PHIN: *Providing Public Health Disaster Management Capabilities w/ RHCPP Partnerships*

Agenda

- **Background**
- **PH Disaster Management Activities**
- **Requirements Pertinent to RHCPP**
- **Strategies and Future Vision**

John McLamb, MSIA, PHDM
NC PHIN Program Mgr
john.mclamb@ncmail.net

"All Disasters are Local"

"Effective systems used in a disaster are every-day systems"

Public Health Information Network
PHIN - Purpose

PHIN is a Framework to improve the capacity of public health to use & exchange information electronically by:

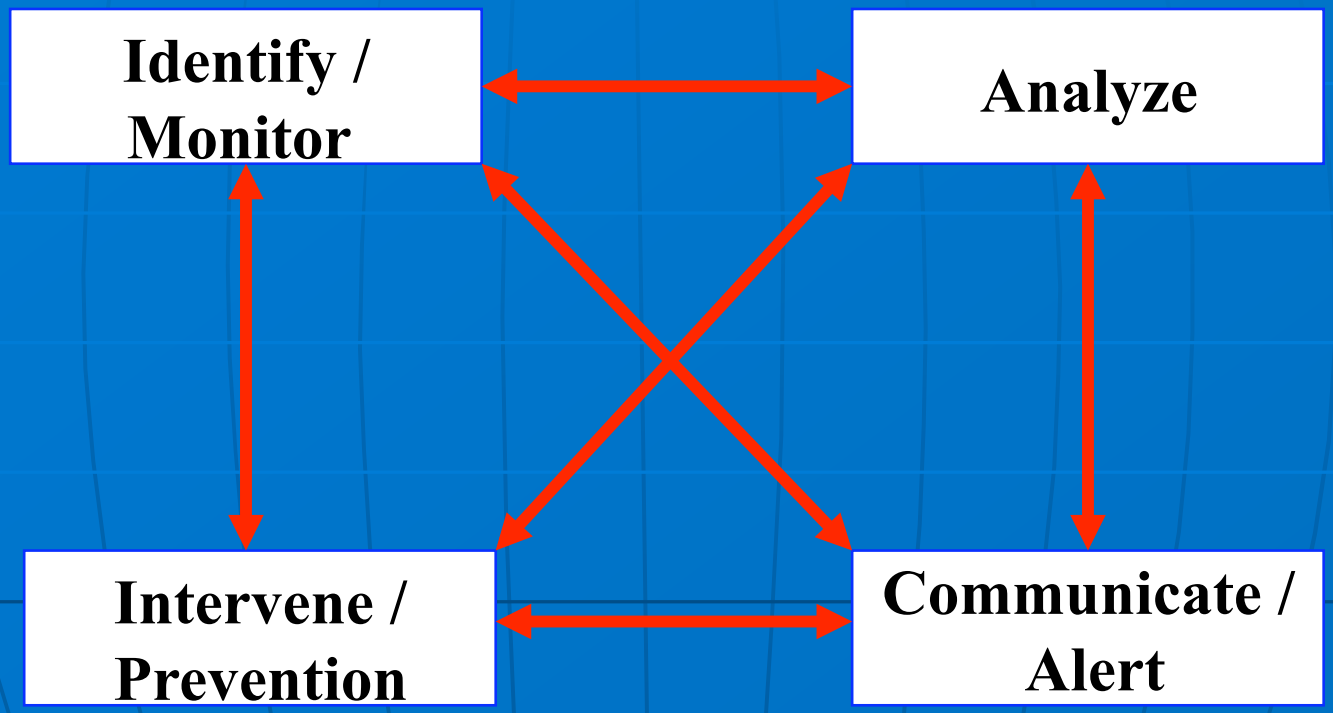
- Promoting the use of standards
- Providing technical specifications
- Defining basic public health priority functions
- Identifying workforce competencies
- Facilitating collaborative development of policies for data sharing
- Strengthening routine use and exchange to be robust and flexible enough to accommodate an emergency
- PHIN Partners: COTS, Home-Grown, CDC Developed Systems to support PHIN

Public Health Information Network

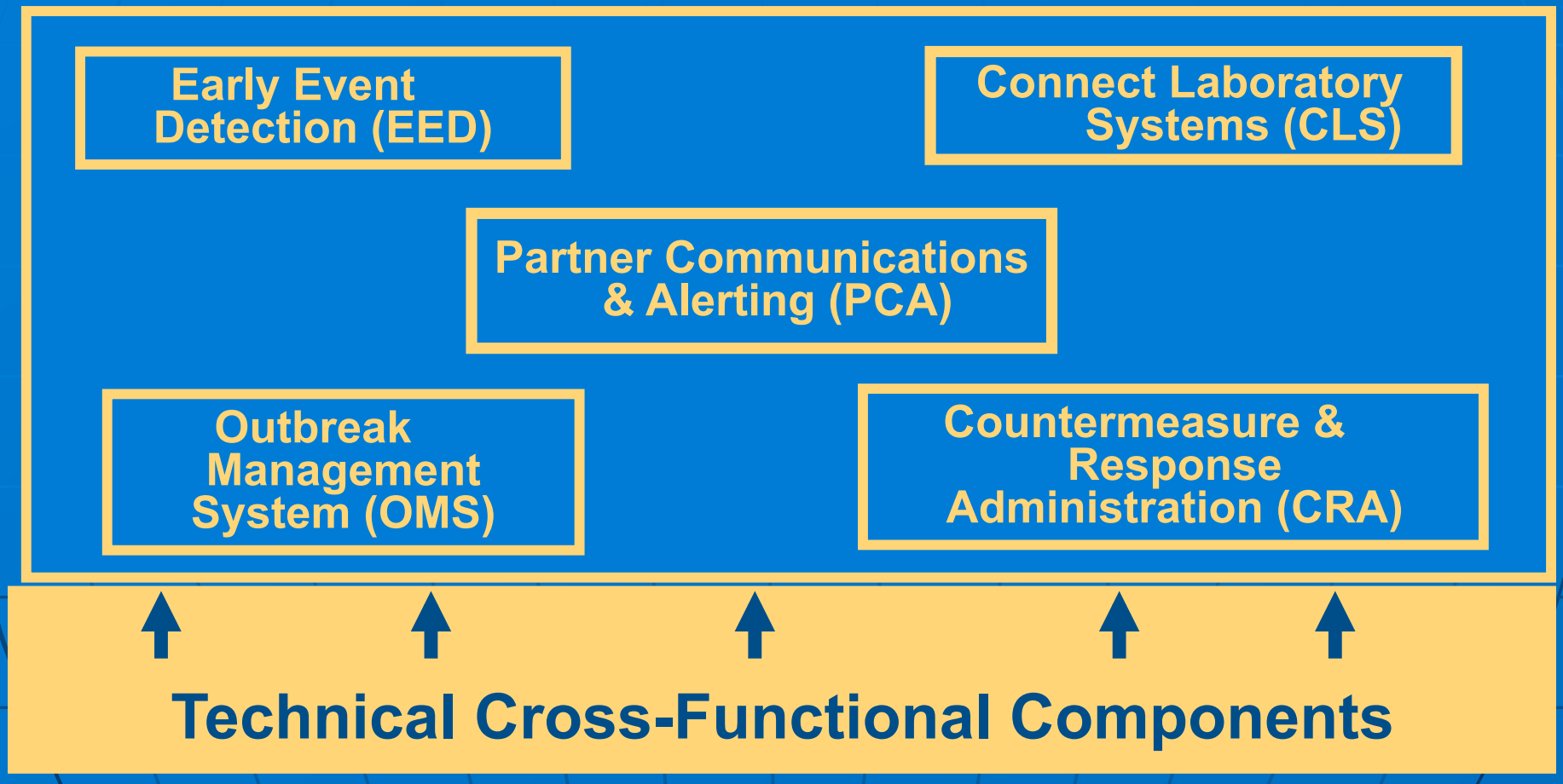
PHIN Evolution

1996	CDC Funded Nation-wide-Health Alert Network (HAN)	24/7 alerts & info for PH emergencies in communities
2002	Bio-Terrorism Act Passed (BT Act)	Response to 9-11
2004	CDC Funded PHIN 1.0	BT Act & 9-11
2005	PHIN 1.0 released by CDC	Support Preparedness
2006	Pandemic and All-Hazards Preparedness Act	Avian Flu Threat
2006	ONC-AHIC-NHIN via President Executive Order	Develop EMR by 2014
2007	PHIN 2.0 Released by CDC Focus on Interoperability for all PH Activity	Align PHIN with NHIN Initiatives

Public Health Activities Cycle
(Business Process)



PHIN
Public Health Disaster Management Preparedness Functional Areas



PHIN 2.0 Requirements

PHIN 2.0 Requirements

PHIN 2.0 Technical Requirements Focus:

- Interoperability & Data Exchange
- Availability and Security

PHIN Certification

- Criteria for Availability & Security certification from NIST 800-53
- Certify the ability of system components perform specific PHIN functions

PHIN 2.0 Security Requirement

5. PHIN Systems must be secure and have the appropriate level of availability and accessibility
Standards
▪ FIPS 199 ▪ FIPS 200 ▪ NIST 800-53

Availability: “Ensuring timely and reliable access to and use of information……

A loss of *availability* is the disruption of access to or use of information or an information system

FIPS 199

Provides a common framework for **security categorization** and determine potential impact on ***Availability.***

3 Levels: Low Moderate **High**

*High Potential Impact: The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals*

FIPS 200

- Specifies minimum security requirements for FIPS 199 Categorization
- Cover 17 areas with regard to protecting the confidentiality, integrity, and availability
- For *high-impact* information systems, must employ appropriately tailored security controls from the high baseline of security controls defined in NIST 800-53

NIST 500-53

Recommended Security Controls

- Provides guidelines for selecting and specifying security controls
- Consistent and repeatable approach for selecting and specifying security controls
- Security controls for the 17 areas defined in FIPS 199

Example: Configuration Management

PHIN 5.3.17 Control: The organization develops, documents, and maintains a current baseline configuration of the information system. ***[Source: NIST 800-53 CM-2]***

NIST 800-53 CM-2 BASELINE CONFIGURATION

(1) The organization updates the baseline configuration of the information system as an integral part of information system component installations.

(2) The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system.

LOW CM-2 MOD CM-2 (1) **HIGH CM-2 (1) (2)**

PHIN Current Status

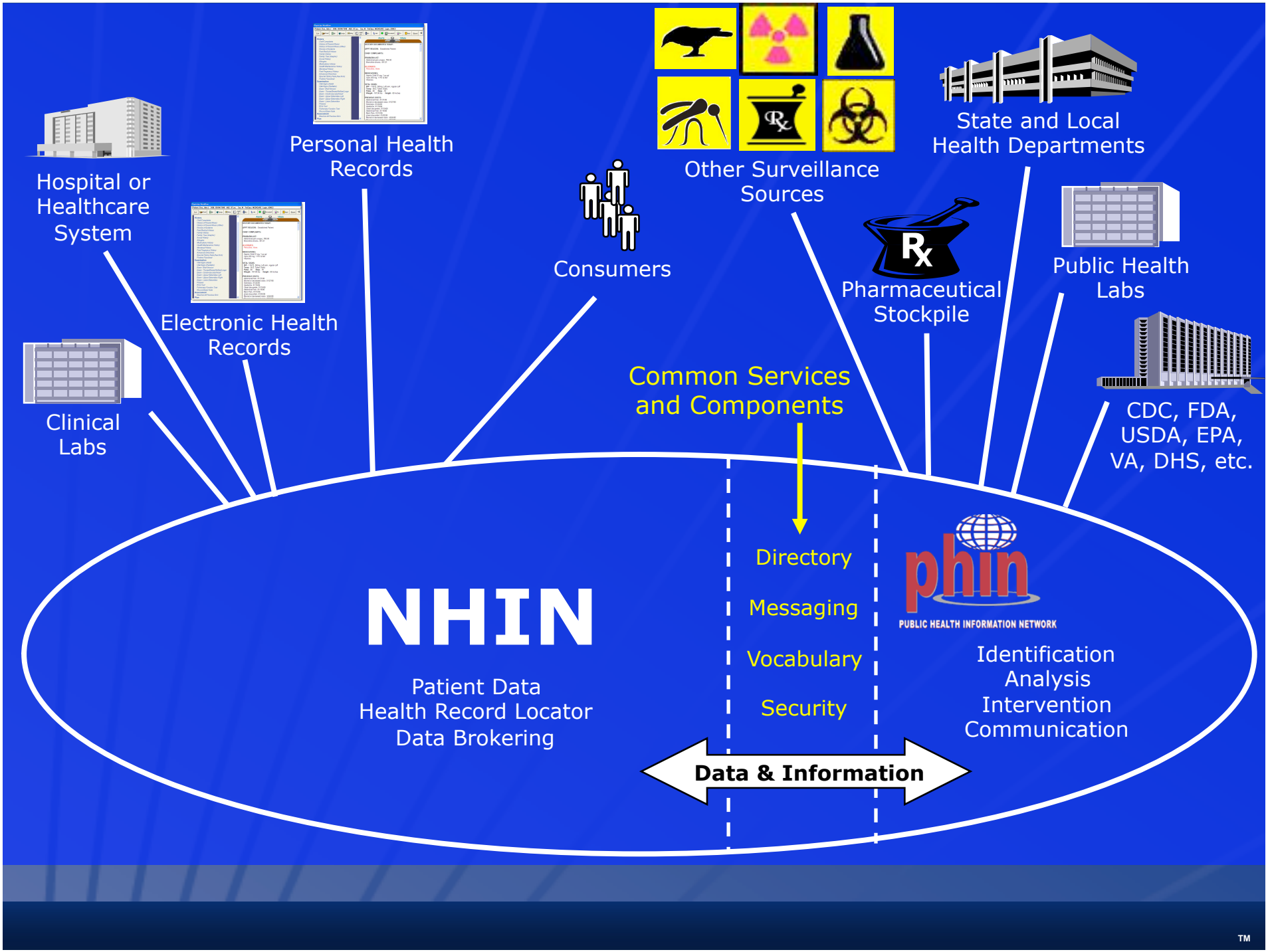
- State - Local Public Health Political Organization Varies
- State HANs – in place; Other systems still various stages of implementation/ development
- NC: State and Local Public Health separate entities (state funding vs. county funding)
- NC: n-tiered, web-based client-server
- Agreement: Local PH uses state-based hosted applications

PHIN

- Future Architectures
  - Service-Oriented Architecture - federated data
  - Distributed Grids
  - Internal and External Partner Interoperability
- Some of the Issues
  - Impact to current PHIN infrastructure
  - Internet Connectivity Local Level- High Availability , Performance
  - Centralized vs. Decentralized Infrastructure and Service Management

PHIN & RHCPP Partnership

Strengths	•Common Needs •Funding Requirements
Weaknesses	•Project Management •Awareness •Champions
Opportunities	•PHIN Coordinator in Each State
Threats	•Funding •Local Resources (Technical-SME)


Hospital or Healthcare System
Personal Health Records
Other Surveillance Sources
State and Local Health Departments
Electronic Health Records
Consumers
Pharmaceutical Stockpile
Public Health Labs
Clinical Labs
Common Services and Components
CDC, FDA, USDA, EPA, VA, DHS, etc.
NHIN
Patient Data
Health Record Locator
Data Brokering
Directory
Messaging
Vocabulary
Security
phin
PUBLIC HEALTH INFORMATION NETWORK
Identification
Analysis
Intervention
Communication
Data & Information
TM

Herded Cat

Conclusions

RHCPP is Very Important for PHIN

- *"All Disasters are Local"*
- *Effective systems used in a disaster are every-day systems*

Relationships with PHIN Coordinator & RHCPP Needed

Resources:
NIST Documents: csrc.nist.gov/publications
CDC PHIN: www.cdc.gov/phin
John.mclamb@ncmail.net
919-707-5063

phin PUBLIC HEALTH INFORMATION NETWORK
CONNECTING PUBLIC HEALTH

NCPH North Carolina Public Health
DPH Information Technology