The Practice **of Informatics**

JAMIA

Implementation Brief ■

The Public Health Information Network (PHIN) Preparedness Initiative

JOHN W. LOONSK, MD, SUNANDA R. MCGARVEY, LAURA A. CONN, MPH, JENNIFER JOHNSON

A b s t r a c t   The Public Health Information Network (PHIN) Preparedness initiative strives to implement, on an accelerated pace, a consistent national network of information systems that will support public health in being prepared for public health emergencies. Using the principles and practices of the broader PHIN initiative, PHIN Preparedness concentrates in the short term on ensuring that all public health jurisdictions have, or have access to, systems to accomplish known preparedness functions. The PHIN Preparedness initiative defines functional requirements, technical standards and specifications, and a process to achieve consistency and interconnectedness of preparedness systems across public health.

■ **J Am Med Inform Assoc.** 2006;13:1–4. DOI 10.1197/jamia.M1815.

The Public Health Information Network (PHIN) Preparedness initiative is implementing, on an accelerated pace, a consistent national network of public health preparedness information systems. PHIN Preparedness uses the principles and practices of the broader PHIN initiative, to ensure that all public health jurisdictions will have, or have access to, systems to accomplish known preparedness functions. The anthrax attacks of 2001 revealed substantial challenges in assimilating and processing data received from multiple disparate data sources in frequently incompatible formats. The attacks, compounded by many events subsequent to the attacks, showed that preparedness systems need to be implemented at all levels of public health. The PHIN Preparedness initiative defines a process to achieve consistency and interconnectedness of preparedness systems across public health.

Case Description

A great deal has been learned about how information systems can contribute to public health preparedness since the anthrax attacks in 2001. At that time, the contributions of information technology were principally considered to be supportive, noncritical, and focused mostly around the technologies of e-mail and fax. During and since the anthrax attacks, a succession of public health events helped define what information systems can do for preparedness. These events showed the need for consistency and interconnectedness of information systems in public health nationally. They also helped to solidify the acceptance of specific information systems as a core element of preparedness.

The Public Health Information Network (PHIN) is a national multiorganizational business and technical architecture for public health information systems. PHIN was first funded in 2004 to help advance and coordinate public health information systems. In 2004, the Department of Health and Human Services and the Centers for Disease Control and Prevention (CDC) awarded $849 million through the Public Health Response and Preparedness Cooperative Agreement to help improve preparedness in all 50 states, 4 metropolitan areas, and 8 US territories.[1] Some estimate that as much as 25% to 30% of these funds were used for information technology. PHIN strives to elevate the capabilities of public health information systems and integrate them across the variety of organizations that participate in public health and the wide variety of public health functional needs. The goal of the PHIN Preparedness initiative is to implement, on an accelerated pace, a consistent national network of preparedness systems. PHIN Preparedness uses the principles and practices of the broader PHIN initiative to concentrate, in the short term, on ensuring that all public health jurisdictions have, or have access to, systems to accomplish known preparedness functions.

Methods

During the fall of 2004, the CDC, the Association of State and Territorial Health Officials (ASTHO), the National Association of County and City Health Officials (NACCHO), the Council of State and Territorial Epidemiologists (CSTE), and the Association of Public Health Laboratories (APHL) completed a series of regional conferences to refine and validate the needs for preparedness systems and the standards necessary to implement them. These requirements, detailed specifications, example systems that instantiate them, and certification tools represent the core PHIN Preparedness elements being used to implement PHIN Preparedness nationally. A glossary of public health terms and standard industry references is available in Appendix 1 as an online *JAMIA* data supplement available at www.jamia.org.

Specifically, the PHIN Preparedness process:

1. Defines the functional requirements that must be supported. In the PHIN Preparedness initiative, this is done collaboratively with public health partners and serves to establish *what* public health activities must be supported as an essential step before determining *how* they must be supported (PHIN Preparedness Functional Requirements: www.cdc.gov/phin). The requirements are divided into separate functional areas, but there is no expectation for a one-to-one correspondence between implemented systems and functional areas.
2. Identifies relevant industry standards. These standards allow public health to interoperate at the federal, state, and local levels and with clinical care and other networks. The first set of standards designated by the Consolidated Health Informatics (CHI) Initiative noted many of those used by PHIN and illustrates the broad acceptance of these standards.

3. Develops specifications based on these standards that are concrete enough to provide explicit direction for implementation. In PHIN, substantial work has gone into developing industry standard specifications for data exchange messages, vocabularies, and technologies, some of which are listed below:

- Industry Standard Messaging Specifications: Health Level 7 (HL7) implementation guides for disease case reports, laboratory tests, and laboratory results, and for the exchange of certain clinical care data with public health. Public health–specific messages are based on HL7 version 3, and messages for the exchange of lab/clinical care data with public health are based on HL7 version 2 messaging standards.
- Industry Standard Vocabularies for messages and data models: Logical Observation Identifier Names and Codes (LOINC), Systematized Nomenclature of Medicine (SNOMED), ICD-10 for mortality, ICD-9CM for morbidity, and HL7 Vocabularies.
- Secure, Bidirectional Automated Exchange of Data over the Internet: ebXML (built on Simple Object Access Protocol [SOAP] Web services), Hypertext Transfer Protocol (HTTP), Public Key Infrastructure (PKI). This can be implemented with any software, but is made available to our partners through the PHIN Messaging System (PHIN MS).[2]
- Strong Security: Used for authentication, digital signature, and encryption of data/information using PKI are a part of the e-Gov E-Authentication initiative.[3] Data are transmitted using Secure Sockets Layer (SSL) over the CDC's Secure Data Network. Currently, CDC has issued over 4,700 certificates nationally to use this system.
- Directories of Public Health and Clinical Personnel: Used to identify people, roles, and contact information for public health participants and supports exchange
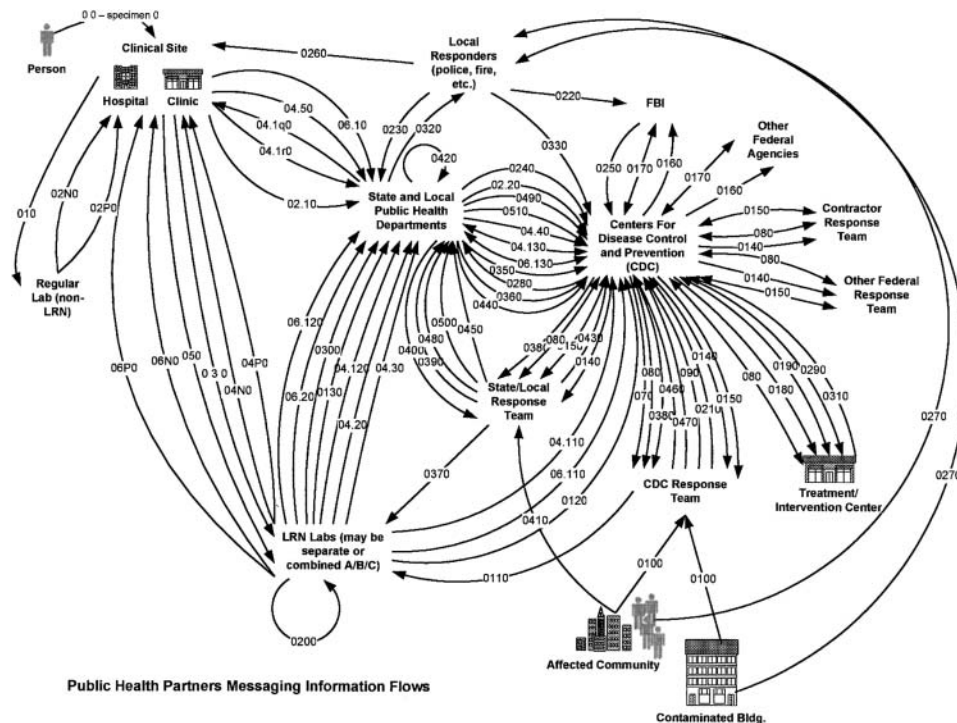

Figure 1.

Table 1 ■ Examples of PHIN Functional Requirements

PHIN Functional Areas	Example Requirements
Early event detection	Secondary use of clinical care and other health-related data for early identification of public health events
	Reportable disease case reporting from clinical care via the Web and 24/7 call reporting systems with triage of disease urgency
	Situational awareness of the size, location, and spread of a health event using secondary use data and case reporting
	Disease data exchange using HL7-specific implementation guides
	Detection algorithms to determine and visualize deviation from normal disease patterns
Outbreak management	Case investigation and management
	Exposure contact tracing
	Exposure source investigation and linking of cases and contacts to exposure sources
	Data collection, packaging, and shipment of clinical and environmental specimens
	Integration with early detection and countermeasure administration capabilities
	Linking laboratory test results with clinical case data
	Flexibility to support agent-specific and emerging requirements while adhering to standard terminology and data relationships
Connecting laboratory systems	Standard HL7 message formats and terminology standards for specimen receipt and laboratory result reporting
	Receipt and management of specimen and sample data
	Monitoring of testing activity to project load distribution during a large-scale event
Countermeasure and response administration	Support and track administration of vaccinations and prophylaxes
	Support apportionment and allocation for limited supplies
	Traceability to drug lot, vaccinator, or clinic
	Adverse events monitoring
	Follow-up of patients (e.g., vaccine "take" response evaluation)
	Isolation and quarantine monitoring and tracking
	Links to distribution vehicles (such as commercial distribution channels and the Strategic National Stockpile[2]) to provide traceability between distributed and administered products
	Integration with immunization and disease registries
Partner communications and alerting	Rapid distribution of health alerts and communications to public health workers, primary care physicians, public health laboratory workers, the public, etc.
	Multiple channels of distribution: e-mail, pagers, voicemail, and/or automated faxing
	Selective distribution based on the urgency and sensitivity of the message
	Collaborative communications (Web boards, threaded discussions, and Web conferencing) among a defined set of involved public health professionals
Cross-functional components	Secure message transport: ensuring messages are received and read only by intended audiences
	Public health directory for consistent, uniform management of people, roles, organizations, organization types, and jurisdictions when exchanging information
	Recipient addressing: identifying appropriate recipient lists for information exchange
	Terminology standards: adhering to standard vocabulary lists and structures
	System security and availability: protecting systems from sabotage or failure, and protecting data from corruption or unauthorized access
	Privacy: protecting patients and organizations from fraudulent or unauthorized use of their information

among partners based on Lightweight Access Directory Protocol's (LDAP) Directory Service Markup Language (DSML).

- Alerts and Notifications for Public Health and Clinical Personnel: Used to send alerts and notifications to specific roles and appropriate public health participants and being developed around the Common Alerting Protocol.[4]
- Information Presentation and Knowledge Management: Metadata for organizing public health information for searches and presentation on the Internet and by other means such as alerts. Standards used include Medical Subject Headings (MESH), ISO-11179, Dublin Core, LOINC, SNOMED, ICD-9CM, expressed through the Public Health Thesaurus extension of the National Library of Medicine Metathesaurus.[5]

4. Makes software solutions available that can be used to fill functional needs. These solutions range from complete applications to services that perform specific functions. The CDC has developed this software for public health partners who do not have systems that meet the functional requirements or specifications. Descriptions of CDC-developed software designed to support preparedness is available in Appendix 2 as an online *JAMIA* data supplement at www.jamia.org.

5. Certifies that partner capabilities meet the functions and specifications. The CDC provides certification tools to support self-assessment against functional requirements and validation of electronic data messages. Formal certification, delivered by an external certification team, follows self-assessment.

The diagram in Figure 1 resulted from a study conducted by the CDC to determine the data and information exchanges involved in the anthrax response of 2001.[6] It illustrates the complexity of the processes that provide or consume information and the interdependencies among the different organizations that form a complete public health response. However, this study was only the beginning and the initial list of requirements has been built on by the diverse organizations and activities that comprise public health.

The PHIN Preparedness initiative has organized these functional requirements into six broad areas: Early event detection, Outbreak management, Connecting laboratory systems, Countermeasure and response administration, Partner communications and alerting, Cross-functional capabilities and components. Examples of these functional requirements are shown in Table 1, and corresponding documents[2] are available at www.cdc.gov/phin.

Discussion

PHIN Preparedness defines a series of functional system areas that are necessary for public health preparedness and a process by which they are being implemented nationally to have a consistent and interoperable preparedness system infrastructure. State and local investment in information technology is respected, but is also guided with specific requirements, standards, specifications, and certification. For those who do not have systems, or those who need a "bridging" system, the CDC has developed software and systems that meet these requirements. The association of PHIN with the CDC preparedness funding makes the implementation of PHIN Preparedness achievable nationally to work to meet the public's expectations of public health preparedness.

References ∎

1. Department of Health and Human Services, Washington, DC, June 17, 2004. HHS awards $849 million to improve public health preparedness [online]. Available at: http://www.hhs. gov/news/press/2004pres/20040617.html. Accessed May 2005.
2. Centers for Disease Control and Prevention, Atlanta, GA. PHIN Preparedness Functional Requirements. Available at: www.cdc.gov/ phin. Accessed May 2005.
3. eGov, Washington, DC. Technical Approach for the Authentication Service Component Version 1.0.0, June 28, 2004. Available at: http://www.cio.gov/eauthentication/documents/ TechApproach.pdf. Accessed May 2005.
4. Organization for the Advancement of Structured Information standards (OASIS). Billerica, MA. Available at: http://www. oasis-open.org/home/index.php. Accessed May 2005.
5. US National Library of Medicine, 8600 Rockville Pike, Bethesda, MD. Available at: http://www.nlm.nih.gov/pubs/factsheets/ umlsmeta.html. Accessed May 2005.
6. Klein T, Morris T. Centers for Disease Control and Prevention, Atlanta, GA. Public Health Messaging Infrastructure Information Flow Analysis and Architecture, August, 2002. Available at: www.cdc.gov/phin. Accessed May 2005.