PHIN Preparedness

(DRAFT for discussion)

CROSS FUNCTIONAL COMPONENTS REQUIREMENTS

Version 0.1 Draft

11/1/2004

TABLE OF CONTENTS

1 INTRODUCTION

This document describes components of Public Health Information Network (PHIN) that are common across PHIN functional areas for preparedness. These "cross functional components" are referenced from appropriate points within the PHIN functional requirements documents, and are an integral part of each area of PHIN preparedness. Cross functional components include directory and directory exchange, terminology, data modeling, secure message transport, security, operations, and privacy. Only those requirements that cross functional areas are described in this document, specific requirements considered unique to a given PHIN functional area are covered in the functional area document.

2 CROSS FUNCTIONAL COMPONENT REQUIREMENTS

The following requirements describe baseline functionality that crosses PHIN functional areas.

2.1 Secure Message Transport: To ensure that data exchange messages are transported across secure channels, received and used by only the intended audience, messages must be encrypted, and be addressed to appropriate recipients.

2.2 Public Health Directory: A detailed record must be kept of the sample from the collection point through the testing and result reporting process.

2.3 Directory Exchange: Information held in public health directories should be shareable.

2.4 Data Message Addressing: A detailed record must be kept of the sample from the collection point through the testing and result reporting process.

2.5 Object identifiers (OIDs): Unambiguous identification is required for vocabularies and entities.

2.6 Vocabulary Standards: Standard vocabulary lists and data structures have been defined by various organizations. Where they exist, preparedness systems should utilize them. As additional standards are defined, they should be accepted and implemented.

2.7 Data Modeling Standards: Standard data models have been defined and data repositories developed be partners should be able to map to the concepts and maintain the associations defined in the standard models.

2.8 Operations: Personnel, roles, and responsibilities necessary to support preparedness systems should be clearly defined**.**

2.9 System Security and Availability: Security includes the protection of data from corruption and access by unauthorized individuals, as well as the protection of the system itself from sabotage or other failure.

2.10 Privacy: Patients and organizations must be protected from fraudulent and unauthorized use of their information.

2.1 SECURE DATA MESSAGE TRANSPORT

Secure Transport Protocol refers to the ability to transport a message or file in a mode that can only be interpreted by the intended party. The PHIN relies on the public Internet to support inter-organizational information data exchange. Security and

privacy requirements necessitate that information generally be encrypted and that communications be performed in a way which ensures delivery to the intended recipient(s) and only the intended recipient(s). Secure Transport requires adoption of standards that include ebXML, PKI, and SSL, which are described below. The CDC has developed PHIN MS as an implementation of the standards supporting secure message transport, and exchange partners must use a secure transport protocol that is compatible with PHIN MS.

> PHIN MS fully implements PHIN standards for secure messaging and is available from CDC. More information on PHIN MS is available at *http://www.cdc.gov/phin/messaging/index.htm*. PHIN MS, however, is not required so long as PHIN data exchange requirements can be met using a PHIN MS compatible solution.

2.1.1 Transport Standard

2.1.1.1 The ebXML Messaging Service (ebMS) is the PHIN standard for message transport across the public internet and must be used when sending sensitive health data information between partner organizations. It supports a neutral format for carrying messages between different systems, such as between legacy systems and web services applications. It is designed to work with any communications protocol, and the content of messages carried over ebMS can be in any format.

The ebMS standard is a set of layered extensions on the Simple Object Access Protocol (SOAP) to support business-to-business transactions. For more information on ebXML and ebMS see *http://www.oasis-open.org/home/index.php*.

2.1.2 Secure Connection

2.1.2.1 Hypertext Transfer Protocol over Secure Socket Layer (SSL), or HTTP over SSL (HTTPS) is a web protocol that encrypts and decrypts user page requests as well as the pages that are returned by the web server. HTTPS is really just the use of SSL as a sub-layer under its regular HTTP application layering. HTTPS is required to ensure secure communication.

2.1.2.2 Strong authentication mechanisms must be applied to data exchange partners, as described in section *2.6 System Security and Availability*.

2.1.2.3 Messaging partners must be authorized to send data, as described in section *2.6 System Security and Availability*.

2.1.3 Message Encryption

2.1.3.1 The XML Encryption standard should be used to represent the encrypted content and the information that enables an intended recipient to decrypt it. The standard makes use of public key infrastructure (PKI) so that only the intended receiver can read the message. The public key of the intended

message recipient is used to encrypt the message. Upon receipt, the recipient decrypts the message using their private key. For more information on XML Encryption see *http://www.w3.org/TR/xml-encryption-req*.

2.1.4 Digital Signatures

2.1.4.1 The XML Digital Signature standard should be used to insure message integrity and signer authenticity. Digital signatures are created by performing an operation on information such that the receiver of the message can confirm that the author of restricted information created the message and that the signed message has not subsequently changed. For more information on XML Digital Signature see *http://www.w3.org/TR/xmldsig-core*.

2.1.5 Message Send and Receipt

2.1.5.1 Exchange partners must be able to acknowledge successful receipt of messages and send an error message for messages that were unsuccessful.

2.1.5.2 Exchange partners must be able to send messages to one or more targeted recipients, and automatically resend messages that failed transport or were not acknowledged as received.

2.1.5.3 Non-repudiation is required to ensure transferred messages have been sent and received by the parties claiming to have sent and received the messages. Non-repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message. Non-repudiation can be achieved through the use of

- Digital signature -- serves as a unique identifier for an individual (much like a written signature).
- Confirmation service -- utilizes a message transfer agent to create a digital receipt (providing confirmation that a message was sent and/or received).
- Timestamp -- proves that a document existed at a certain date and time.

2.1.5.4 The initiator of an exchange should have the ability to recognize receipt acknowledgement and discontinue resends to the recipient. (Once and Only Once)

2.1.5.5 Stored data from messages should be protected using strong authentication and authorization as described in section *2.6 System Security and Availability*.

2.2 MESSAGE ADDRESSING

2.2.1 Exchange partners must have the ability to target HL7 messages for distribution to the appropriate recipient(s).

2.2.2 Messages may be addressed automatically via information associated with the data (such as “test requestor”), or may be addressed individually through a user interface.

2.2.2.1 The system should be able to interface with a directory service (or registry) to address message recipients.

2.2.2.2 An enhanced capability is to determine message recipients based on the message type or priority (messages that should initiate an alert, or that provide lab positive case confirmation should have a higher priority and potentially a broader or different audience.).

2.2.2.3 Exchange partners must be able to include the appropriate level of "identifying" information in each message based upon the level of privacy that to be maintained for each addressed party.

2.2.3 It must be possible to address a copy of a message to multiple recipients.

2.3 PUBLIC HEALTH DIRECTORIES

A local instance of a directory is a central secure repository that stores contact information for public health organizations, personnel and health responders (including primary clinical practitioners). Public health directories support alerting and partner communications, as well as organization and person information for other preparedness applications. Directories can be used to support access control to resources. Local instances of a Public Health Directory must contain contact information, roles, jurisdictions and communication devices for organizations and persons involved in public health activities.

2.3.1 Local instances of a public health directory must be compatible with the PHIN DIR schema v1.1. (More information regarding PHIN DIR schema v1.1 may be found at *http://www.cdc.gov/phin/phindir/docs.htm*.) Compatibility here means that the local implementation use the same attributes and vocabularies as defined in PHIN DIR v1.1, or equivalent, mapable attributes are used and directory information can be exchanged according to the requirements described in section *2.3 Directory Exchange* of this document

2.3.2 Unique identifiers should be defined for people and organizations stored in the directory. Please reference the object identifiers section in this document for more detail regarding unique identification across a namespace.

2.3.3 The directories should, minimally, be able to support the retrieval of individuals based on name, public health role, organizational affiliation, geographical location, jurisdiction, or combinations of this list.

2.3.4 Local instances of a Public Heath Directory should be integrated with applications and systems requiring access to contact information (i.e., Alerting systems).

2.3.5 The directories can be used to support authentication and authorization of identified personnel to control access to electronic resources.

2.4 DIRECTORY EXCHANGE

Information held in local instances of a public health directory must be shareable to ensure that partners have the most current contact information and can support cross-jurisdictional communications. Directory exchange is aimed at increasing directory

accuracy, reducing redundant maintenance of information in local directories and distributing the burden of maintenance across organizational entities.

There are three main aspects involved in directory exchange: a common exchange schema is required to describe the attributes to be exchanged, a standard exchange protocol must be used to describe the content and the action to be taken by the recipient, and the exchange must be executed in adherence with secure transport requirements.

2.4.1 Current directory information should be exchanged a minimum of once a month.

2.4.2 Exchange Schema

PHIN DIR is the schema that describes the common set of directory attributes to be exchanged among public health partners. It is a reference model for LDAP directories in public health that provides a common definition of attributes.

2.4.2.1 Exchange partners are not required to implement the PHIN DIR schema in as their directory but they are encouraged to implement the schema if at all possible to simplify the data exchange process.

2.4.2.2 Exchange partners are required to be able to map their directory attributes and terms to the required schema attributes defined within the Public Health Directory schema.

2.4.2.2.a The directory exchange schema includes the following classes: people, public health roles, organizations and organization types. Exchange partner must be able to map their directory attributes to these classes and vocabularies.

2.4.3 Directory Service Markup Language (DSML)

DSML is the language used to describe directory content during an exchange and the action that should be taken by the exchange recipient. DSML combines directory services technology (LDAP) with XML syntax and to provides an easy way to share directory data across organizations, different directory implementations and different platforms. It provides an XML DTD and a schema for reference (DSML namespace: http://www.dsml.org/DSML).

2.4.3.1 Exchange partners are required to be able to participate in DSML-based directory exchange as if they had an LDAP directory.

2.4.3.2 Exchange partners are encouraged to implement an LDAP directory if possible.

2.4.4 Secure Message Transport for Directory Exchange

2.4.4.1 Exchange partners are required to send and receive directory exchange messages using secure message transport protocol that is PHINMS compatible. Please reference the secure message transport section in this document for more detail regarding unique identification across a namespace.

2.4.5 Directory Sharing Policy

Directories contain a combination of public and private information. Inter-organizational policy is required to protect private information and ensure it is used appropriately and viewed only by authorized individuals and used appropriately.

2.4.5.1 Partners will prevent users of their directory from viewing information of people in other organizations.

2.4.5.2 Partner organizations will not release directory information shared by another partner to a third party without specific consent of the owning party.

2.4.5.3 Public person attributes can be exchanged across organizations, replicated to other directories and viewed by all users.

2.4.5.4 Private person attributes must be treated as sensitive but unclassified (SBU) information. Therefore, exchange partners will implement security controls to limit access to private information, including encryption of private information during exchange.

2.4.5.4.a Private person attributes may be read and utilized by authorized individuals when addressing alerts.

2.4.5.4.b Private person attributes may be accessed by administrators when performing maintenance.

2.4.5.4.c Private person attributes may be accessed by authorized individuals in the event that manual override is required to resolve communications issues.

2.4.5.5 Organization attributes can be exchanged among organizations and are considered to be public.

2.4.5.6 Role attributes can be exchanged among organizations and are considered to be public.

2.5 OBJECT IDENTIFIERS (OID) USAGE

Object identifiers are, basically, strings of numbers that are allocated in a hierarchical manner. Once allocated a valid OID root assignment, the owner automatically has the right to assign any subsequent OIDs under their root. In order to insure uniqueness across the global namespace, OID assignment under any root must conform to established standard archetypes. So, for example, if assigned the branch "1.2.3", the owner is the only one that can say what "1.2.3.4" (or 1.2.3.n…) means. OIDs are used to provide unambiguous identification for a vast array of objects. There are a number of registries that currently allocate OIDs, and millions have already been assigned. Public health partners can contact the CDC for an OID root assignment.

In the PHIN preparedness documents, OID references are written this way: numeric form of the OID, a hyphen, the symbolic name. All of the OID(s) that are being defined for use within the PHIN are under the PHIN root. The CDC has defined branch four, under the CDC OID, for the PHIN:

2.16.840.1.114222.4 - PHIN root

However, messages such as those for HL7-registered coding systems are under the HL7 root, though they are used within PHIN.

Several categories exist under the PHIN root. A set of branches under this root have been defined which loosely mirror the branches that have been defined for HL7 to manage its own kinds of OID namespace. These branches are:

OID	Symbolic Name	Description
2.16.840.1.114222.4	CDC_PHIN_root	Root of the OIDs used in the CDC PHIN (Public Health Information Network)
2.16.840.1.114222.4.1	Partner IDs	Root for Messaging Partner IDs (LRNs, DOHs, Field Team System, etc.)
2.16.840.1.114222.4.11	CDC_Value_Sets	CDC Defined Value Sets
2.16.840.1.114222.4.19	PHIN_EXAMPLES	Root for published examples for messaging and coding systems, etc.
2.16.840.1.114222.4.2	PhysObjects	Root for Physical Objects
2.16.840.1.114222.4.3	InfoArtifacts	Root for Information Artifact Namespaces
2.16.840.1.114222.4.4	SRTClass	Root for SRT Class Definitions
2.16.840.1.114222.4.5	CDC_CS	CDC-Authored and maintained coding systems
2.16.840.1.114222.4.6	CDC_External_Code_Systems	External coding system used by CDC

2.5.1 In PHIN Preparedness systems, OID(s) must be used for three primary purposes:

1. Identification of vocabulary items – Code Systems and Value Sets, SRT(s)
2. Identification of namespaces used in Public Health – Subject IDs, Specimen IDs, Result IDs, etc.
3. Identification of well known Objects – Messaging Partners, Physical Locations, Organizations, Contacts, etc.

2.5.2 Public health partners must contact from bttech@cdc.gov to request an OID branch.

2.5.3 In PHIN Preparedness systems, OID(s) must be used to uniquely identify organizations, physical locations, contacts, subjects and specimens.

2.5.4 PHIN Preparedness systems must include assigned OIDs when exchanging data with partner organizations.

2.5.5 Data recipients must retain OIDs received as a part of data exchange (i.e. Specimen ID received with a test order), and include them when returning information to the sender (i.e. include the Specimen ID when returning test results for the test order).

2.6 VOCABULARY

It is recommended the PHIN data at standards be used with all preparedness systems; however, it is required that vocabulary standards be used when exchanging data.

2.6.1 Standardized vocabulary must be used to exchange data among public health partners to ensure that the data can be read and understood.

2.6.2 Adherence to standards may be accomplished either by mapping local codes to standard codes, by directly implementing standard codes, or by a combination of direct implementation and mapping. Mappings of local codes to standards should be maintained at local sites and the mappings do not need to be shared or registered with PHIN.

2.6.3 PHIN Vocabulary can be downloaded from PHIN VADS (Vocabulary Access and Distribution System). Vocabulary downloads are available from PHIN VADS through browser, web services and Java API methods. Downloaded PHIN Vocabulary may be maintained in a local version of PHIN VADS or another local vocabulary service.

> PHIN VADS stores and provisions standard code sets and value sets. More information on PHIN VADS is available at *http://cdc.gov/phin/vocabulary/index.htm* .

2.6.4 Vocabulary use must be regularly coordinated with the PHIN Vocabulary Services (PHIN VADS) to ensure use of the most current updates and promote consistent coding across messaging partners.

2.6.5 A mechanism must be available to implement new data standards as they become available, while still retaining the link between existing data and the standards in place when the data was created.

2.6.6 Changes and additions to standard PHIN vocabulary must be submitted though the PHIN Vocabulary Change Request process (*http://cdc.gov/phin/vocabulary/index.htm*)

2.7 DATA MODELING AND DATA REPOSITORIES

A data model is a visual diagram representing the information used in an organization, and the structure of that information. It describes how data is categorized and related, as well as other aspects of the data, such as whether a particular item is numeric or a character string. The model also describes the nature of the data relationships; for example whether the related data is required or optional, or whether one structure is a component of the other.

There are many different types of models, varying in scope and degree of detail. Some represent an entire "domain" (i.e., the domain of public health information), while others may be more specific and smaller in scope (i.e., laboratory specimen and test results). Conceptual data models present high level information concepts with limited details about specifics. Logical data models represent an image of the types of information to be captured, how it is described by attributes, and how the logical structures relate to each other. A physical data model specifies the structures, relationships, and details that are physically implemented in a system to support an application. A data repository is a physical implementation of a data model to support an application(s).

2.7.1 Data models developed to support preparedness requirements should be compatible with the PHIN Logical Data Model (PHIN LDM). This means that the model should be able to accurately represent each of the information concepts in it's domain in a manner consistent with the PHIN LDM. The PHIN LDM is available from *http://www.cdc.gov/phin/data_models/index.htm*.

2.7.1.1 Data can be discussed in terms created and defined in the PHIN Logical Data Model.

2.7.1.2 Standard vocabulary is used for coded elements where available.

2.7.1.3 Data used in an application data base, can be mapped to an accurate representation within the PHIN Logical Model

2.7.2 Data repositories should be structured to support standards-based interaction with commercial products for reporting, statistical analysis, geographic mapping, as well as the processing or queued data from and for electronic messages.

2.7.3 Data repositories should be able to associate received data with existing data (i.e., link test results with a specimen, and link a specimen with the corresponding subject).

2.7.4 Data repositories should implement common database technology (i.e. Sybase, Oracle, SQL Server) running on Windows NT / 2000 / XP. LINUX or UNIX and supporting ODBC, ANSI standard SQL and JDBC access.

2.8 OPERATIONS

Operational requirements, such as system backup policies and procedures, continuity of operations, system monitoring, and employee training ensure that public health partners can effectively support preparedness activities.

2.8.1 Operational processes must be defined in detail for successful data exchange (bundling, parsing, formatting, etc), data mapping, analysis, visualization, reporting, and alerting of public health events.

2.8.2 Operational requirements including processes, personnel, and responsibilities must provide clear instruction about supporting, maintaining, testing and exercising preparedness systems and data exchange capabilities.

2.8.3 Policies must be in place to ensure personnel are trained to support and maintain preparedness systems.

2.8.4 Policies must be in place to ensure security patches and configuration corrections are applied promptly, and to manage application of new versions of software, components or terminologies.

2.8.5 Operational processes must be defined to create and maintain data usage agreements.

2.8.6 Personnel should be available to quickly resolve any data exchange and connectivity issues.

2.8.7 Interfaces with other systems must be monitored and managed by trained, qualified personnel to ensure the lines of communication remain constantly open and accessible.

2.8.8 Continuity of Operations (COOP) – Electronic Data Exchange capabilities are subject to COOP requirements and should conform to service levels and be recoverable in the event of disaster.

2.8.8.1 A backup process should be fully defined for use in the event that the intended electronic data management system is temporarily unavailable.

2.8.8.2 A system backup and restore plan must be implemented to recover active laboratory data in the event of a catastrophic system failure.

2.8.8.3 Regular backups of the entire system should be conducted.

2.8.8.4 Daily data backups should be stored at an off-site facility.

2.8.9 Infrastructure and operational processes around electronic data exchange must support security and stability standards as indicated in NIST 800 series guidance.

2.9 SYSTEM SECURITY AND AVAILABILITY

Systems supporting preparedness must be protected from sabotage or other system corruption. This capability involves assuring that access to sensitive or critical information and information systems is not lost, destroyed, misappropriated or corrupted by a internal or external malefactor or by systems failure or catastrophic event and that information is protected is ways that meet or exceed Health Insurance Portability and

Accountability Act (HIPAA) standards. The function should also assure that processes cannot be initiated or controlled by unauthorized individuals and that continuity of operations can be maintained subsequent to a catastrophic event.

2.9.1 The security layer must be managed for authentication, authorization, and access control.

2.9.1.1 Authentication is required to validate that the user is registered to use the system and has signed on with the appropriate user name and password or other identifiable key. Strong, two factor authentication mechanisms, such as X.509 certificates or secure token based technology, are required.

2.9.1.2 Authorization levels must be supported to manage access to system functions and data. Authorization levels can include user based, role based and/or context based authorization.

2.9.1.3 Access control rules must be implemented to enforce authorization levels and control user access to the system. For example, access control should allow a jurisdiction to view its own data but should not allow access to data for other jurisdictions, unless expressly permitted.

2.9.2 Authentication should utilize a local instance of a public health directory, or a directory service to determine which users should have access to an application or system.

2.9.3 Security patches and configuration corrections should be applied promptly.

2.9.4 Desktop and server based virus scanning, intrusion detection, network vulnerability analysis including port scanning, security policy monitoring, regular penetration testing and active threat intelligence should be employed.

2.9.5 Systems supporting preparedness must provide 24 x 7 x 365 availability, including the support of a failover system.

2.9.6 A secure internet connection should be available at all times to be used to electronically transmit or receive data. The connection should be a minimum of 56Kbps with a strong recommendation for 384Kbps or greater.

2.9.7 Messages among partners must utilize secure transport methods, as described in section 2.1 Secure Message Transport above.

2.9.8 A firewall must be employed to protect resources from external users. Firewalls will need to securely provide access to an ebXML SOAP receiver to present a service for secure Internet receipt of public health information as well as secure access to restricted access web sites.

2.9.9 PHIN security standards may be viewed using the following link: *www.cdc.gov/phin/architecture/automated_data_exchange.htm*.

2.10 PRIVACY

Privacy requirements ensure that sensitive information is not accessibly to unauthorized uses. Additional information concerning HIPAA and public health can be found in the

May 2003 MMWR report "HIPAA Privacy Rule and Public Health" http://www.cdc.gov/mmwr/pdf/wk/mm52SU01.pdf.

2.10.1 Privacy requirements ensure that sensitive information is not accessibly to unauthorized uses.

2.10.2 Privacy concerns must be addressed in order to protect the patient and organizations from fraudulent or unauthorized use of their information.

2.10.3 The confidentiality and integrity of sensitive data must be constantly protected.

2.10.4 Confidentiality agreements and data use and sharing agreements should be used as tools to address privacy concerns.

2.10.5 Protected health information (PHI) collected outside the scope of legally authorized public health data collection activities must conform to HIPAA rules regarding identifiable data.