PUBLIC HEALTH INFORMATION NETWORK (PHIN) CERTIFICATION CRITERIA AND PROCESS VERSION 1.0

AUGUST 21, 2008

The following CDC staff and contractors directly participated in the development of this document.

Lynn Gibbs-Scharf, CDC
Tim Morris, CDC
Steven Steindel, CDC
Glenn Moore, CDC
LCDR Bernetta Lane, USPHS, CDC
Mark Winarsky, CDC
Gilberto Ramirez, CDC
Roniqua Watkins, CDC
Robb Chapman, CDC
Brett Carpenter, Northrop Grumman
Kashmira Date, Northrop Grumman
Daniel Friedman, Northrop Grumman
Mark Jensen, Northrop Grumman
Morgan Lestat-Alexander, Northrop Grumman
Roy Gibson Parrish, Northrop Grumman
Loni Finley, Northrop Grumman

In addition, numerous public health partners provided significant contribution to this effort.

Revision History

Version	Date	Revision Summary
1.0	08/21/2008	PHIN Certification and Process Document - Initial version

Table of Contents

Introduction

Public Health Information Network (PHIN) Certification provides an objective assessment, designed to evaluate the compliance of public health information systems with *PHIN Requirements Version 2.0*[1]. The goal of PHIN Certification is to support the development and implementation of applications and information systems that comply with the PHIN Requirements to help ensure that public health partners can securely, effectively and efficiently exchange data. PHIN Certification is designed to provide meaningful and achievable targets, a consistent method to report capabilities and demonstrate progress. It also offers flexibility to support the evolving nature of PHIN and the Nationwide Health Information Network (NHIN).

The purpose of this document is to define and provide an understanding of PHIN Certification by:

- providing a detailed description of PHIN Certification and the individual PHIN Certifications that will be available
- articulating the certification criteria that will be used to evaluate compliance
- identifying the general steps in the PHIN Certification process

Partners seeking PHIN Certification will use this document, along with the *PHIN Requirements Version 2.0* and other PHIN implementation guides, message guides and specification documents. The scope of PHIN Certification will be limited to electronic information system(s) directly involved in providing the functionality necessary to meet the certification criteria for the specific PHIN certification. Partners may choose to meet the certification requirements by: building or enhancing their own systems, purchasing commercial vendor solutions or using CDC developed systems and services.

[1] The *PHIN Requirements Version 2.0* document is available on the PHIN website (http://www.cdc.gov/phin)

PHIN Certification

Description

PHIN Certification for *PHIN Requirements Version 2.0* will certify the ability of an application (or multiple applications, components or systems) to perform specific functions in compliance with the PHIN Requirements. Individual PHIN Certifications for specific functionality will be defined, including identifying the PHIN Requirements and the associated certification criteria used to evaluate compliance.

Each PHIN Certification is based on one or more of the PHIN Requirements. For example, the PHIN Certification for sending Varicella case notification messages from a partner to the CDC is "**PHIN Varicella Case Notification Message – Send**". The functionality required is: (i) the ability to compose functional Varicella case notification messages; (ii) the ability securely send the messages to the CDC and (iii) the application(s) used must be secure and available. The table below identifies the PHIN Requirements applicable to this certification and the certification evaluation.

Table 1 - Example PHIN Certification

PHIN Certification for: **PHIN Varicella Case Notification Message – Send**	
Applicable PHIN Requirements	#1 – Compose Electronic Message #2 – Securely Send Electronic Message #5 – Security and Availability of Electronic Information Systems
Certification Evaluation	– Assess ability to compose Varicella Case Notification messages using the certification criteria for PHIN Requirement #1 – Assess ability to securely send Varicella Case Notification messages using the certification criteria for PHIN Requirement #2 – Assess the security controls and availability of the application(s), processes and/or platforms used to compose and securely send Varicella Case Notification messages using the certification criteria for Requirement #5.

The certification evaluation will be limited to the application(s) directly involved in performing functions included in the specific PHIN Certification. As part of the certification evaluation, the partner must identify the application(s) utilized to perform the function[2]. In order to be awarded the specific PHIN Certification, the partner's application(s) must successfully meet all of the identified certification criteria.

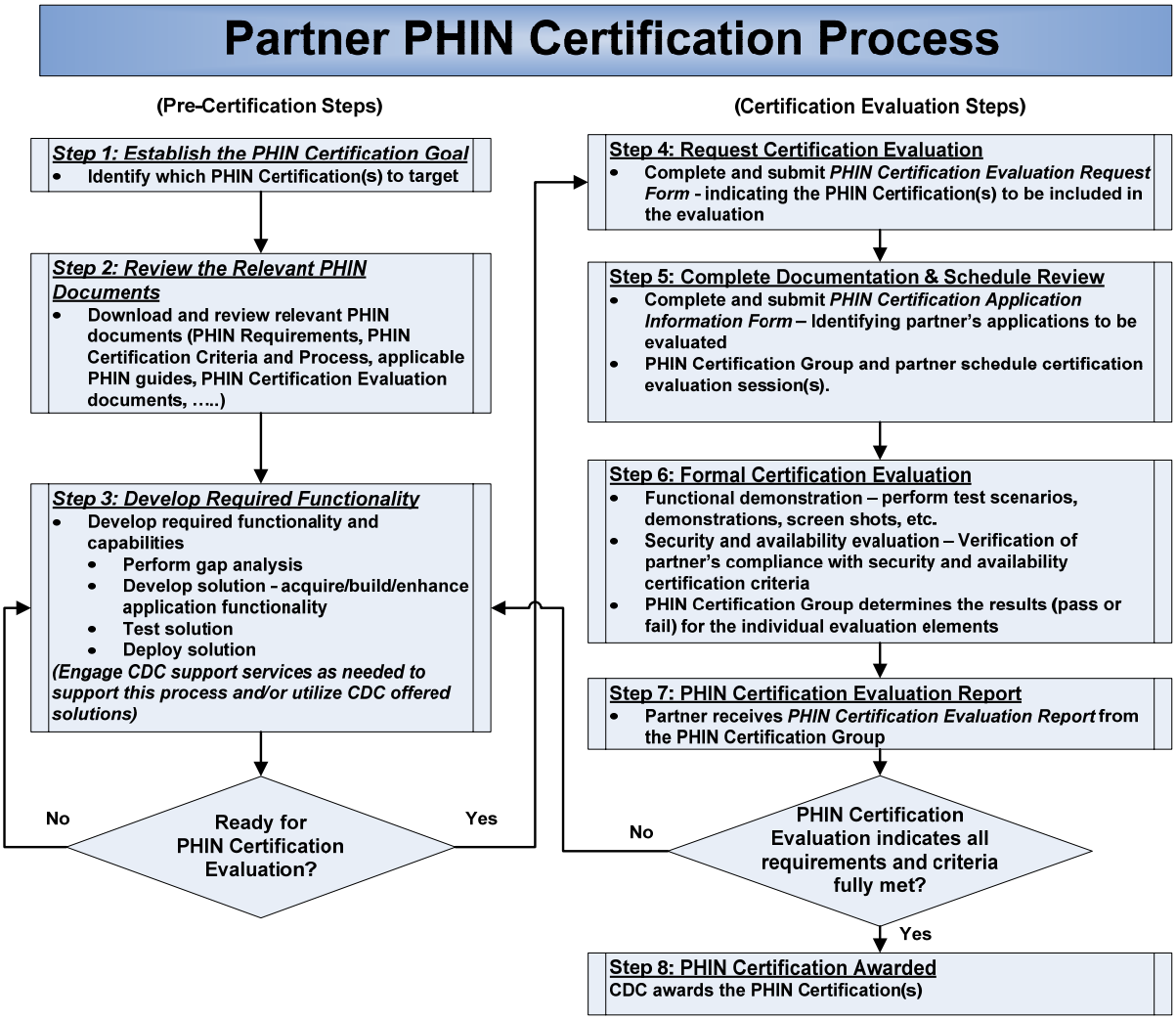
[2] Identifying the application(s) will include providing: the application name, vendor, product, version / build and description of the functionality it provides related to the specific PHIN Certification.

PHIN Certification Process

The PHIN Certification process identifies the steps required for PHIN Certification; the process uses a combination of functionality demonstrations, interoperability testing and documentation submittal and review. CDC will establish the PHIN Certification Group who will perform PHIN certification evaluations. The PHIN Certification Group will develop and provide detailed test scenarios for each PHIN Certification. CDC will develop and provide tools, such as message validation tools, to assist partners in developing the necessary capabilities and functionality.

One or more individual PHIN Certifications could be targeted during the process. The PHIN Certification Group will perform the evaluation to determine if the partner meets the requirements and the certification criteria. CDC will award partners the specific PHIN Certification(s) they successfully achieve. An overview of the general PHIN Certification Process is pictured in **Figure 1**.

Figure 1 – Partner's PHIN Certification Process



PHIN Certification Criteria

This section lists the PHIN Certification Criteria to evaluate partner application(s) and information system(s) for compliance with *PHIN Requirements Version 2.0.* The specific certification criteria for each of the five PHIN Requirements are listed below.

CDC will publish a list of the currently available PHIN Certifications on the PHIN website (http://www.cdc.gov/phin). The list will identify the applicable implementation guides, message guides and message specification documents for each PHIN Certification. These documents provide detailed information to fully define functionality (i.e. secure message transport) or the message specification details including structure, formats and vocabulary. The *PHIN Requirements Version 2.0* document contains the identified standards for each PHIN Requirement.

The term "Application" or "system" in the criteria statements listed below refers to an application, a system or any combination of applications or systems used by partners to fulfill the specified criteria.

Certification Criteria for PHIN Requirement #1

PHIN Requirement #1

PHIN REQUIREMENTS: FUNCTIONS OF ELECTRONIC INFORMATION SYSTEMS	
	CDC requires that each state or local health department—or its agent—
1	be able to compose electronic messages using standard protocols, formats, and terminologies.
1.1	be able to identify, extract, and compile the data elements required for a specified message from existing data sets or documents.
1.2	be able to convert data content stored in non-standard formats or terminologies into standard formats and terminologies that are current.
1.3	be able to construct messages from standardized data content using specified messaging standards.

The certification criteria for PHIN Requirement #1 (Compose electronic messages) are listed below.

1 Is the application able to construct functional electronic messages that comply with the applicable implementation guides, message guides, message specifications, and associated standards for PHIN electronic messages?

1.1 Is the application able to construct a functional message that contains all *required* message segments in the proper order, separated by appropriate and properly located delimiters?

1.2 Is the application able to construct functional message segments that contain all *required* data elements (and any *required* components), properly ordered and separated by appropriate delimiters?

1.3 Is the application able—without error or loss of *required* information—to convert content obtained for *required* data elements from local formats, terminologies, classification schemes, or value domains into PHIN compliant terminologies, classification schemes, and value domains?

1.4 Is the application able to obtain appropriate content for all *required* data elements (i.e., fields) either directly or through electronic interfaces with existing data sources?

Certification Criteria for PHIN Requirement #2

PHIN Requirement #2

PHIN REQUIREMENTS: FUNCTIONS OF ELECTRONIC INFORMATION SYSTEMS	
	CDC requires that each state or local health department—or its agent—
2	be able to securely send to one or more recipients electronic messages composed using standard protocols, formats and terminologies.
2.1	uniquely identify the sending and receiving parties within the message.
2.2	verify that the receiving systems and parties are trusted.
2.3	be able to request a message acknowledgement
2.4	be able to respond to a notification from a recipient that an error was encountered during the processing or interpreting of a message.

The certification criteria for PHIN Requirement #2 (Securely send electronic messages) are listed below.

2 Is the application able to send functional electronic messages that comply with the applicable implementation guides, message guides, message specifications, and associated standards?

2.1 If necessary, is the application sending electronic messages able to interface with, and without error transfer the message from, an application that composes the message?

2.2 Is the application sending electronic messages able to uniquely identify the sending and receiving parties within the message?

2.3 Is the application sending electronic messages able to address the message and verify that the receiving parties exist and are trusted using an appropriate means of authentication?

2.4 Is the application sending electronic messages able to request acknowledgment that the message was received by the appropriate receiving parties in compliance with the implementation guides and standards?

2.5 Is the application sending electronic messages able to respond to a message from a recipient that an error was encountered when processing a message?

Certification Criteria for PHIN Requirement #3

PHIN Requirement #3

PHIN REQUIREMENTS: FUNCTIONS OF ELECTRONIC INFORMATION SYSTEMS	
	CDC requires that each state or local health department—or its agent—
3	be able to securely receive, process, and interpret electronic messages sent using standard protocols, formats, and terminologies.
3.1	verify that the sending systems and parties are trusted.
3.2	be able to process and interpret received messages and, as appropriate, store their content in locally maintained datasets.
3.3	be able to send acknowledgement of message receipt when requested.
3.4	be able to send a notification indicating that an error was encountered during the processing or interpreting of a message.

The certification criteria for PHIN Requirement #3 (Securely receiving, parsing and processing electronic messages) are listed below.

3 Is the application able to receive and process functional electronic messages that comply with applicable implementation guides, message guides, message specifications, and associated standards for PHIN electronic messages?

- 3.1 Is the application receiving electronic messages able to identify the sending party within the message and verify that the sending party exists and is trusted using an appropriate means of authentication?
- 3.2 Is the application receiving electronic messages able to send acknowledgement of message receipt when requested?
- 3.3 If necessary, is the application receiving electronic messages able to interface with, and without error transfer the message to, an application that processes the message?
- 3.4 For each type of message, is the application processing electronic messages able—without error or loss of *required* information—to map and convert all *required* data elements from PHIN compliant terminologies, classification schemes, and value domains to any local terminologies, classifications schemes, and value domains that may be used for these data elements?
- 3.5 Is the application processing electronic messages able to send a message indicating that an error was encountered when processing a message?

Certification Criteria for PHIN Requirement #4

PHIN Requirement #4

PHIN REQUIREMENTS: FUNCTIONS OF ELECTRONIC INFORMATION SYSTEMS	
	CDC requires that each state or local health department—or its agent—
4	be able to electronically enter, edit, and retrieve identifying and other information about persons, organizations, or other entities from an electronic directory that adheres to standard directory protocols, formats, and terminologies, and to which the department has authorized access.

The certification criteria for PHIN Requirement #4 (Public Health Directory) are listed below.

4 Does the directory system provide the ability to maintain a secure repository of information about persons, organizations, and other entities involved in public health activities?

- 4.1 Does the directory system provide the ability to maintain information on people that includes names, contact information, roles, jurisdictions, organizational affiliation, and communication devices?
- 4.2 Does the directory system have an interface through which to provide information to other applications that require directory information?
- 4.3 Does the directory system require and use a unique identifier for each person, organization and other entity stored in the directory?
- 4.4 Does the directory system provide for retrieval of person information based on name, public health role, organizational affiliation, geographical location, and/or jurisdiction?
- 4.5 Is the directory system able to exchange directory information with other electronic directories using the electronic message format and transport protocol specified in applicable implementation guide?

Certification Criteria for PHIN Requirement #5

PHIN Requirement #5

PHIN REQUIREMENTS: FUNCTIONS OF ELECTRONIC INFORMATION SYSTEMS	
	CDC requires that each state or local health department—or its agent—
5	ensure that its electronic information systems that support PHIN requirements are secure and have the appropriate level of availability and the information contained is only accessed or used by authorized users for authorized purposes.
5.1	have an Internet connection available to support data exchange and PHIN interoperability initiatives.
5.2	implement administrative and physical safeguards that conform to current standards to prevent unauthorized access to, and use of, its information systems.
5.3	identify persons and other electronic information systems authorized to access its electronic information systems.
5.4	provide system access to authorized senders that conforms to current standards for securely exchanging messages and data.
5.5	maintain a record of all persons and electronic devices that access its electronic information systems and the actions taken during such access.

The certification criteria for PHIN Requirement #5 (Security and availability of electronic information systems supporting the PHIN Requirements) are listed below. The certification criteria that pertain to security of public health information and electronic information systems are derived and adapted from the standards developed by the National Institute of Standards and Technology (NIST) and published in NIST Special Publication 800-53 Revision 1 "Recommended Security Controls for Federal Information Systems December 2006"[3].

[3] Available at http://csrc.nist.gov/publications/nistpubs/index.html

Availability of information systems

5.1 Is an Internet connection available for components of the information system(s) that require Internet access?

5.2 Do the components of the information system(s) that support the PHIN requirements have the appropriate level of availability?

Security of information and information systems

5.3 Are the electronic information systems that support PHIN requirements secure, and have the appropriate auditing and safeguards to prevent unauthorized access and use?

[Access Control]

5.3.1 Does the organization (i) manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts, (ii) review information systems accounts at an organization-defined frequency, and (iii) perform risk analysis of access controls? *[Source: NIST 800-53 AC-2, RA-3]*

5.3.2 Does the organization employ access control policies (e.g., identity-based policies, role-based policies, ruled-based policies) and associated access enforcement mechanisms (e.g., access control lists, access control matrices, cryptography) to control access between users (or processes acting on behalf of users) and objects (e.g., devices, files, records, processes, programs, domains) in the information system? *[Source: NIST 800-53 AC-3]*

5.3.3 Does the information system enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks? *[Source: NIST 800-53 AC-6]*

5.3.4 Does the information system enforce a limit to the number of consecutive invalid access attempts by a user (or processes acting on behalf of the user) during a defined time period? *[Source: NIST 800-53 AC-7]*

5.3.5 Does the information system display an approved, system use notification message, warning of unauthorized use and appropriate privacy and security notices, before granting system access? *[Source: NIST 800-53 AC-8]*

5.3.6 Does the organization authorize, document, monitor, and control all methods of access to the information system, including remote and system to system access? *[Source: NIST 800-53 AC-4, AC-17, CA-3]*

[Awareness and Training]

5.3.7 Does the organization provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, if required by system changes, and at an organization defined frequency (at least annually) thereafter? *[Source: NIST 800-53 AT-2]*

[Audit and Accountability]

5.3.8 Does the organization define and periodically review and update the list of auditable events and generate audit records for those events? *[Source: NIST 800-53 AU-2]*

5.3.9 Does the information system capture sufficient information, including time stamps, in audit records to establish what events occurred, the sources of the events, and the outcomes of the events? *[Source: NIST 800-53 AU-3, AU-8]*

5.3.10 Does the organization regularly review/analyze audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions? *[Source: NIST 800-53 AU-6]*

5.3.11 Are automated mechanisms employed to immediately alert security personnel of inappropriate or unusual activities? *[Source: NIST 800-53 AU-6]*

5.3.12 Does the information system protect audit information and audit tools from unauthorized access, modification, and deletion? *[Source: NIST 800-53 AU-9]*

5.3.13 Does the organization retain audit logs for a defined period of time to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements? *[Source: NIST 800-53 AC-11]*

[Certification, Accreditation, and Security Assessments]

5.3.14 Does the organization conduct an assessment of the security controls in the information system at least annually, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system? *[Source: NIST 800-53 CA-2]*

5.3.15 Does the organization develop and update a plan of actions and milestones for the information system that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system? *[Source: NIST 800-53 CA-5]*

5.3.16 Does the organization monitor the security controls in the information system on an ongoing basis? *[Source: NIST 800-53 CA-7]*

[Configuration Management]

5.3.17 Does the organization develop, document, and maintain a current, baseline configuration of the information system and an inventory of the system's constituent components? *[Source: NIST 800-53 CM-2]*

5.3.18 Does the organization manage and monitor changes to the information system and conduct security impact analyses to determine the effects of the changes? *[Source: NIST 800-53 CM-4]*

5.3.19 Does the organization configure the security settings of information technology products to the most restrictive mode consistent with information system operational requirements? *[Source: NIST 800-53 CM-6]*

5.3.20 Does the organization configure the information system to provide only essential capabilities and specifically prohibit and/or restrict the use of unnecessary or insecure functions, ports, protocols and/or services? *[Source: NIST 800-53 CM-7]*

5.3.21 Does the organization develop, document, and maintain a current inventory of the components of the information system and relevant ownership information? *[Source: NIST 800-53 CM-8]*

[Contingency Planning][4]

5.3.22 Does the organization develop and implement a contingency plan for the information system addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure? *[Source: NIST 800-53 CP-2]*

5.3.23 Do designated officials within the organization review and approve the contingency plan and distribute copies of the plan to key contingency personnel? *[Source: NIST 800-53 CP-2]*

5.3.24 Does the organization test the contingency plan for the information system at least annually to determine the plan's effectiveness and the organization's readiness to execute the plan? *[Source: NIST 800-53 CP-4]*

5.3.25 Do appropriate officials within the organization review the contingency plan test results and initiate corrective actions? *[Source: NIST 800-53 CP-4]*

5.3.26 Does the organization review the contingency plan for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing? *[Source: NIST 800-53 CP-5]*

5.3.27 Does the organization conduct backups of user-level and system-level information (including system state information) contained in the information system, perform test to ensure the reliability and integrity of the backups and stores backup information at an appropriately secured location? *[Source: NIST 800-53 CP-9]*

5.3.28 Does the organization employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to the system's original state after a disruption or failure? *[Source: NIST 800-53 CP-10]*

[Identification and Authentication]

5.3.29 Does the information system uniquely identify and authenticate users (or processes acting on behalf of users)? *[Source: NIST 800-53 IA-2]*

5.3.30 Does the organization manage user identifiers by: (i) uniquely identifying each user; (ii) verifying the identity of each user; (iii) receiving authorization to issue a user

[4] Aspects of Continuity of Operations Plans may be relevant and used to meet these criteria

identifier from an appropriate organization official; (iv) ensuring that the user identifier is issued to the intended party; (v) disabling inactive user identifier; and (vi) archiving user identifiers? *[Source: NIST 800-53 IA-4]*

5.3.31 Does the organization manage information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: (i) defining initial authenticator content; (ii) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and (iii) changing default authenticators upon information system installation; and (iv) changing/refreshing authenticators periodically? *[Source: NIST 800-53 IA-5]*

5.3.32 Does the information system provide feedback to a user during an attempted authentication and that the feedback does not compromise the authentication mechanism (e.g. the system does not display passwords while being entered)? *[Source: NIST 800-53 IA-6]*

[Incident Response]

5.3.33 Does the organization implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery? *[Source: NIST 800-53 IR-4]*

5.3.34 Does the organization track and document information system security incidents on an ongoing basis? *[Source: NIST 800-53 IR-5]*

[Maintenance]

5.3.35 Does the organization schedule, perform, and document routine preventative and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organizational requirements? *[Source: NIST 800-53 MA-2]*

5.3.36 Does the organization obtain maintenance support and spare parts for key information system components in the event of a failure within a time period that supports the targeted level of availability? *[Source: NIST 800-53 MA-6]*

[Media Protection]

5.3.37 Does the organization (i) protect information system media, both digital and non-digital and, (ii) limit access to information on information system media to authorized users? *[Source: NIST 800-53 MP-2, MP-4]*

[Physical and Environmental Protection]

5.3.38 Does the organization develop and keep current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issue appropriate authorization credentials (e.g., badges, identification cards, smart cards)? *[Source: NIST 800-53 PE-2]*

5.3.39 Do designated officials within the organization review and approve the access list and authorization credentials at least annually? *[Source: NIST 800-53 PE-2]*

5.3.40 Does the organization control all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verify individual access authorizations before granting access to the facilities? *[Source: NIST 800-53 PE-3]*

5.3.41 Does the organization also control access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk? *[Source: NIST 800-53 PE-3]*

5.3.42 Does the organization control physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible and escorts visitors and monitors visitor activity, when required? *[Source: NIST 800-53 PE-7]*

[Planning]

5.3.43 Does the organization develop, implement and maintain a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements and do designated officials within the organization review and approve the plan? *[Source: NIST 800-53 PL-2]*

[Personnel Security]

5.3.44 Does the organization complete appropriate access agreements (e.g., nondisclosure agreements, acceptable use agreements, rules of behavior, conflict-of-interest agreements) for individuals requiring access to organizational information and information systems before authorizing access? *[Source: NIST 800-53 PS-6]*

[Risk Assessment]

5.3.45 Does the organization categorize the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan and do designated senior-level officials within the organization review and approve the security categorizations? *[Source: NIST 800-53 RA-2]*

5.3.46 Does the organization conduct assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency? *[Source: NIST 800-53 RA-3]*

5.3.47 Does the organization update the risk assessment periodically or whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system? *[Source: NIST 800-53 RA-4]*

5.3.48 Does the organization use appropriate vulnerability scanning tools and techniques to scan for vulnerabilities in the information system periodically or when significant new vulnerabilities affecting the system are identified and reported? *[Source: NIST 800-53 RA-5]*

[System and Communications Protection]

5.3.49 Does the information system protect against or limit the effects of denial of service attacks? *[Source: NIST 800-53 SC-5]*

5.3.50 Does the information system monitor and control communications at the external boundary of the information system and at key internal boundaries within the system? *[Source: NIST 800-53 SC-7]*

5.3.51 Does the organization physically allocate publicly accessible information system components to separate subnetworks with separate, physical network interfaces (Publicly accessible information system components include, for example, public web servers)? *[Source: NIST 800-53 SC-7]*

5.3.52 Does the organization prevent public access into the organization's internal networks except as appropriately mediated? *[Source: NIST 800-53 SC-7]*

5.3.53 Does the information system protect the confidentiality of transmitted information? *[Source: NIST 800-53 SC-9]*

5.3.54 If cryptography is employed within the information system, does the system perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation? *[Source: NIST 800-53 SC-13]*

5.3.55 Does the information system provide mechanisms to protect the authenticity of communications sessions? *[Source: NIST 800-53 SC-23]*

[System and Information Integrity]

5.3.56 Does the organization identify, report, and correct information system flaws? *[Source: NIST 800-53 SI-2]*

5.3.57 Does the information system implement malicious code protection (e.g. virus protection software) that includes a capability for automatic updates? *[Source: NIST 800-53 SI-3]*

5.3.58 Does the organization employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorized use of the system and monitor outbound communications for unusual or unauthorized activities indicating the presence of malware (e.g. malicious code, spyware, adware)? *[Source: NIST 800-53 SI-4]*

Certification Target Date

CDC will establish certification priorities by setting the target date for partners to obtain each PHIN certification. CDC will update certification target dates as required to maintain alignment with public health priorities and initiatives. CDC will collaborate with partners to establish or update certification target dates.

New Certifications and Change Control

The change control process supports the introduction of new certifications and provides the ability for managing modifications to existing documents that potentially impact current PHIN Certifications.

The PHIN Certification version is associated to specific PHIN documents. When there are substantive changes to these documents, CDC will assign a new version number for the specific PHIN Certification and assign an appropriate certification target date. This new version will have a ***current*** status and the original version will be assigned a ***prior*** status.

When CDC creates a new version, partners who were awarded certification for the prior version, must undergo the certification process for the new version by the established target date.

The example below describes how the version and status attributes would be updated to assign a new certification version due to a Varicella case notification message guide change. This example establishes the new PHIN Certification target date as 12/31/09.

(Original)

PHIN Certification	PHIN Cert. Version	Status	Cert. Target Date
PHIN Varicella Case Notification Message – Send	1	current	08/09/09

(After implementation guide update forces new version)

PHIN Certification	PHIN Cert. Version	Status	Cert. Target Date
PHIN Varicella Case Notification Message – Send	2	current	12/31/09
PHIN Varicella Case Notification Message – Send	1	prior	-

Certification Expiration and Renewal

PHIN Certifications expire two years from the date issued. Partners must renew each certification prior to its expiration. Certifications expire to ensure ongoing compliance with the PHIN Requirements.

Listing of PHIN Certifications and Details

CDC will publish a list of the currently available PHIN Certifications on the PHIN website (http://www.cdc.gov/phin). The list includes the specific PHIN Certification name, version, status, applicable PHIN Requirements and Certification criteria, applicable PHIN guides and certification target dates for each PHIN Certification. An example of how the listing of PHIN Certifications[5] and details may be displayed on the PHIN website is included in ***Appendix A***.

[5] The most updated listing of available PHIN Certifications will be maintained on the PHIN website (http://www.cdc.gov/phin)

Appendices

Appendix A: Example of Listing of PHIN Certifications

CDC will publish a list of the currently available PHIN Certifications on the PHIN website (http://www.cdc.gov/phin). The following examples show how the listing of PHIN Certifications and a detailed listing for a specific PHIN Certification may be displayed the PHIN website.

Example 1: Listing of the PHIN Certifications

Listing of PHIN Certifications			
PHIN Certification *(click on the link for the complete details including: applicable PHIN Requirements, Certification Criteria, specifications and guides)*	**Version**	**Status**	**Target Date**
PHIN Varicella Case Notification Message – Send	1	Current	08/09/2009
PHIN TB Case Notification Message – Send	1	Current	08/09/2009
PHIN Direct Alerting	1	Current	08/09/2009
PHIN Cascade Alerting	1	Current	08/092010

Example 2: Detailed listing for "PHIN Varicella Case Notification Message – Send"

Details for: PHIN Varicella Case Notification Message - Send
Certification Attributes:
Version: 1 Status: Current Target Date: 08/09/2009
PHIN Requirements and PHIN Certification Documents
PHIN Requirements v2.0 PHIN Certification Criteria and Process v1.0
The applicable PHIN Requirements and associated Certification Criteria (Only the checked ones apply)
PHIN Requirement #1 (Compose Messages) PHIN Requirement #2 (Securely Send Messages) PHIN Requirement #5 (Security and Availability of Electronic Information Systems) (Note: PHIN Requirements #3 & #4 do not apply to this certification)
Applicable Implementation and Specification Guides
Message Structure Specification for National Condition Reporting Version 1.0, 08/18/2007 Message Structure Specification for National Condition Reporting Errata and Clarifications, 05/23/2008 Varicella Notification Message Mapping Guide Version 1.0, 08/17/2007 Varicella Case Notification MMG Errata and Clarifications, 05/23/2008 PHIN Secure Message Transport Guide, Version 1.0, 5/30/2007
Evaluation and Test Scenarios
PHIN Certification Evaluation for PHIN Varicella Case Notification – Send

Appendix B: Example of PHIN Certification

An example of the process details for PHIN Certification for PHIN Varicella Case Notification Message – Send is provided below.

PHIN Certification	PHIN Varicella Case Notification Message - Send
Version	1
Status	Current
Certification Target Date	08/30/2008
Documents	*PHIN Requirements* • PHIN Requirements Version 2.0 Available at http://www.cdc.gov/phin/resources/requirements.html *PHIN Certification Criteria and Process* • PHIN Certification Criteria and Process Version 1.0 Available at http://www.cdc.gov/phin/resources/certification.html *Implementation Guide(s)* • Message Structure Specification for National Condition Reporting Version 1.0 August 18, 2007 (Including Errata and Clarifications) Available at: http://www.cdc.gov/phin/resources/guides.html • Varicella Notification Message Mapping Guide Version 1.0 08/17/2007 (Including Errata and Clarifications) Available at: http://www.cdc.gov/phin/resources/guides.html • PHIN Secure Message Transport Guide, Version 2.0, 7/31/2008 Available at http://www.cdc.gov/phin/resources/guides.html
Applicable PHIN Requirements and Certification Criteria	#1 (Compose Message) #2 (Securely Send Message) #5 (Security and Availability of Electronic Information Systems)

Certification Evaluation Process	**Request Certification Evaluation** Partner Submits *PHIN Certification Evaluation Request Form*[6] requesting PHIN Certification evaluation for "PHIN Varicella Case Notification Message – Send" **Complete and Submit Requested Documentation** Partner submits documentation requested by the PHIN Certification Group • Completed *PHIN Certification Application Information Form*[7] **Certification Evaluation** Part #1: PHIN security and availability evaluation – Partner will complete form(s) provided by the PHIN Certification Group to verify the partner's compliance with the security and availability certification criteria. Part #2: Partner demonstrates the ability to successfully perform the specific test scenarios for the "Varicella Case Notification Message – Send" certification • Compose and use secure message transport to send the test Varicella messages to the CDC o Using test data files for notifications (Test notification activation messages) o Using test data file(s) for update(s) (Test notification update message) o Using test data file(s) for deletion(s) (Test notification deletion message) *(Note: Parts 1 and 2 of the certification evaluation may be separate sessions)* **Certification Evaluation Report** The PHIN Certification Group will provide the partner with a formal PHIN Certification Evaluation Report with the results of the evaluation, including: 1) the determination on whether the partner fully met all of the requirement for certification 2) identifying and providing specific details for any deficiencies or non-compliance items found

[6] *PHIN Certification Evaluation Request Form* will be available on the PHIN website.
[7] *PHIN Certification Application Information Form* will be available on the PHIN website. Application details would include: vendor, product name, version, etc.

Appendix C: Glossary

access

Definition: "obtain, examine, or retrieve (data or a file)" (*Source*: OAD)

appropriate level of availability

Definition: systems that are able to be used within a suitable timeframe based on the criticality of the services or programs supported by the system

Example or Comment: A public health jurisdiction would consider the system availability requirements to support emergency response, as well as, other national, state, local or program level requirements and priorities to determine the appropriate level of availability to target for its electronic information systems. For example, systems supporting critical functions, like emergency response, might require an availability level of 7x24x365, while systems supporting routine functionality might require an availability level of 8-5 M-F.

auditable events

Definition: any occurrences that may affect or change the security state of the system

Example or Comment: Auditable events might include any attempted or actual violation of the system access control or accountability security policies, or both. As this relates to the NIST 800-53 controls for *Audit and Accountability*, auditable events are important events which need to be audited as significant and relevant to the security of the information system. The organization defines auditable events that are adequate to support after-the-fact investigations of security incidents.

authenticate user

Definition: the process of verifying with some established degree of confidence the identity of a user, often as a prerequisite to allowing access to resources in an information system (*Source:* NIST 800-53)

Example or Comment: The process typically will involve unique identifiers assigned to users (e.g. logins, accounts, etc.) and authenticators (e.g. tokens, passwords, certifications, etc.) for the unique identifiers.

classification scheme

Definition: is the descriptive information for an arrangement or division of objects into groups based on characteristics which the objects have in common

configuration management

Definition: the process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation. (*Source:* NIST 800-53)

contingency plan

Definition: An alternative plan to be put into operation in needed, especially in case of emergencies, or if a primary plan fails *(Source:* Wiktionary*)*

data elements

Definition: "a unit of data for which the definition, identification, representation and permissible values are specified by means of a set of attributes" (*Source*: ISO 11179)

directory system

Definition: a system, or multiple systems acting in common, that provides structured information about people, organizations, and resources important or of interest to an organization, used to facilitate management and communication

format

Definition: "a defined structure for the processing, storage, or display of data" (*Source*: OAD)

incident

Definition: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies (*Source*: NIST 800-53)

information system

Definition: "a system, whether automated or manual, that comprises people, machines, or methods organized to collect, process, transmit, and disseminate data" (*Source*: Wikipedia)

malicious code / malware

Definition: software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system (*Source*: NIST 800-53)

Example or Comment: A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

risk assessment

Definition: the process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals arising through the operation of the information system (*Source*: NIST 800-53)

Example or Comment: Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses, and considers mitigations provided by planned or in place security controls.

secure messaging

Definition: a process to exchange electronic messages that is free from the risk of eavesdropping, interception or discovery

Example or Comment: PHIN uses a standards-based approach for secure, reliable, bi-directional message transport across the Internet.

security controls

Definition: the management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information (*Source:* NIST 800-53)

spyware

Definition: software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code (*Source:* NIST 800-53)

substantive changes

Definition: changes that are substantial, considerable, important, have substantial consequence or modify required functionality

Example or Comment: Examples of substantive changes would include, but not be limited to: the addition of required data element(s), modification to the acceptable coding of data element or the addition of certification criteria.

transport protocol

Definition: "a set of rules governing the exchange or transmission of data electronically between devices" (*Source*: OAD)

Example or Comment: The hypertext transfer protocol (http) is a set of rules for transferring data on the World Wide Web.

unauthorized access

Definition: obtaining, examining, or retrieving (data or a file) from an (electronic) information system without official permission or approval

uniquely identify

Definition: a means of designating an entity so that it can be distinguished from all other entities of its own type or of different types

Example or Comment: Object identifiers (OID) provide a system for uniquely identifying entities. Social security numbers are sometimes used to uniquely identify persons in the United States, although there limitations to their use for this purpose.

value domain

Definition: a set of permissible values for a data element

vulnerability

Definition: weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source (*Source:* NIST 800-53)

REFERENCES:

- ISO 11179. International Organization for Standardization. Metadata registries, second edition. Part 1: Framework. Geneva: International Organization for Standardization; 2004. Available from: http://metadata-standards.org/11179.
- NIST 800-53. National Institute of Standards and Technology, Recommended Security Controls for Federal Information Systems. NIST Special Publication 800-53 Revision 1, December 2006. Available from: http://csrc.nist.gov/publications/nistpubs/index.html
- OAD. New Oxford American Dictionary, Second Edition, Erin McKean (Editor), New York: Oxford University Press, May 2005.
- Wikipedia: the free encyclopedia. Available from: http://en.wikipedia.org/wiki/Main_Page.
- Wiktionary: a wiki-based open content dictionary. Available from: http://en.wiktionary.org/wiki/Main_Page.