37".
sender	Identifier of msg sender. Req'd.	PHIN PCA *Agency Identifier.* E.g. "CA-LOSANGELES-COUNTY".
source	Text identifying source of alert.	Readable text describing system originating this alert. E.g. "CDC Health Alerting System"
sent	Date & time of alert, ISO 8601 format. Req'd.	E.g. "2005-05-11T17:30:00-04:00" for May 11, 2005, 3:30 P.M.
status	Code denoting handling of alert. Req'd.	PHIN PCA *status* attribute (Actual, Exercise, Test).

Cascade Alerting

PHIN PCA Specification of CAP Protocol

Element Name	CAP Definition	PHIN Usage
scope	Intended distribution of msg. Req'd.	PHIN PCA *Sensitivity* attribute. "Restricted" = non-sensitive. "Private" = sensitive. "Public" is not used.
code	Special handling of msg. Req'd.	PHIN PCA *Acknowledge* attribute. 0=no special handling. 1=acknowledgement required.
msgType	Code denoting nature of msg. Req'd.	PHIN PCA *Message Type* attribute (Alert, Update, Cancel, Error).
references	ID of earlier referenced message.	Req'd when msgType is "Update", "Cancel" or "Error" to reference earlier message.
category	Code denoting category of event.	Presumably most PHIN alerts will fall into "Health" category.

Cascade Alerting

PHIN PCA Specification of CAP Protocol

Element Name	CAP Definition	PHIN Usage
severity	Code denoting severity of event.	PHIN PCA *Severity* attribute (Extreme, Severe, Moderate, Minor, Unknown). Req'd.
audience	Text describing intended audience.	PHIN PCA Role*Role* attribute. Contains list of public health roles.
sender Name	Text naming originator of msg.	Human readable name of organization sending alert.
headline	Text headline of message.	PHIN PCA "Title" field.
description	Text describing the event.	Main alert text.

Cascade Alerting

PHIN PCA Specification of CAP Protocol

Element Name	CAP Definition	PHIN Usage
web	Hyperlink for additional information.	URL of web page with more information about this alert.
contact	Text describing follow-up contact.	Name & contact info of person responsible for follow-up and more information. Req'd for urgent alerts.
areaDesc	Text describing affected area.	
geoCode	code delineating geographic area for distribution.	For PHIN PCA, list of 2 digit state and/or 5 digit state+county FIPS codes.
parameter	Additional code/value pairs.	Used for two PHIN PCA attributes: DELIVERYTIME (15M, 60M, 24H, 72H). LEVEL (National, State, Regional, Local).

Integration of PCA and Directory