phin

PUBLIC HEALTH INFORMATION NETWORK

CONNECTING PUBLIC HEALTH

“RHCPP & PHIN Relationships for Providing Public Health Disaster Management Capabilities”

Focus on Rural Health Care
Pilot Program Workshop
October 16 & October 17, 2008

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

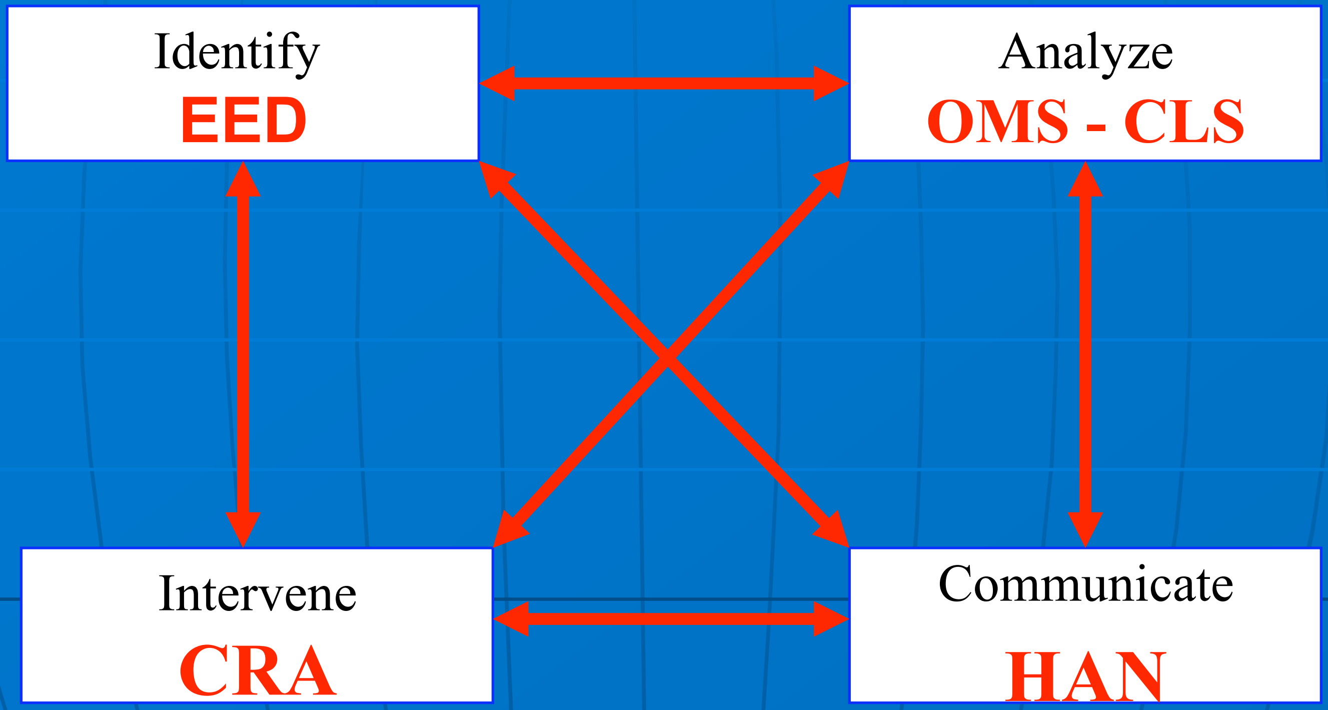
PHIN TimeLine

1996	CDC Funded Health Alert Network (HAN)	
2002	Bio-terrorism Act Passed	After 9-11
2004	CDC Funded PHIN	
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

PHIN
Preparedness Functional Areas

1. Early Event Detection (EED)
2. Outbreak Management System (OMS)
3. Countermeasure & Response Administration (CRA)
4. Partner Communications & Alerting (PCA)
5. Connecting Laboratory Systems (CLS)
6. Cross Functional Components (CFC)

PHIN Preparedness Activities Cycle



Identify
EED

Analyze
OMS - CLS

Intervene
CRA

Communicate
HAN

PHIN Requirements & RCHPP Recipients

PHIN 2.0 Technical Requirements Focus

- Interoperability & Data Exchange
- Availability and Security

PHIN Certification

- Assessment / audit every 2 years
- Scope of audit

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 ***<u>Availability.</u>***

3 Levels: **Low** **Moderate** **<u>High</u>**

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
PUBLIC HEALTH INFORMATION NETWORK

CONNECTING PUBLIC HEALTH

Discussion / Questions

Resources:
NIST Documents
http://csrc.nist.gov/publications/PubsSPs.html
CDC PHIN
http://www.cdc.gov/phin/

More Info, PHIN Coordinator in Your State:
John.mclamb@ncmail.net
919-707-5063

NCPH
North Carolina
Public Health
DPH Information Technology