

PHIN Certification Evaluation

This document includes the PHIN Certification details, specific notes for applicants and the evaluation steps and test scenarios for the PHIN Certification listed below. The evaluation steps and test scenarios detailed in this document are designed to test compliance with specific PHIN Certification Criteria. The PHIN Certification Group will evaluate the applicant's performance against the expected results. The applicant must successfully complete all of the steps in order to receive this PHIN Certification.

PHIN Certification: Direct Alerting

Certification Details

Certification Attributes:

Version: 1 Status: Current Target Date: 08/09/2009

PHIN Requirements and PHIN Certification Documents

- PHIN Requirements Version 2.0, 06/22/2007; Available at: <http://www.cdc.gov/phn/resources/requirements.html>
- PHIN Certification Criteria and Process Version 1.0, 08/21/2008; Available at: <http://www.cdc.gov/phn/resources/certification/index.html>

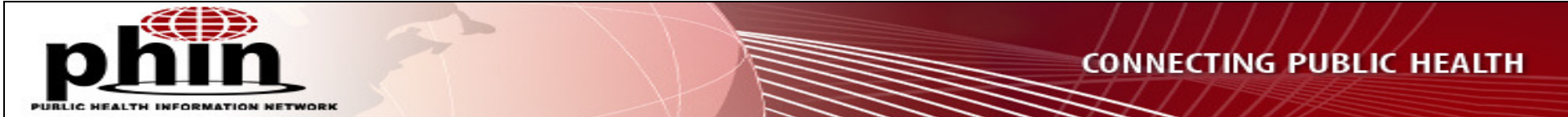
The applicable PHIN Requirements and associated Certification Criteria

- 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 and #4 do not apply to this PHIN Certification)

Applicable Implementation and Specification Guides

- PHIN Communication and Alerting (PCA) Guide, Version 1.1, 03/17/2009; Available at: <http://www.cdc.gov/phn/resources/guides.html>



Notes to applicants:

- The evaluation steps and test scenarios detailed in this document are designed to test compliance with specific PHIN Certification Criteria.
- The direct alerts composed by the applicant will be validated for compliance with the PHIN Communications and Alerting Guide
 - The alerts must have or convey the required data attributes and follow the vocabulary specified in the guide

Certification Evaluation:

The PHIN Certification evaluation for **Direct Alerting** includes two parts:

Part #1: Security and Availability Evaluation

Part #2: Alerting Demonstration

Part #1 Security and Availability Evaluation

Preparation for Applicant:

- Download and use the *PHIN Security and Availability Assessment Tool* (Available at: <http://www.cdc.gov/phn/resources/certification/index.html>) to assist with self-evaluating compliance with the PHIN Certification Criteria for PHIN Requirement #5.
- Download the *PHIN Certification Security and Availability Self-Attestation Form* (Available at: <http://www.cdc.gov/phn/resources/certification/index.html>) and identify the appropriate individual to sign the form.

Process steps:

The security and availability evaluation is a self-assessment performed by the applicant. A designated individual for the applicant signs the *PHIN Certification Security and Availability Self-Attestation Form* to verify the self-assessment determined compliance with the PHIN Certification Criteria for PHIN Requirement #5.

| Step ID | Evaluation Steps | Expected Result | Pass / Fail | Certification Criteria Reference | Actual Result / Detailed Description of Failure (Required if score is “Fail”) |
|---------|--|--|-------------|-------------------------------------|---|
| 1.1 | Applicant completes the <i>PHIN Certification Security and Availability Self-Attestation Form</i> and submits to the PHIN Certification Group. | The applicant has completed a self-assessment and returns the signed self-attestation form to indicate compliance with the security and availability certification criteria. | | CC #: 5.1, 5.2, 5.3, 5.3.1 – 5.3.58 | |

Part #2 – Alerting Demonstration

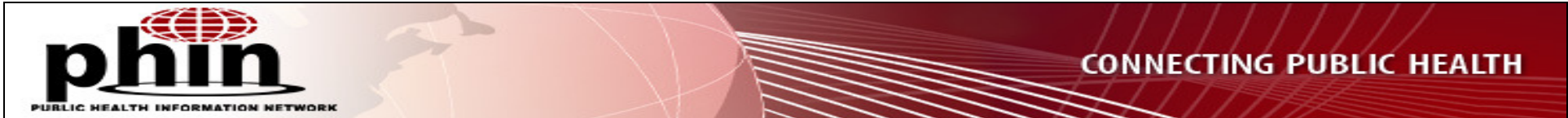
Partner Preparation:

1. PHIN Certification Group will send the partner the test data file sends partner test data file(s) a minimum of 2 business days prior to certification evaluation date.
2. PHIN Certification Group will provide the partner instructions for sending or delivering the alerts to the PHIN Certification Group (PCG) via a method approved by the PCG.

| Step ID | Evaluation Steps | Expected Result | Pass / Fail | Certification Criteria Reference | Actual Result / Detailed Description of Failure (Required if score is “Fail”) |
|---------|--|--|-------------|----------------------------------|---|
| 2.1 | Compose direct alert using the data supplied in test case #1 to demonstrate the ability to compose standard test alert of “Moderate” severity. Partner will send the generated alert to the PCG. | The received alert will contain valid vocabulary values and all the required attributes including: <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Severity = “Moderate” ○ Status = “Test” ○ Title ○ Message | | CC #1, 1.1, 1.2, 1.3, 1.4 | |
| 2.2 | Compose direct alert using the data supplied in test case #2 to demonstrate the ability to compose standard test alert of “Severe” severity. Partner will send the generated alert to the PCG. | The received alert will contain valid vocabulary values and all the required attributes including: <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Severity = “Severe” ○ Status = “Test” ○ Title ○ Message | | CC #1, 1.1, 1.2, 1.3, 1.4 | |

| Step ID | Evaluation Steps | Expected Result | Pass / Fail | Certification Criteria Reference | Actual Result / Detailed Description of Failure (Required if score is "Fail") |
|---------|---|---|-------------|--|---|
| 2.3 | Compose direct alert using the data supplied in test case #3 to demonstrate the ability to compose sensitive test alert of "Extreme" severity. Partner will send the generated alert to the PCG. | <p>The received alert will contain valid vocabulary values and all the required attributes including:</p> <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Severity = "Extreme" ○ Sensitive = "Sensitive" ○ Status = "Test" ○ Title ○ Message <p>The message should direct recipient to a secure means to obtain the message, rather than contain the content provided in the test data. Unless the partner has secure means of delivery.</p> | | CC #1, 1.1, 1.2, 1.3, 1.4, 2.1, 2.2, 2.3 | |
| 2.4 | Compose direct alert using the data supplied in test case #4 to demonstrate the ability to compose standard test alert of "Moderate" severity and requesting an acknowledgement from recipient. Partner will send the generated alert to the PCG. | <p>The received alert will contain valid vocabulary values and all the required attributes including:</p> <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Severity = "Moderate" ○ Acknowledgement = "Yes" ○ Status = "Test" ○ Title ○ Message | | CC #1, 1.1, 1.2, 1.3, 1.4, 2.4 | |

| Step ID | Evaluation Steps | Expected Result | Pass / Fail | Certification Criteria Reference | Actual Result / Detailed Description of Failure (Required if score is "Fail") |
|---------|---|---|-------------|----------------------------------|---|
| 2.5 | Compose a direct alert to update the direct alert composed in test scenario step 2.1. Update should change the Severity from "Moderate" to "Minor". | The received alert will contain valid vocabulary values and all the required attributes including: <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Severity = "Minor" ○ Status = "Test" ○ MsgType = "Update" ○ Reference = (alert identifier msg composed in test scenario 2.1) ○ Title ○ Message | | CC #1, 1.1, 1.2, 1.3, 1.4 | |
| 2.6 | Compose a direct alert to cancel the direct alert composed in test scenario step 2.1. | The received alert will contain valid vocabulary values and all the required attributes including: <ul style="list-style-type: none"> ○ Agency name ○ Alert identifier ○ Send time / date ○ Status = "Test" ○ MsgType = "Cancel" ○ Reference = (alert identifier msg composed in test scenario 2.1) ○ Title ○ Message | | CC #1, 1.1, 1.2, 1.3, 1.4 | |



For PHIN Certification Group Use:

| | |
|--|--|
| Applicant: | |
| Evaluation Date(s): | |
| Evaluation Result (Pass/ Fail): | |
| Evaluator: | |
| Evaluator Notes / Comments: | |