PHIN Preparedness

CROSS FUNCTIONAL COMPONENTS REQUIREMENTS

Version 1.0

04/26/2005

TABLE OF CONTENTS

1 INTRODUCTION

This document describes the components of the 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 preparedness functional requirements documents, and are an integral part of each area of PHIN preparedness. Only those requirements that span functional areas are described in this document; specific requirements unique to a given PHIN functional area are covered in the functional area requirements document.

2 CROSS FUNCTIONAL COMPONENT REQUIREMENTS

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

2.1 Message Construction: Source data must be translated into standard message formats. A message must adhere to a specific implementation guide and data structure to ensure data exchange consistency.

***2.2 Message Routing*:** Messages must be routed to the correct destination and recipient(s).

2.3 Secure Message Transport: Messages must be securely and reliably exchanged over the Internet using the ebXML protocol.

2.4 Message Parsing: Received messages must be parsed and validated. Extracted data must be written to the appropriate data store.

2.5 Public Health Directories: Directories are repositories for contact information used for message addressing. They may also be used to support systems access controls.

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

2.7 Object Identifier Usage: Object Identifier are required in all PHIN messages to uniquely identify coding systems, identifier namespaces, and other well known objects, such as organizations.

2.8 System Architecture: Broad system-level needs, such as platforms and design standards, should be addressed by PHIN preparedness systems.

2.9 Audit Trail: A record of who has accessed records and what activities were performed must be captured.

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

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

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

2.13 System Security and Availability: Security of systems supporting PHIN preparedness includes the protection of data from corruption and access by unauthorized individuals, as well as the protection of systems from sabotage or other failure. A plan must be established for continuing activities when PHIN preparedness systems are unavailable.

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

2.1 MESSAGE CONSTRUCTION

Data is frequently communicated across public health organizations, where it is aggregated and linked with data from other sources. For partner organizations to understand information that is exchanged electronically, the information must be organized in a format that is understood by both the sender and the receiver. Since exchange partners handle many different kinds of information, more than one message format must be available for use. Consistent formats provide the rules that partner organizations follow when constructing a message to be sent and when interpreting the contents of a message that has been received. For messages to be interpreted correctly, the information must be described using a consistent set of terminologies*. *A message translator performs data validation, translation and transformation of source data into a standard message format for transmission to an external party.

2.1.1 Systems supporting data exchange must be able to construct messages for transmission.

2.1.2 Messages may contain an individual record or a batch of records.

2.1.3 Message content must comply with the PHIN message implementation guides available at *www.cdc.gov/phin*.

2.1.4 Message translators should be able to interface with an application that routes or transports a message.

2.1.5 Message translators may be developed internally, or a service or interface may be used.

2.2 MESSAGE ROUTING

Systems supporting message routing require the capability to inspect the content of the message to determine its proper destination. This relieves the message translators of performing this task and avoids coupling message translators to specific routes. The process must forward the message and routing information to a message queue or a message transport system. Message routing may be performed by a simple implementation supporting basic point-to-point messaging or the system may support dynamic message routing via advanced electronic content inspection and content filtering mechanisms.

2.2.1 Exchange partners must have the ability to automatically route specific message types to the appropriate recipient(s).

2.2.1.1 An enhanced capability is to determine message recipients based on the message type or priority (e.g., 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 Messages may be routed individually through a user interface.

2.2.2.1 An enhanced capability is to interface with a directory service (or registry) to address message recipients.

2.2.3 Systems supporting message routing must be able to route a message to multiple recipients.

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

2.2.4 Systems supporting message routing must be able to deliver routing information and message payload to a message sender.

2.2.5 A Collaborative Protocol Agreement (CPA) must be created for each sender/receiver pair. The CPA is an ebXML compliant file that specifies the conditions under which the sender and receiver will conduct transactions such as endpoints, protocols and security settings.

2.3 SECURE MESSAGE TRANSPORT

Secure Message Transport refers to the secure, reliable, bi-directional exchange of information between public health partners. 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) only. Messages are securely transported over the Internet using standards such as ebXML, PKI, and SSL, which are described below.

> The CDC has developed PHIN Messaging Service (MS) as an implementation of the standards supporting secure message transport. 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 about PHIN MS is available at *www.cdc.gov/phin*. However, PHIN MS is not required as long as PHIN data exchange requirements can be met using a PHIN MS compatible solution.

2.3.1 Transport Standard

The PHIN standard for message transport across the Internet is the ebXML Messaging Service (ebMS), used to exchange 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. More information on ebXML and ebMS is available at http://www.oasis-open.org/home/index.php.

2.3.1.1 Systems must transport messages across secure channels using the ebXML protocol. This requirement is identified as a key performance measure for assessing preparedness as described in *PHIN Preparedness Key Performance Measures,* available at *www.cdc.gov/phin*.

2.3.1.2 Each site must have a unique and valid Message Partner OID (as described in section *2.7 Object Identifiers Usage* of this document). The Message Partner OID is a unique identifier for an organization.

2.3.1.3 For partners who use PHIN MS as their method of secure transport, each instance of PHIN MS at the partner site must have a unique and valid Party Identifier (PartyID). PartyIDs are OIDs comprised of a root PHIN MS OID, sections of the message partner's OID and a unique number for the particular instance of PHIN MS at the partner's site. The PartyID indicates which instance of the software implemented within the organization sent or received a message.

2.3.2 Secure Connection

2.3.2.1 Messages among partners must use secure transport methods. PHIN security standards are available at *www.cdc.gov/phin***.**

2.3.2.2 Hypertext Transfer Protocol over Secure Socket Layer (SSL), or HTTP over SSL (HTTPS), is required to ensure secure communication. 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 the use of SSL as a sub-layer under its regular HTTP application layering.

2.3.2.2.a For user interactions with PHIN systems over the Internet, the HTTPS protocol must be used to protect communication confidentiality at all times.

2.3.2.2.b For system-to-system communication over the Internet, the HTTPS protocol must be used to protect communication confidentiality at all times.

2.3.2.2.c HTTPS should be used for communication between DMZ components and Intranet components. DMZ, or "demilitarized zone", refers to a computer or sub network that sits between a trusted internal network and an untrusted external network.

2.3.2.3 Strong authentication mechanisms must be applied to data exchange partners, as described in section *2.11 System Security and Availability* of this document.

2.3.2.4 Stored data from messages should be protected using strong authentication and authorization as described in section *2.11 System Security and Availability* of this document.

2.3.2.5 Messaging partners must be authorized to send data, as described in section *2.11 System Security and Availability* of this document.

2.3.3 Message Encryption

2.3.3.1 The XML Encryption standard should be used to represent the encrypted content and the information that enables an intended recipient to decrypt it. This 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. More information on XML Encryption is available at *http://www.w3.org/TR/xml-encryption-req*.

2.3.4 Digital Signatures

2.3.4.1 The XML Digital Signature standard should be used to insure message integrity and non-repudiation. Digital signatures are created by performing an operation on information such that the receiver of the message can confirm that the message originator created the message and that the signed message was not subsequently changed. More information on XML Digital Signature is available at *http://www.w3.org/TR/xmldsig-core*.

2.4 MESSAGE PARSING

The parser transforms a received message into the appropriate records for storage.

2.4.1.1 Systems supporting data exchange must be able to parse received messages and store parsed content in a data store.

2.4.1.2 Systems supporting data exchange must be able to save unique identifiers (such as OIDs) when storing a record.

2.4.1.3 Systems supporting data exchange must have the ability to assign unique identifiers, in the event that they are missing, to parsed records prior to storage in a data store.

2.4.1.4 Parsers must be able to interface with applications that receive and transmit messages, including error events and acknowledgements.

2.4.1.5 Systems supporting data exchange must be able to acknowledge successful parsing of messages and send an error message for messages that were unsuccessful.

2.5 PUBLIC HEALTH DIRECTORIES

A local instance of a public health directory is a secure central repository that stores contact information for public health organizations, personnel and health responders (including primary clinical practitioners). Public health directories support communication and alerting, as well as organization and person information for other preparedness applications. Directories can be used to support access control to resources.

2.5.1 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.

2.5.2 Local instances of a public health directory must be compatible with the PHIN directory exchange schema v2.0. Compatibility here means that the local implementation uses the same attributes and vocabularies as defined in PHIN DIR exchange schema v2.0, as referenced in *Appendix A*, *Appendix B,* and *Appendix C* of this document.

2.5.2.1 Local instances of a public health directory that do not use the same attributes and vocabularies as defined in the PHIN directory exchange schema v2.0 must use equivalent, mapable attributes and exchange directory information according to the requirements described in section *2.6 Directory Exchange* of this document.

2.5.3 Unique identifiers should be assigned to people and organizations stored in the directory. For more detail regarding unique identification within a namespace, please refer to section *2.7 Object Identifier Usage* of this document.

2.5.4 The directories must minimally support the retrieval of individuals based on name, public health role, organizational affiliation, geographical location, jurisdiction, or combinations of this list.

2.5.5 Local instances of a public heath directory should be integrated with applications and systems that require access to contact information (e.g., alerting systems).

2.5.6 Local instances of a public health directory may be used to support authentication and authorization of identified personnel to control access to electronic resources.

2.6 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.

2.6.1 Current directory information should be exchanged at least once a month.

2.6.2 Exchange Schema

The PHIN directory exchange schema 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.

2.6.2.1 Exchange partners are encouraged, but not required, to implement the PHIN directory exchange schema v2.0 as their directory to simplify the data exchange process.

2.6.2.2 Exchange partners must be able to map their directory attributes and terms to the required schema attributes defined within the PHIN directory exchange schema v2.0, as referenced in *Appendix A*, *Appendix B*, and *Appendix C* of this document.

2.6.2.2.a The PHIN directory exchange schema v2.0 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.

2.6.3 Directory Service Markup Language

Directory Service Markup Language (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 provides an easy way to share directory data across organizations, different directory implementations and different platforms. It provides an XML Document Type Definition (DTD) and a schema for reference. More information about the DSML namespace is available at http://www.dsml.org/DSML.

2.6.3.1 Exchange partners must be able to participate in DSML-based directory exchange as if they have an LDAP directory.

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

2.6.4 Secure Message Transport for Directory Exchange

2.6.4.1 Exchange partners are required to send and receive directory exchange messages using the ebXML protocol. For more detail regarding secure message transport, please reference section *2.3 Secure Message Transport* of this document.

2.6.5 Directory Sharing Policy

Directories contain a combination of public and private information. Inter-organizational policy must be established to ensure that private information is protected, used appropriately, and viewed only by authorized individuals.

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

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

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

2.6.5.4 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.

2.6.5.4.a Private person attributes may be read and used by authorized individuals when addressing alerts.

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

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

2.6.5.5 Organization attributes may be exchanged among organizations and are considered to be public.

2.6.5.6 Role attributes may be exchanged among organizations and are considered to be public.

2.7 OBJECT IDENTIFIER USAGE

PHIN has adopted Object Identifiers (OIDs), a standard used to construct globally unique identifiers for a vast array of objects. OIDs are strings of numbers (i.e., numeric without embedded spaces or special characters) assigned to a namespace. The complete string is hierarchical and architected as a tree. Each node on the tree represents a namespace, where all branches under each node are unique. Each node in the tree is assigned a unique, numeric identifier. The OID is constructed by placing a dot after the node, then assigning a unique integer. This process is repeated to construct a tree of arbitrary depth. The concatenation of an OID namespace and a jurisdictionally unique object identifier creates a globally unique identifier for the object that will not collide with any other identifier for the object assigned.

Partners can request OIDs from a number of organizations, including but not limited to: International Standards Organization (ISO), International Telecommunications Union-Technical Sector (ITU-T), American National Standards Institute (ANSI), Health Level Seven, Inc. (HL7) and Centers for Disease Control and Prevention (CDC). Once an OID is assigned to a partner, the partner assumes responsibility for the maintenance of additional branch assignments under that assigned OID.

2.7.1 PHIN OID Structure and Use

2.7.1.1 In PHIN preparedness systems, OIDs must be used for three primary purposes:

1. Identification of vocabulary items (e.g., code systems, value sets, and SRTs)
2. Identification of public health related namespaces within which unique identifiers (e.g., specimen identifiers, result identifiers) are assigned.

3. Identification of well known Objects (e.g., messaging partners, physical locations, organizations,)

The CDC has defined branch four (4) under the CDC OID for the PHIN root, which is 2.16.840.1.114222.4. To request an OID branch under the PHIN root, public health partners must contact bttech@cdc.gov.

2.7.1.2 PHIN preparedness systems should support the categories, or branches, that exist under the PHIN root. These branches, which loosely mirror the branches defined for HL7 to manage its own kinds of OID namespaces, are:

OID	**Symbolic Name**	**Description**
2.16.840.1.114222.4	CDC_PHIN_root	OID used in the CDC PHIN
2.16.840.1.114222.4.1	Partner IDs	Root for Messaging Partner IDs (e.g., LRNs, DOHs, Field Team System)
2.16.840.1.114222.4.11	CDC_Value_Sets	CDC-Defined Value Sets
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

The following examples illustrate how CDC builds upon the InfoArtifacts OID namespace to represent a PHIN MS sender and receiver for data exchange.

Example 1:

2.16.840.1.11422.4.3.2.2.1 – PHIN MS_Sender

```
2.16.840.1.11.422.4.3       – PHIN InfoArtifacts root
                      .2.2  – PHIN MS instance
                         .1 – Sender
```

Example 2:

2.16.840.1.11422.4.3.2.2.2 – PHIN MS_Receiver

```
2.16.840.1.11.422.4.3       – PHIN InfoArtifacts root
                      .2.2  – PHIN MS instance
                         .2 – Receiver
```

2.7.1.3 PHIN preparedness systems must include assigned OIDs when exchanging data with partner organizations.

The following example illustrates how CDC uses a jurisdictionally unique identifier and a PHIN OID to create a globally unique identifier.

- Subject ID: 556-094560
  Uniquely identifies Jane Doe in the state public health lab LIMS system (this is a jurisdictionally unique identifier).
- PHIN OID: 2.16.840.1.11422.4.3.2.2.1.100.1
  Identifies the specific LIMS system in the state laboratory in Columbus, Ohio that assigned the Subject ID to the subject.
- Globally Unique ID: 2.16.840.1.11422.4.1.100.1 556-094560
  PHIN OID + Subject ID creates a globally unique identifier.

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

2.7.1.5 Remote, disconnected systems collect data should use OIDs to avoid identifier collisions.

2.7.1.6 The root of an identifier namespace may be used to help identify erroneous or enigmatic behaviors during the testing and debugging of deployed software.

2.7.2 OID Accessibility

2.7.2.1 A list of defined and registered OIDs must be available on a 24/7/365 basis.

2.7.2.2 The update of new OID assignments must be propagated appropriately and rapidly so they can be readily used.

2.7.2.3 An OID registry should be used to support rapid OID lookups.

2.8 SYSTEM ARCHITECTURE

2.8.1 Platforms

2.8.1.1 PHIN preparedness systems should run on Windows NT/2000/XP, LINUX or UNIX platforms.

2.8.2 Development Standards

2.8.2.1 PHIN preparedness systems should be developed using generally-accepted application programming standards, including component-based development, object-oriented code development, and cross-platform implementation.

2.8.3 Design Standards

2.8.3.1 The design and development of PHIN preparedness systems should be compliant with all relevant guidelines established by Section 508 which requires that Federal agencies' electronic and information technology be accessible to people with disabilities. More information about Section 508 is available at *www.section508.gov*.

2.8.3.2 PHIN preparedness systems should be designed using generally accepted user-centered design principles, which include, but are not limited to: identifying the target audience, documenting user needs and tasks; developing task flows and models for system activities; developing screen level wire frames to illustrate system behaviors and actions; developing use cases; obtaining user approval through design review sessions; and establishing an iterative system evaluation process for collecting the user's input on the system design .

2.9 AUDIT TRAIL

2.9.1 PHIN preparedness systems must support an audit trail of data records.

2.9.2 The audit trail must record date created, created by, date modified, modified by, and the changes made to a record.

2.9.3 PHIN preparedness systems must support an audit trail of access attempts (whether successful or unsuccessful) to electronic systems and system functions.

2.9.4 An audit trail must retain the original value of key fields before and after each value modified, the modified result identified as a change, and the reason for the modification (including appropriate default values).

2.9.5 An audit trail should include information related to record modification, including: the authorization for the modification, the jurisdiction affected, and non-key fields before and after each value modified.

2.10 VOCABULARY STANDARDS

Standard vocabularies and systems of encoding data have been defined by various standards development organizations (SDOs). Reliance on these standards for terminology and coding of data greatly improves semantic understanding and therefore the value of the data to analysis and decision making. Where they exist, preparedness systems should use these standard vocabularies and coding systems. As additional standards are defined, they should be accepted and implemented.

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

2.10.2 Adherence to standards may be accomplished by mapping local codes to standard codes, by directly implementing standard codes, or by a combination of direct implementation and mapping.

2.10.2.1 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.

2.10.3 PHIN Vocabulary should be downloaded from the PHIN Vocabulary Access and Distribution System (VADS). Vocabulary downloads are available from PHIN VADS through browser, web services and Java Application Program Interface (API) methods. 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 about PHIN VADS is available at *www.cdc.gov/phin*.

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

2.10.5 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.

2.10.6 Changes and additions to standard PHIN vocabulary must be submitted though the PHIN Vocabulary Change Request process. More information about this process is available at *www.cdc.gov/phin*.

2.11 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" (e.g., the domain of public health information), while others may be more specific and smaller in scope (e.g., laboratory specimens, 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 that information 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).

2.11.1 Data models developed to support preparedness requirements must be compatible with the PHIN Logical Data Model (LDM). This means that the model must be able to accurately represent each of the information concepts in its domain in a manner consistent with the PHIN LDM. The PHIN LDM is available at *www.cdc.gov/phin*.

2.11.1.1 Data must be able to be accurately discussed in terms created and defined in the PHIN LDM.

2.11.1.2 Standard vocabulary must be used for coded elements where available.

2.11.1.3 Data used in an application database must be mapped to an accurate representation within the PHIN LDM.

2.11.2 A physical data model should be fully documented, including all essential metadata (e.g., data typing and length limits, constraints) and definitions.

2.11.2.1 An electronic data dictionary must be documented.

2.11.3 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.

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

2.11.5 Data repositories should implement common database technology (e.g., Sybase, Oracle, SQL Server) that supports ODBC, ANSI standard SQL and JDBC access.

2.12 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.

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

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

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

2.12.4 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.

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

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

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

2.12.8 Continuity of Operations

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

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

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

2.12.8.1.c Regular backups of the entire system should be conducted.

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

2.12.8.2 Infrastructure and operational processes around electronic data exchange should support security and stability standards as indicated in NIST 800 series guidance available at *http://csrc.nist.gov/publications/nistpubs/index.htm* and *http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf*.

2.13 SYSTEM SECURITY AND AVAILABILITY

Systems supporting PHIN 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 an 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.

2.13.1 User Authentication and Authorization

2.13.1.1 A user authentication mechanism must be used 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.

2.13.1.1.a Two-factor authentication (e.g., combination of password and user certificate) should be used for user interactions with PHIN systems over the Internet.

2.13.1.2 Strong authentication mechanisms, such as X.509 certificates or secure token based technology, are recommended.

2.13.1.3 User 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 (e.g., work hours vs. after-hours; on-site vs. remote; during investigation vs. normal business) authorization.

2.13.1.4 Authorization mechanisms should use a local instance of a public health directory or a directory service to determine which users should have access to an application or system.

2.13.1.5 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.

2.13.2 Secure System Management

2.13.2.1 Security patches and configuration corrections should be applied promptly.

2.13.2.2 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.

2.13.2.3 A firewall must be employed to protect resources from external threats.

2.13.2.3.a 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.

2.13.2.4 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.

2.13.2.5 Security resources such as passwords and key stores that are relied upon for user or system authentication should be protected from tampering and theft.

2.13.3 System Availability

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

2.14 PRIVACY

Privacy requirements ensure that sensitive information is not accessible 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" available at http://www.cdc.gov/mmwr/pdf/wk/mm52SU01.pdf.

2.14.1 Privacy requirements ensure that sensitive information is not accessible to unauthorized users.

2.14.2 Privacy concerns must be addressed to protect a patient, organizations, and personnel from fraudulent or unauthorized use of their information.

2.14.3 The confidentiality and integrity of sensitive data must be protected.

2.14.4 Confidentiality agreements and data use and sharing agreements must be used as tools to address privacy concerns.

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

APPENDIX A – DIRECTORY EXCHANGE ATTRIBUTES: PERSON

The following "Person" attributes or mapable equivalents noted as "Required" must be provided by a directory supporting PHIN preparedness systems. Attributes noted as "Optional" may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	Description	Required/ Optional
cn (commonName)	The person's common name, usually a first name followed by a surname.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
sn (surname)	The person's surname, or last name. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
externalUID	The person's Unique Identifier (UID) within the public health directory. This is a reference from the originating source of the data.	Optional
description	Text description of the person. This often includes their role or work assignment (e.g., Manager for the IT Services group).	Optional
displayName	Preferred name of a person, used when displaying directory entries. This is most often a concatenation of given name and surname.	Optional
givenName	The person's given, or first, name. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
mail	The person's primary e-mail address. This field is required and will be used as part of a multi-field key in the de-duplication of records within the directory.	Required
preferredLanguage	A person's preferred written or spoken language.	Optional
title	The person's job title.	Required
roles	The role(s) a person has within their primary organization.	Required
county	The FIPS code of the person's county for alerting purposes. This is a required field.	Required

Attribute	Description	Required/ Optional
organizations	Distinguished Name (DN) of the primary organization for this person. The DN is the Directory Server name to uniquely distinguish an entry. To simplify implementation, initially only one organization per person will be supported.	Required

APPENDIX B – DIRECTORY EXCHANGE ATTRIBUTES: ORGANIZATION

The following "Organization" attributes or mapable equivalents noted as "Required" must be provided by a directory supporting PHIN preparedness systems. Attributes noted as "Optional" may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	**Description**	**Type and Multiplicity**
cn (commonName)	Common name of the organization. Values for this attribute will come from the standardized vocabulary lists.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
externalUID	The organization's Unique Identifier for the sending organization. Used to support record matching.	Optional
description	Text description of the organization.	Optional
fax (facsimileTelephoneNumber)	The organization's fax number.	Optional
l (localityName)	City or town in which the organization is located.	Required
postalAddress	The organization's mailing address.	Required
postalCode	The postal code for this address (e.g., United States ZIP code).	Required
st (stateOrProvinceName)	State or province in which the organization is located.	Required
street	Street address at which the organization is located.	Required
telephoneNumber	The organization's telephone number.	Required
county	The FIPS code of the county in which an organization is located.	Required
alertingJurisdictions	A list of the county FIPS codes which define an organization's jurisdictional boundary for alerting.	Required

Attribute	Description	Type and Multiplicity
primaryOrganizationType	An organization's primary organization type. Values for this attribute will come from the standardized vocabulary lists.	Required

APPENDIX C – DIRECTORY EXCHANGE ATTRIBUTES: COMMUNICATION DEVICE

The following "Communication Device" attributes or mapable equivalents noted as "Required" must be provided by a directory supporting PHIN preparedness systems. Attributes noted as "Optional" may be provided in addition to the required attributes. These attribute names are in accordance with the PHIN directory exchange schema v2.0.

Attribute	Description	Type and Multiplicity
cn (commonName)	Common name of the communication device, such as email or telephone. This value needs to be unique within for a specific person.	Required
objectClass	Object class of the entry. Used by the server to determine required and allowed attributes for an entry.	Required
description	Text description of the communication device.	Optional
deviceName	This field contains the unique name for each device. This name will be used in most user interfaces (UI) to select the associated device.	Required
deviceType	This field contains the type of device (e.g., e-mail, telephone, fax, pager). Values for this attribute will come from the standardized vocabulary lists.	Required
coverage	This field contains the type of coverage for the device (e.g., Normal Business Hours, After Hours, 24/7/365). Values for this attribute will come from the standardized vocabulary lists.	Required
emailAddress	This field contains the e-mail address for the device. E-mail address is only valid for devices that support email addressing. Standard e-mail formatting applies.	Optional
areaCode	This field contains the area code for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional
exchange	This field contains the exchange for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional

Attribute	**Description**	**Type and Multiplicity**
line	This field contains the line for the device. This field is only valid for devices that are addressed by phone numbers (e.g., telephone, fax, mobile phone).	Optional
rank	Rank defines the contact order for devices. When contacting people, this order will be followed until the person is reached. The rank is unique for all of a person's communication devices.	Optional
pin	This field contains the pin associated with a device. This field is only valid for devices that require pin numbers (e.g., pagers).	Optional
countryPrefix	This field contains the country prefix for foreign phone numbers. Values for this attribute will come from the standardized vocabulary lists.	Optional
internationalNumber	This field contains the phone number for international numbers. This field is only valid for international phone numbers. Non-international numbers should use the areaCode, exchange and line attributes previously defined.	Optional
emergencyUseInd	This field indicates if the device can be used for emergency contact. This is a Boolean field and should be set to "true" if selected. All other values will be interpreted as false.	Optional
homeInd	This field indicates if the device is associated with a person's home. This indicator should be used to protect the identity of the defined device that is associated with a person home. If the identity of this device needs to be protected, this indicator should be set. This is a Boolean field and should be set to "true" if selected. All other values will be interpreted as false.	Optional