Request for Proposal for Health Information Service Provider (HISP) Services

Provided by:
Wisconsin Statewide Health Information Network (WISHIN)
And
National Institute for Medical Informatics (NIMI)

May 31, 2011

TABLE OF CONTENTS:

1 General Information

1.1 Introduction

In December 2010, the US Department of Health and Human Services Office of National Coordinator (ONC) for Health Information Technology (HIT) approved Wisconsin's strategic and operational plan titled "WIRED for Health". WIRED for Health was developed to promote and improve the health of individuals and communities in Wisconsin through the development of health information exchange (HIE)—electronic sharing of the right health information at the right place and right time.

The WIRED for Health plan recognizes the important role electronic health information exchange plays in enabling transformation in the health care delivery system and health care reform in Wisconsin.

Adopting and using health information technology and sharing health information electronically are essential building blocks for this transformation. To achieve this transformation, the WIRED for Health plan describes several evolutionary steps in building a statewide health information network (SHIN). The SHIN will facilitate the exchange of health information within Wisconsin and establish connectivity for border state exchange initiatives as well as Nationwide Health Information Network (NwHIN). It will leverage existing technology assets throughout the state and will take into account Wisconsin's unique health care environment. The SHIN will be available to all HIPAA providers and will cover the entire state, including rural areas.

1.2 Background

In 2010, Governor Doyle signed Wisconsin Act 274, authorizing the State to select a qualified nonprofit corporation to serve as the State Designated Entity (SDE) to govern statewide health information exchange. Following a competitive application process, the WIRED for Health Board recommended Wisconsin Statewide Health Information Network (WISHIN) for designation as the state-level HIE governing body to the Secretary of the Wisconsin Department of Health Services. WISHIN is a non-profit organization founded by the Wisconsin Hospital Association, the Wisconsin Health Information Organization, the Wisconsin Collaborative for Health Care Quality and the Wisconsin Medical Society. On October 25, 2010, the State officially announced its intention to designate WISHIN as the state-level governing organization to assume the responsibilities of the current WIRED for Health Board, as well as the programmatic responsibilities of the State HIE Cooperative Agreement Program.

WISHIN has assumed leadership for this initiative and is overseeing implementation of the WIRED for Health plan for a statewide health information network and services. The plan requires multi-stakeholder collaboration and emphasizes ongoing development of governance and policy structures. The WISHIN Board has broad and balanced public and private stakeholder representation, including Medicaid, public health, hospitals, providers, commercial payers, employers, and consumers.

This Phase 1 project, implementing a Health Information Service Provider to provide Direct Secure Messaging for Wisconsin providers, is a foundational step. These HISP services will provide for sending and receipt of Direct Secure Messages through enabled Electronic Health Record systems, secure e-mail enabled clients and a web portal. In addition to serving as a conduit for exchanging Continuity of Care Documents (CCD), the HISP will provide services to

deliver laboratory test results from reference labs to providers and for providers to send prescriptions to local pharmacies enabled with Direct.

HISP services are a foundational step for state wide health information network, with subsequent application to include providing a conduit for connecting the various health information exchanges operating in the state. To assist in setting a context, in Phase 1, the HISP will provide an “on-ramp” to the fully functional bi-directional services that will be available in Phase 2 of WISHIN. Phase 2 will establish a network of networks to enable these exchanges.

To assist WISHIN in their technical initiatives, they have contracted with The National Institute for Medical Informatics (NIMI), a nonprofit organization which operates the Wisconsin Health Information Exchange (WHIE) a regional HIE, as their Technical Manager. In this capacity, NIMI will have responsibility for all of the technical aspects of HISP and fully functional HIE services.

To assist WISHIN and NIMI in advancing Direct Secure Messaging as a foundational step for HIE, this RFP is issued by NIMI. NIMI will serve as the sole point of contact for questions related to this RFP process. The person responsible for managing the procurement process, referred to herein as the Technical Lead, is Michael Gagnon. His contact information is provided in Section 1.4.4. The contract resulting from this RFP will be administered by NIMI. The person responsible for this contract is Kim R. Pemble, President of NIMI.

1.3 Definitions

The following definitions are used through the RFP:

1. The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.
2. Bidder – the Solution Provider proving a proposal in response to this RFP.
3. Continuity of Care Document – CCD, refers to the HL7 Clinical Document Architecture (CDA), providing a specification for XML based document.
4. Continuity of Care Record – CCR refers to the ASTM standard for health and data information exchange.
5. Solution Provider – refers to the vendor that is responding to this RFP and will be providing HISP Services.
6. Solution – refers to the HISP services, including certificate credentialing and provider on-boarding process defined through the response to this RFP.
7. HIN – Health Information Network, the entity, WISHIN for our purposes, that provides the HIE services in WI

8. Direct – Refers to the ONC's Direct project and all associated standards. Initially Direct, will support "Push" only functionality for Phase 1.

9. Fully functional HIE refers to the "Push – Pull" structure of exchange and value added services anticipated in Phase 2 of WISHIN project. This will establish a network of networks in WI for HIE.

10. State-level does not mean or imply state government and refers to organizations formed and activities conducted at a state level to provide statewide benefit versus organizations formed and activities conducted at a regional or local level. State government as a health care payer, purchaser, regulator, and public health authority is one of the key stakeholders in state-level HIE.

11. Payload is defined to mean attachments to the Direct Message, which may be in human readable form or machine readable form and include however not be limited to:

    11.1. PDF Document

    11.2. HL7 Transaction(s)

    11.3. CCD and/or CCR

    11.4. Word Document

12. Help Desk Levels:

    12.1. Traditional

        12.1.1. Tier 1 provides basic application software and/or hardware support to callers. Tier 2 Support provides more complex support on application software and/or hardware and is usually an escalation of the call from Tier 1. Tier 3 Support provides support on complex hardware and operating system software and usually involves certified systems engineers.

    12.2. Anticipated WISHIN

        12.2.1. Tier 1 provides local support for workstation, LAN, Internet connectivity problem resolution. Tier 2 is provided by WISHIN and receives calls escalated from Tier 1 and/or end users. This provides core HISP support and more advanced problem trouble shooting and resolution. Tier 3 is provided by Solution Provider and has calls escalated from Tier 2 only.

13. Hosting Data Center Tier Level Requirements Traditional Definitions:

    13.1. Tier 1

        13.1.1. Single non-redundant distribution path serving the IT equipment
        13.1.2. Non-redundant capacity components
        13.1.3. Basic site infrastructure guaranteeing 99.671% availability

13.2. Tier 2 Fulfills all Tier 1 requirements and:

13.2.1. Redundant site infrastructure capacity components guaranteeing 99.741% availability

13.3. Tier 3 Fulfills all Tier 1 and Tier 2 requirements and:

13.3.1. Multiple independent distribution paths serving the IT equipment
13.3.2. All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture
13.3.3. Concurrently maintainable site infrastructure guaranteeing 99.982% availability

13.4. Tier 4 Fulfills all Tier 1, Tier 2 and Tier 3 requirements and:

13.4.1. All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems
13.4.2. Fault-tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability

14. Administrative (e.g. Requirement #77) is defined to include local operations, management and maintenance of the Solution through technical staff at WISHIN (e.g. account management, password "reset", trouble shooting).

1.4 Bidder Format & Response

The following requirements are provided to Bidders.

- Read the RFP completely and thoroughly and present questions to michael.gagnon@hiepartners.com by 6/15/2011. Questions and answers will be shared with all Solution Providers but the asking Solution Provider will not be identified.
- Request a one-hour meeting or conference call with NIMI to answer any questions Bidder may have. Each conference call will be between one Solution Provider and NIMI.
- Be prepared to provide a prototype or scripted demonstration if requested.
- Late responses will not be accepted unless circumstances mandate a late submission and prior approval is granted.
- Customer site visits to show working systems which are similar to the proposed system.
- Provide and sign Bidder's Signature Form.
- Provide a sample copy of your standard contract as part of this submission.
- Prepare a written response according to the outline below. A complete response is required or the proposal will be disqualified.
- An on-site visit to Wisconsin may be required to present the proposal to the NIMI teams.

Solution Providers considering submitting a proposal are expected to raise any questions, exceptions, or additions they may have concerning this RFP document prior to the date and time noted in Section 1.3.3. If a Solution Provider discovers any significant ambiguity, error, conflict, discrepancy, omission, and/or other deficiency in this RFP, the Solution Provider should immediately notify via electronic means (e-mail or facsimile) the above named project manager of such error and request modification or clarification to the RFP.

In the event it becomes necessary to provide additional clarifying data or information, or to

revise any part of this RFP, any revisions, amendments, and/or supplements will be made available in the same manner as the original release of this RFP.

Table 1: Response Format

RESPONSE SECTION	TITLE	FORMAT OR MAXIMUM NUMBER OF PAGES
A	Cover Letter	Letter with company letterhead of no more than 3 pages. Signed by representative that has the legal capacity to contract with the NIMI.
B	Introduction to Bidder Proposal	No more than 3 pages
C	Table of Contents (list all documents comprising this response)	Word or PDF document with table of contents
D	Response to Section 2 – Bidder Responses	
D1	Corporate Background	No more than 1 page
D2	Product Information	No more than 3 pages
D3	Financials	No more than 1 page
D4	Certificate Granting and Resolution	No more than 10 pages
D5	General HISP Services	No more than 10 pages
D6	Help Desk/Education	No more than 5 pages
D7	Legal/Privacy/Security	No more than 5 pages
D8	Audit and Logging	No more than 1 page
D9	Operational/Infrastructure/SLA	No more than 5 pages
D10	Provider Directory Integration	No more than 5 pages
D11	Portal User Interface	No more than 5 pages
D12	Project Management	No more than 5 pages
D13	Support	No more than 5 pages
D14	Response to Pricing	No more than 5 pages
E	RFP Forms	Bidder's Signature Form
F	Customer References	No more than 5 pages
G	Standard Contract	No limit

1.4.1 Number of copies and delivery specifications

The Bidder shall provide 1 electronic copy via email. If additional materials are required then the Bidder can send a CD, DVD or flash drive copy.

Media should be delivered either in person or via US postal service or their approved delivery service in a sealed package (box or envelope), which is conspicuously labeled

"SEALED PROPOSAL – NIMI". The package should also contain the name, address, and telephone number of the proposing firm.

The proposal should be addressed to:
NIMI HISP RFP Response
National Institute for Medical Informatics
Attention: Kim R. Pemble
1009 W. Glen Oak Lane, Suite 101
Mequon, WI 53092

1.4.2 Proposal Format

Word documents shall be Arial with no less than 10 point fonts. Margins shall be no less than 1 inch.

1.4.3 Proposal Schedule

DATE	ACTIVITY
May 31, 2011	RFP Issued
June 15, 2011, 5PM CDT	Deadline for submitting questions to NIMI
June 2 - June 15	Bidders' calls with NIMI (if requested)
June 20, 2011	Bids due at 5:00 p.m. Central Daylight Time
July 1, 2011	Review Responses, References Checked Final Evaluation
July 8, 2011	Initiate Contract Discussion
July 31, 2011	Board approval and Solution Provider award
September 6, 2011	Expected date for system Go-Live

1.4.4 Bidders' Call with NIMI

Bidders may request a conference call with the NIMI Technical Team to clarify any section and/or answer questions by emailing or calling:

Michael Gagnon
Technical Lead
Email: michael.gagnon@hiepartners.com
Phone: 802-735-1837
Mobile: 802-355-2377

Each call will involve only one Bidder and NIMI. These calls are not required. Every attempt will be made to set up that meeting/conference call as soon as possible. These meetings/calls are specifically for Q&A and will not be for Solution Provider presentations or demonstrations. The conference call will not exceed 1 hour.

1.4.5 Questions

All questions concerning this RFP must be submitted by the time established in the Proposal Schedule in this document. All questions are to be sent to michael.gagnon@hiepartners.com, cc to kpemble@whie.org. NIMI will respond within 2 business days.

No other contact may be made by Solution Provider to other organizations or individuals with regards to this proposal. Contact with others regarding this proposal may result in Solution Providers proposal being rejected.

Each proposal shall stipulate that it is predicated upon the requirements, terms, and conditions of this RFP and any supplements or revisions thereof.

1.4.6 Closing Date

All RFP responses must be received by 5:00 P.M., Central Daylight Time, June 20, 2011.

1.4.7 Incurred Expense and Release

NIMI will not be responsible for any expenses incurred by the Bidder in preparing, presenting and submitting a proposal. By submitting a proposal, Bidder agrees that it will not bring any claim or action against NIMI or WISHIN based on any misunderstanding concerning the information provided in the RFP or concerning NIMI's failure, negligent or otherwise, to provide the Bidder with pertinent information in this RFP

1.4.8 Right to reject proposals / waive or correct minor irregularities

NIMI reserves the right to withdraw this Request for Proposal, to reject any proposals, to waive minor irregularities in proposals or to allow the Bidder to correct a minor irregularity if the best interest of the WISHIN and NIMI will be served by doing so. NIMI also may request or require the Solution Provider to partner with another Solution Provider. The content of a Proposal submitted by a Bidder is subject to verification. If NIMI determines in its sole discretion that the content is in any way misleading or inaccurate, NIMI may reject the Proposal.

1.4.9 Links to additional information

NIMI/WHIE: www.whie.org
WISHIN: http://www.wishin.org/
WI State Plan, as approved by ONC:
http://www.dhs.wisconsin.gov/ehealth/SOP01.25.11Posted.pdf

1.5 Bidding Conditions

1.5.1 Prices

The pricing policy that you choose to submit must address the following concerns:

- The structure must be clear, accountable and auditable;
- It must cover the full spectrum of services required;
- Costs and compensation must be consistent with the rates established or negotiated as a result of this RFP or Purchase Order issued based on this contract.

1.5.2 Quantities

The quantities given in the proposal are best estimates and are given as a basis for the comparison of the proposals. Quantities may be increased or decreased as deemed necessary.

1.5.3 Funding

Once a Bidder is selected, a presentation will be submitted to WISHIN, the WISHIN Board and the NIMI Board. Approval to move forward must be obtained from NIMI and funding must be obtained from WISHIN before this project will move into the implementation phase. Solution Providers must agree to a payment schedule based on enrollees to the HISP structure and will only be paid for work once NIMI is paid by WISHIN.

1.5.4 Business References

Reference checks will be based on the RFP response, unless changes or additions are included in the RFP. NIMI reserves the right to contact any reference to assist in the evaluation of the Proposal, to verify information contained in the Proposal and to discuss the Solution Provider's qualifications and the qualifications of any subcontractor identified in the Proposal. NIMI reserves the right to obtain and consider information from other sources concerning a Solution Provider, such as capability and performance under other contracts, the qualifications of any subcontractor identified in the Proposal, the Solution Provider's financial stability, past or pending litigation, and other publicly available information.

1.5.5 RFP Responses

NIMI holds the Solution Provider responsible for the accuracy of all responses in this RFP and reserves the right to include any details of the Bidder response to this RFP in any contract with the selected Bidder. Representations of functionality and other capabilities must be in a delivered product that is in production use at one or more Solution Provider customer sites unless specifically identified as such.

In addition any statements, pricing or other RFP responses may be used by NIMI for inclusion in any contract with the potential Solution Provider.

1.6 Instructions for Price Tables and Schedules

The pricing proposal as outlined in section 2.16 must provide detail for all items in the table. This is not a comprehensive list of costs however you must include all costs in your proposal.

1.6.1 Subcontract

The Bidder must bid on all the components of the RFP. If portions of the work are to be executed by subcontractors or teaming partners, those portions of technologies or services must be identified in the Responses Section and Pricing Tables. Solution Provider will be responsible for the performance of any subcontractors.

1.6.2 Purpose of Price Schedules & Tables

The purpose of the price schedules and tables is to allow NIMI to evaluate the likely cost associated with each Bidder's proposal. NIMI will assume that any item not separately priced on the price schedules is either included in the price of some other item or will be provided at no additional charge. The Bidder shall be responsible for the costs incurred in providing any of the software, supplies, materials and services that are not identified on the price schedules. The Bidder shall be liable for any required supplies, materials or services, within the scope of the contract, that were not presented in the business proposal.

1.6.3 Price Response

It is the WISHIN's and NIMI's long-term intent to implement all functionality described in the RFP; however, NIMI has identified some optional items that should be priced individually. These items must be clearly identified in the document and in the pricing. Additionally NIMI has a limited budget for the project and the Solution Provider will be judged according to this budget.

1.7 Criteria for Bidder Selection

The final Bidder selection will take into consideration the demonstration, reference checks, client site visits, and the Bidder's RFP response. Bidder response scorecard below identifies a summary of how the overall Bidder response to this RFP will be evaluated.

Bidder Response Scorecard

Points are assigned to each of the functional requirements areas.

Key Factors	Maximum Points
Certificate Granting and Resolution	15
General HISP Services & Standards (including EHR and secure e-Mail client integration)	15
Authentication, Audit and Logging, Legal/Privacy/Security	5
Operational Infrastructure and SLA, Help Desk	5
Provider Directory Integration	5
Portal User Interface	5
Support and Project Management	5
TOTAL	**55**
Corporate Background & Financials	5
TOTAL	**5**
Pricing and payment terms	40
TOTAL	**40**
Total Points	**100**

Finalists selected from the above scoring will further be rated on responses to the Phase II Anticipated Functionality, Section 2.16. .

Key Factor	Maximum Points
HIE Node Routing as Initiator and recipient of Direct Messages	**5**
HIE Nodes value add functions including expanded message delivery/routing.	**5**
On-Ramp services	**5**
Web Portal Form Factors	**5**

Key Factor	Maximum Points
WISHIN ROI support	**5**
Total	**25**

1.8 Additional Selection Details

1.8.1 Basis of the Award

Based on approval from WISHIN and NIMI Board of Directors and funding obtained, NIMI shall award this contract to the most responsible and responsive Bidder who best meets the terms and conditions of the proposal.

NIMI reserves the right to not award this RFP, to reject any or all proposals in whole or in part, to make multiple awards, partial awards, award by types, item by item, or lump sum total, or select more than one Solution Provider whichever may be most advantageous to the NIMI. The intent however is to award this contract to one (1) Bidder.

At the discretion of NIMI revisions may be permitted after submissions of proposals and prior to award for the purpose of obtaining best and final offers. Negotiations will be conducted with responsible Bidders who submit proposals found to be reasonably likely to be selected for award. The contents of any proposal shall not be disclosed so as to be available to competing Bidders during any part of this process.

1.8.2 Scoring Criteria

NIMI will review all proposals submitted in response to this RFP. Each Proposal will be evaluated to determine if it meets the mandatory RFP provisions. Any proposal failing to meet those requirements is subject to immediate disqualification without further review. Relative merits of all remaining proposals will be evaluated against criteria as listed in this RFP. The NIMI's findings will be presented to the NIMI Board of Directors and WISHIN which funded this work. The Board will review the team's findings and may request that top Bidders present oral presentations along with their prototype demonstrations.

1.8.3 Ability to Deliver Solution

In addition to the above criteria the Solution Providers ability to get the requested HISP infrastructure operational by September 6, 2011 will also be taken into consideration in the selection.

1.9 Volume Estimates

The following metrics may be used to estimate the potential usage. WISHIN continues to refine "white space" numbers and projections for phased rollout over two year period and will share as these become available. There is no commitment to these volumes, they are provided only for reference.

Category	Total #
Physicians	~13,000
Pharmacies	~1,260
Laboratories	~760
All Medicaid Providers (including non HIPAA)	~58,000

2 Bidder Responses

2.1 Corporate Background

Please provide the following contact information:

Company Name	
Address	
Contact name and title	
Contact telephone number	
Contact fax number	
Contact email address	

Please provide the following corporate information:

Year founded	
Years in Business	
Corporate Headquarters location	
Closest Field Support location to Milwaukee, WI	
Total Employees (at all locations)	
Total Installation Staff (FTEs)	
Total Support Staff (FTEs)	
Total Development Staff (FTEs)	
Total client education Staff (FTEs).	
Call Center location and hours of support	
Insurance – Proof of insurance, with limits, for general liability, errors and omissions, and Cyber/Breech insurance	

2.2 Product Information

Please provide the following information regarding your HISP Product:

Product name(s)	
Current Product Version and Date Generally Available	
Number of current clients using this product	
Total number of HIE's using this product	
Largest installation	
Total number of installed sites (locations)	
Next planned release/average timing of releases	

2.3 Financial Information

Please provide the following financial information. If any of these time frames is not applicable to your firm, based on year of organizational start, please indicate so. Audited financial statements may be requested from finalists as part of selection process.

Total Annual revenue 2008	
Total Annual revenue 2009	
Total Annual revenue 2010	
Public or Private Company?	
What is your bond rating?	
Number of Years in the HIE, HISP or network security Market	
% Of total Revenue spent on Research and Development in 2008	
% Of total Revenue spent on Research and Development in 2009	
% Of total Revenue spent on Research and Development in 2010	

In the following sections, Requirements are numbered. Please respond to each and all Requirements and note the Requirement number in your response.

2.4 Certificate Granting and Resolution

Req. ID	Weight Status (Mandatory/ Optional)	Description
9.0	Mandatory	Solution Provider or Solution must generate, provision, assign, and manage requests for X509 V3 certificates to individuals and entities. Solution must follow RFC3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
10.0	Mandatory	Certificate generated in previous requirement must be associated with Direct Address of the forms as established by WISHIN (e.g. userx@direct.wishin.org or entityx@direct. wishin.org).
11.0	Optional	Define the options available for single year or multi year term cycles on certificates issues as noted previously.
12.0	Mandatory	Solution Provider must support resolution of Direct Addresses issued by WISHIN and other certificate granting authorities (e.g. userx@direct.authority.org or entityx@direct.authority.org).
13.0	Mandatory	Solution Provider must provide a complete participant provisioning and de-provisioning solution that verifies a participant's identification in accordance with national standards prior to the issuance of the X.509v3 certificate. This may be triggered as part of a revocation of a certificate and as certificates expire.
14.0	Mandatory	Solution Provider must support distributed granting (certificate assigned to entity who assigns to employees) of X509 V3 certificates to trusted nodes/entities and align trust structure for these certificates as part of Provider Directory
15.0	Mandatory	Solution must support the ability to serve as proxy for a certified individual or entity, at the request of that individual or entity based on local storage of private key for that individual or entity
16.0	Mandatory	Solution must be able to automatically assess and evaluate trustworthiness of certificates issued by Certificate Authorities that are routed by other HISPs presented in the course of sending and receiving messages Direct Messages.

Req. ID	Weight Status (Mandatory/ Optional)	Description
17.0	Mandatory	Solution Provider must operationalize the following provisioning process (note that these are minimum requirements): To issue an X.509 certificate, through Solution, the following criteria must be met (see also comments to for this requirement): 1) The participant has completed a WISHIN-specific participant application. 2) The participant has signed (or e-signed) a WISHIN-specific participant agreement. 3) The participant has submitted the necessary identity verification documents and those documents have met the verification requirements. 4) Individual participants must have a valid license or certification verified against the appropriate granting agency as defined by WISHIN. 5) Individual or organizational participant has paid required fees as established by WISHIN. As an option for payment, Solution Provider must be able to accept payment electronically through WISHIN branded web portal related to HISP.
18.0	Mandatory	Certificate discovery must occur prior to a Direct message being sent in order to fulfill the encryption functions of the S/MIME format. Discovery must be based on existing Internet protocols (existing specifications exist for discovery via DNS (If DNS is not supported, an alternate method must be offered)
19.0	Mandatory	Must support automated certificate publication and resolution in a directory structure and process that operates intra and inter HISP

2.5 General HISP Services

Req. ID	Weight Status (Mandatory/ Optional)	Description
20.0	Optional	Discuss how messages may be prioritized, such as e-mail "high priority" vs. "low priority" messages. Define action that a client must take to set these priorities.
21.0	Mandatory	Solution Provider must support routing and delivery of various "payloads" as attachments to Direct Messages. Such "payloads" include but are not limited to machine and person readable attachments (e.g. HL7 messages, CCD and PDF).

Req. ID	Weight Status (Mandatory/ Optional)	Description
22.0	Mandatory	Solution Provider and Solution shall demonstrate routing (inter and intra HISP) of "push" transactions originated from any Direct node (e.g. @wishin.direct.org or @minnesota.direct.org)
23.0	Mandatory	Must be Direct-enabled, including 1) Direct Addresses 2) Security & Trust Authority Services 3) Direct Messages (RFC 5322) 4) Message Transport & Delivery (Simple Mail Transport Protocol - SMTP)
24.0	Mandatory	Solution must support Direct-compliant gateways that implement the *Applicability Statement for Secure Health Transport specification* while harmonizing local standards/mechanisms to Direct-equivalents. (e.g., XDR and XDM for Direct Messaging specify such a solution when using IHE XDR for local transport, ITI and S&I). http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport
25.0	Mandatory	Solution must be able to format the “payload” as an Internet Message Format (IMF) RFC5322-compliant email message with a valid MIME body (RFC2045, RFC2046).
141.0	Mandatory	Solution Provider must provide a list of all EHR systems to which they have developed Direct messaging interfaces. Please describe those which are currently live and those that you have planned. Please describe the technical details of how this is accomplished.

2.6 Help Desk/Education

Req. ID	Weight Status (Mandatory/ Optional)	Description
26.0	Optional	Please provide a quotation for providing various levels of Helpdesk services, from Tier 1, Tier 2 and Tier 3 as defined, such that WISHIN and Participating Organizations may determine the level of Help Desk Services it wishes to provide/contract for. Indicate in these quotes whether there are limits to the call volumes allowed in any given tier of support.
27.0	Mandatory	Solution Provider must provide and support an administrative web portal to manage user accounts remotely, re-set passwords remotely and track resets.

Req. ID	Weight Status (Mandatory/ Optional)	Description
28.0	Mandatory	Solution Provider shall establish and maintain Tier3 Help Desk services, with WISHIN providing Tier 2 Help Desk services. Where available, local users will employ their local Help Desk as Tier 1 Help Desk and where not, the WISHIN Helpdesk will serve this function.
29.0	Mandatory	Solution Provider must offer technical training to WISHIN, specific to their tool kit at a level sufficient for WISHIN to support operations (including new client set up/provisioning and deprovisioning), trouble shooting and defect resolution related Tier 2 Help Desk services.
30.0	Mandatory	Solution Provider must collaborate with WISHIN to establish various "alarms" or "alerts" related to operation of HISP enabling WISHIN Helpdesk to be proactive to end users when issues are identified, rather than waiting for users to report arise.
31.0	Mandatory	Solution Provider shall offer end user training materials in electronic format to facilitate WISHIN education sessions and establishment of on-line education services.
32.0	Mandatory	Solution Provider must provide various operational reports related to level of Help Desk services contracted from Solution Provider. For example, but not limited to, Nature of calls, Course of solution, source of calls, time to resolution from reported issue. List all standard reports available.
33.0	Mandatory	Solution Provider shall provide educational material regarding Help Desk Support for technical operations, granting and revocation of certificates.

2.7 Legal/Privacy/Security

Req. ID	Weight Status (Mandatory/ Optional)	Description
34.0	Mandatory	Solution Provider and Solution complies with all applicable federal (including HIPAA and NIST) and Wisconsin regulations mandates and rules regarding security and privacy of protected health information (e.g. http://www.dhs.wisconsin.gov/guide/legal/index.htm). Solution Provider and solution adheres to "Transparency and Data Handling" from Best Practices for HISPs
35.0	Mandatory	Solution Provider must address the risk assessments and residual risks as outlined in this link to Direct Project Threat Model Process
36.0	Mandatory	Solution Provider must execute sub BAA with WISHIN who will in turn have BAA executed with each participating entity and/or provider.
37.0	Mandatory	Solution Provider must use industry best practices to protect access to the system with a firewall and appropriately structured firewall rules and block all improper or other unauthorized access attempts.
38.0	Mandatory	Solution Provider must demonstrate the ability to monitor, prevent and deter unauthorized system access. Any and all known attempts must be reported to WISHIN within the timeframe established in mutually agreeable Service Level Agreement (SLA). Solutions Provider will conduct or provide evidence of a successful intrusion detection test performed by independent firm within 6 months before WISHIN go live.
39.0	Mandatory	Solution Provider must provide reporting for risk assessment related to and identification of various attacks (including Denial of Service (DOS) and “brute force”) and initiate defensive actions, as well as for all breech events of the Solution.
40.0	Mandatory	Solution Provider must use industry best practices to provide and maintain protection against virus/Trojan horse/malware/ worms on all servers and network components. Identify which tools are used for these purposes.
41.0	Mandatory	Provide indication of completion of SAS70 audit, if such has occurred or indicate why such audit has not been undertaken.
42.0	Mandatory	Solution Provider shall provide a copy of security standards and practices, including upgrade and patching procedures to WISHIN.
43.0	Mandatory	Solution Provider must use industry best practices to provide and maintain all operating systems at current or not greater than 1 generation back from current and system intrusion detection and prevention tools at current levels.

Req. ID	Weight Status (Mandatory/ Optional)	Description
44.0	Mandatory	Solution Provider must use industry best practices to maintain all systems, firewall, switches, routers and third party software security patches to current revisions allowing for continuation of maintenance agreements. Further that hardware maintenance agreements and/or replacement equipment must be maintained for all network elements. Further that firmware and software maintenance agreements must be maintained for all network components. Upgrade/maintenance work to be scheduled, in rolling manner across redundant equipment to minimize standard scheduled "downtime" in conjunction with SLA.
45.0	Mandatory	Solution Provider must provide ability to comply with WISHIN directions/resolutions to remediate the results of the security/vulnerability assessment to align with the accepted industry standards.
46.0	Mandatory	Solution Provider must allow for all operational elements of the HISP to function in a manner consistent with ensuring the integrity of all data stored or routed through the HISP.
47.0	Mandatory	Solution Provider must allow for WISHIN to establish security controls for audit logs.
48.0	Mandatory	Solution Provider shall collaborate with WISHIN to establish and maintain appropriate levels of disaster recovery and regularly tested process for all HISP services. Discuss options available as part of Solution related to the above. It is WISHIN preference that this include local hot swap/hot fail over redundancy in all critical components as well as hot site operations with database replication. Pricing of this capability should be established separately.
49.0	Mandatory	Solution Provider shall provide standard reports and ability for WISHIN to establish adhoc reports through Solution Provider tools, or ability to export data to a WISHIN provided tool, related to the above named Legal/Privacy/Security requirements.
50.0	Mandatory	Vendor till attest/certify to WISHIN that it has established and will share a breech notification policy and program.
51.0	Mandatory	Solution Provider will agree in contract to indemnify and hold harmless WISHIN as part of the language in a contract resulting from selection in this RFP process.
52.0	Mandatory	Solution Provider will agree in contract to Wisconsin as State of Law as part of the language in a contract resulting from selection in this RFP process.
53.0	Optional	Solution Provider will manage any out sourcing contracts related to hosting/providing or related operations.

2.8 Authentication

Req. ID	Weight Status (Mandatory/ Optional)	Description
3.0	Mandatory	Solution Provider must support signature, encryption, decryption and payload verification directly or as proxy using S/MIME.
4.0	Mandatory	Such Web Portal User Interfaces shall include User ID and Authentication (two factor identification/authentication), with passwords being required to change no less frequently than 90 days, with password history maintained for past two passwords to prevent repetition of recent passwords. Industry standard password structure must be supported.
5.0	Mandatory	Solution must provide for a maximum number of login retries to the web portals for both HISP and Admin Services and such to be configurable by WISHIN. Upon such failure, describe options for actions within Solution including support for actions such as: Lock Out of Account, Priority Alert to Audit Log.
6.0	Mandatory	Solution must provide for online "User Account Management" including the ability for a User to reset their password.
7.0	Mandatory	Solution Provider must support HISP User Account Management via a web portal service. This may be integrated with HISP Account with access granted on the basis of defined role for these Administrative Users, or as a separate unique portal.
8.0	Mandatory	Solution must support LDAP for authentication related to Web Portal accounts. Such LDAP to be maintained separately from the Provider Directory for security purposes. Provide audit reports related to the LDAP service.

2.9 Audit and Logging

Req. ID	Weight Status (Mandatory/ Optional)	Description
1.0	Mandatory	Solution Provider shall maintain audit logs (Source, Destination, Message Type/Protocol, Date, Time, Status, and Count) for all routing actions, all data access, all applicable proxy actions, and all administrative functions within the HISP. Define options for duration of logs related to operations of and access to HISP.
2.0	Mandatory	Solution Provider must provide for reporting, both "defined standard" (provide examples) reports and ad-hoc reporting tools, from the Audit Logs related to all aspects of operations and administration of the HISP.

2.10 Operational/Infrastructure/SLA

Req. ID	Weight Status (Mandatory/ Optional)	Description
54.0	Mandatory	Solution Provider must offer hosted solution with all servers, connectivity, and basic operational support. Such hosted environment, including help desk, must be located and managed/operated within US and US Territories.
55.0	Mandatory	Solution Provider will offer and price out an optional "turn key" solution that could be hosted at a site designated by WISHIN as an alternative to full hosted model.
56.0	Mandatory	Solution Provider data centers selected for hosting services shall meet or exceed the Tier 3 specifications. Solution Provider will provide reports demonstrating tracking of events impacting availability and cumulative time unavailable for assessment of compliance with SLA.
57.0	Mandatory	Solution Provider and Solution must demonstrate the routing of messages in real time as well as the ability to manage batches of messages delivered from one or more sources (e.g. lab result reporting).
58.0	Mandatory	Solution Provider shall commit to Service Level Agreements for: Initial Login (Web Portal) Performance, Screen to Screen Performance (Web Portal), scheduled and unscheduled up time, and average latency in message routing. Solution Provider will report statistics on these metrics. See also #56.
59.0	Mandatory	Solution must scale to support all HIPAA providers in State of WI (see Appendix for WI volumes) maintaining system performance and uptime within Service Level Agreement (SLA). SLA will include uptime associated with hosting site level uptime commitments (see also #55) excluding scheduled events and for web portal access, 3 second or less screen to screen, sub second within screen response time. SLA will further establish parameters for provider directory performance and latency of messages routed through Solution.
60.0	Mandatory	Solution Provider data center will have operational redundant Internet connections, routed from separate providers and telecommunications central offices with separate building entry points as part of high availability plan.
61.0	Mandatory	Solution Provider shall, with mutually agreeable lead time, allow WISHIN or its delegate to conduct onsite visit/audit at the primary and hot site environments and Security infrastructure and architecture.
62.0	Mandatory	Solution Provider shall provide copies of security audit procedures, and documentation related to the most recent events, including who performed the audits and resolution/mitigation steps taken to address items identified.

Req. ID	Weight Status (Mandatory/ Optional)	Description
63.0	Mandatory	Solution Provider shall provide documentation for: 1) Their change control process 2) Their unit, integration and system level testing plans 3) Their local fail over, hot site fail over, and disaster recovery plans for hosted solutions.
64.0	Mandatory	Solution Provider hosted solution must include all required data storage for primary, hot site and onsite back up purposes, as well as development, test and production staging.
65.0	Mandatory	Solution Provider must have Change and Configuration Management processes and tools that facilitate the reporting, prioritization, and resolution of defects, including source code control, code promotion, and versioning. Provide documentation related to the above.
66.0	Mandatory	Solution Provider selected hot site, included as part of the hosted solution, shall be located a minimum of 100 miles separate from the primary operations site and configured in a manner providing a level of separation from Internet Service Providers to isolate ISP as an up time risk.
67.0	Mandatory	Solution Provider hosted and turn key solutions shall offer ability to configure and manage the level of backup requested by WISHIN.
68.0	Mandatory	Solution Provider must examine system and error logs daily and/or provide tools for this work to be completed by WISHIN, to identify pending issues, predict and minimize system problems and initiate appropriate corrective and/or mitigation action.
69.0	Mandatory	Solution provider must include as part of the implementation the following environments in addition to the primary operations and hot site: Development, Test, Pre-Production Staging and Training. Such environments may be structured in a virtual machine environment, provided that testing and training appropriately reflects production operation and performance.
70.0	Mandatory	Solution Provider shall provide documentation on source control, versioning protocols, and staging for pre production migration for all system upgrades and functional enhancements.
71.0	Mandatory	Solution Provider must perform routine maintenance during a planned weekly maintenance period. Routine maintenance shall include, but is not limited to, server upgrades/patching, software upgrades/patching and hardware maintenance. In order to maintain system availability, the Solution Provider is expected to have the capability to rollover to local redundant servers with patches being applied in a rolling manner during maintenance periods. Such periods to be determined in alignment with regional client expectations for all servers that are "shared" across regions.
72.0	Mandatory	Solution Provider must perform non-routine maintenance at a mutually agreeable time with minimum one (1) week advance notice for all change control to WISHIN. Exceptions for emergent situations

Req. ID	Weight Status (Mandatory/ Optional)	Description
		shall be mutually arranged.
73.0	Mandatory	Solution Provider must have the ability to handle emergency maintenance situations that may be required to bring down the system by giving, when possible, advance notice, before the system goes down for maintenance, to WISHIN and its users. It is expected that the Solution Provider must have the ability to rollover to a backup site during any such emergency maintenance.
74.0	Mandatory	Solution Provider must maintain statistics on (e.g. users, transactions, and message traffic volumes (bandwidth use) by date, day of week, time of day, user, and destination) with ability to provide flexible audit report function (including on demand feature) and audit logging ability. Such tracking and reporting to be constrained by what is "known" in HISP as result of routing messages.
75.0	Mandatory	Solution Provider must track and report on system and network performance metrics (e.g. CPU Usage, Memory swapping, etc.) mutually agreed to as part of SLA, as part of system administration service.
76.0	Mandatory	Solution Provider must provide reports on, or management tools for WIHIN to use for, system monitoring and usage statistics, including metering, data feeds, network, web service access, audit trails and logging, exception handling, configuration management, session management and reporting on same.
77.0	Mandatory	Solution Provider must provide an "Administrative" level user interface for management and maintenance of the HISP services. Define any limits in number or function of admin accounts.
78.0	Mandatory	Solution Provider Solution services must meet or exceed Direct Project Best Practice guidelines as established at http://wiki.directproject.org/Best+Practices+for+HISPs Solution Provider will stay current to updates to these guidelines within 90 days of adoption.

2.11 Provider Directory Integration

Req. ID	Weight Status (Mandatory/ Optional)	Description
79.0	Mandatory	Solution Provider must provide and maintain a provider directory for Direct users that establish accounts directly through the HISP for Direct services.
80.0	Mandatory	Solution must provide for import of extracts from "regional" provider directory to support operations of HISP and association of Certificate between local and state provider directory
81.0	Mandatory	Solution must comply with ONC supported standards direction related to Provider Directory services. These may include ASC X12 Transaction 274 and 275, and /or IHE XD*. Solution provider shall present material in regard to their involvement in and tracking on these evolving standards initiatives.
82.0	Mandatory	Solution must be able to establish and maintain relationships between individuals and entities (individuals associated with 0 or many entities) as appropriate (e.g., Dr. X at Clinic A), following the recommendations and standards established through the ONC. The directory must support multiple Direct addresses for an individual or entity.
83.0	Mandatory	Solution shall store the certificates; however, certificates may be stored in DNS servers during phase I
84.0	Mandatory	Solution shall store audit tracking information on the participant agreement "signature" (e-signature), including but not limited to date and time "signed".
85.0	Mandatory	Solution must store information resulting from the participant vetting process, including but not limited to key information found on the identity documents (e.g., type of document, key details on the document, etc)
86.0	Mandatory	Solution must store key data provided by Wisconsin Medical Society, used by WISHIN for Phase I services, and participant provisioning, including but not limited to provider specific key, license number, license type, license expiration.
87.0	Mandatory	Solution must support the daily refresh/load of data provided by WMS or connect to WMS in real-time to ensure timely and accurate information for vetting participants.
88.0	Mandatory	Solution must store in local Provider Directory Direct address issued with the associated Certificate.
89.0	Mandatory	Solution must store Direct addresses issued by other Certificate Authorities.

Req. ID	Weight Status (Mandatory/ Optional)	Description
90.0	Mandatory	Solution must support web portal for "search" of Provider Direct addresses by Provider Name, Clinic (if entity tracked), and other parameters that appropriately refine identification of an individual Provider.
91.0	Mandatory	Solution Provider and Solution must demonstrate ability to import HIPAA Provider level data from "trusted" external sources (e.g. interstate).
92.0	Mandatory	Solution Provider must support ITI-58 Provider Directory Information Query and ITI-59 Provider Directory Information Feed
93.0	Mandatory	Solution must maintain an audit log for all edits, deletions, insertions to the Provider Directory as part of audit tracking. Such data to be accessible by Solution Provider and/or WISHIN through standardized reports and for adhoc reporting by WISHIN.

2.12 Portal User Interface

Req. ID	Weight Status (Mandatory/ Optional)	Description
97.0	Mandatory	Solution Provider, through Solution, must offer and operate a web portal supporting enrollment, composition, sending, routing, receiving, reading, printing and importing of Direct Secure Messages and allowable attachments to these messages.
98.0	Mandatory	Such Web Portal User Interfaces shall include User ID and Authentication (two factor identification/authentication), with passwords being required to change no less frequently than 90 days, with password history maintained for past two passwords to prevent repetition of recent passwords. Industry standard password structure must be supported.
99.0	Mandatory	Solution must provide for a maximum number of login retries to the web portals for both HISP and Admin Services and such to be configurable by WISHIN. Upon such failure, describe options for actions within Solution including support for actions such as: Lock Out of Account, Priority Alert to Audit Log.
100.0	Mandatory	Solution Provider must support HISP User Account Management via a web portal service. This may be integrated with HISP Account with access granted on the basis of defined role for these Administrative Users, or as a separate unique portal.

Req. ID	Weight Status (Mandatory/ Optional)	Description
101.0	Mandatory	Solution will offer and support use of standard e-mail client (e.g. Outlook, GMAIL, etc.) that have the ability to encrypt messages, as entry point supporting composition, sending, routing, receiving and reading Direct Secure Messages. Solution Provider shall discuss platforms currently supported in operations.
102.0	Mandatory	Solution Provider shall indicate support of the following: 1) Web-based e-mail clients that offer secure (e.g. SSL) e-mail. 2) POP-S and 3) IMAP-S as platforms related to the use of e-mail clients as interface to your HISP platform.
103.0	Mandatory	Solution must support use of Direct Enabled EHR systems as entry point supporting enrollment, composition, sending, routing, receiving and reading Direct Secure Messages and attachments.
104.0	Mandatory	Solution must support LDAP for authentication related to Web Portal accounts. Such LDAP to be maintained separately from the Provider Directory for security purposes.
105.0	Mandatory	Solution web portal must provide users with the status of their participation (i.e., participation agreement received, waiting for identity documents, approved, denied, etc). In addition, the web portal should provide users with any error messages or key communications regarding their account or the vetting process (for example, the user would receive a message if we were not able to verify their medical license and the message would inform the user of the next steps to correct the problem).
106.0	Mandatory	Solution web portal must automatically append a WISHIN drafted confidentiality statement to each Direct message sent by an end user.
107.0	Mandatory	Solution web portal must support a WISHIN configurable auto time out capability for all active sessions. Such configuration at a minimum established at the WISHIN level.
108.0	Mandatory	Solution must include a public-facing interface, perhaps integrated with the previously discussed web portal that supports authorized user searching of the Provider Directory in order to locate another participant's Direct address and public certificate.
109.0	Mandatory	Solution Provider Web Portal must support commonly used Internet browsers such as Internet Explorer, Firefox, Safari, or other HTML5 supported platforms. Solution Provider shall further identify which versions of these browsers are supported.

Req. ID	Weight Status (Mandatory/ Optional)	Description
110.0	Mandatory	Solution Provider must ensure that all health information in transit and at rest (at Solution) is unusable, unreadable, or indecipherable to unauthorized individuals through use of a technology or methodology specified by the Secretary of the Federal Department of Health and Human Services in the guidance issued under section 13402(h) (2) of the American Recovery and Reinvestment Act of 2009 (P.L. 111-5), or any update to that guidance. Solution Provider must apply updates within a 90 day window.
111.0	Mandatory	Solution Provider and Solution must provide for WISHIN branding on all User Interface and Administrative Interface screens. For example: "WISHIN powered by…"
112.0	Mandatory	Solution should provide a mechanism for Single Sign On (SSO) for authenticated users from trusted domains.

2.13 Standards

Req. ID	Weight Status (Mandatory/ Optional)	Description
94.0	Mandatory	Solution Provider and Solution must support existing and evolving standards including but not limited to: Direct, Direct XDR and XDM, HL7 2.x, HL7 3.x, CDA, IHE, SMTP (SMTP/TLS), S-MIME, DNS, X12 274 and S&I Framework. Compliance is defined in the Applicability Statement for Secure Health Transport.
95.0	Mandatory	In addition to SMTP, the primary delivery standard for Direct, the Proposed Solution must support healthcare environments that have adopted other profiles: 1) SOAP – format for exchanging structured information, based on XML for message format 2) XDR and XDM for Direct Messaging (XDR – supports a direct push model using Web Services transport, XDM – supports a direct push model with SMTP as a transport) 3) XD* Conversion (enables interoperability between Direct participants who may be using SOAP+XDR, SMTP+XDM, or SMTP+MIME) 4) HITSP T17 Secured Communications Channel. 5) IHE XDA, XDE, XD*
96.0	Mandatory	Solution Provider will present documentation on operation of Solution in the context of retries on delivery (e.g. number of retries) and reporting, including local logs and messages to sender, in regards to failures to deliver

2.14 Support

Req. ID	Weight Status (Mandatory/ Optional)	Description
113.0	Mandatory	Describe your support model (i.e. 7x24, 365, guaranteed call back, etc.)
114.0	Mandatory	Do you have response time guarantees associated with different types of calls?
115.0	Mandatory	What are your normal support hours (specify time zone)? Where is support staff located?
116.0	Mandatory	What is the response time for problems reported: 1) during regular business hours and 2) off-hours?
117.0	Mandatory	Which of the following support features are available? Toll Free Hotline Remote Monitoring Remote Diagnostics Online training tutorials Web-based support tracking Open and track tickets online
118.0	Mandatory	Please describe an example of a reported problem and how it was handled. Describe your problem reporting software and tools. Are they available via the Internet? Can a list of outstanding problems and enhancements by client be viewed on-line and downloaded?
119.0	Mandatory	Please list the top 5 support questions you receive from your clients.
120.0	Mandatory	Describe your support process for evaluating and fixing “bugs” or problems in your software. How would you coordinate problem analysis and resolution with the RHIO and other third party products?
121.0	Mandatory	Do you have user groups? If so, who sponsors the user group? How often do they meet? What is the meeting format?
122.0	Mandatory	Do you have advisory groups? What is their membership?
123.0	Mandatory	Please provide a guideline for the type of internal support that will be required, for information systems personnel and also non-information systems personnel (i.e., practice based).
124.0	Mandatory	Do you offer centralized core support services together with localized support for stakeholders?
125.0	Mandatory	Who provides front line support to users of the HIE (i.e. Bidder, HIE, health system, etc.)
126.0	Mandatory	Is any customer support provided offshore? If so describe.

2.15 Project Management

Req. ID	Weight Status (Mandatory/ Optional)	Description
127.0	Mandatory	Please provide a sample project plan including phases and tasks of projects
128.0	Mandatory	Describe the normal skill level of the project manager. Provide your job description.
129.0	Mandatory	Provide a sample status reports. What is included in the status report (i.e. Activities planned, work accomplished, problems, deliverables, etc?)
130.0	Mandatory	Provide a sample team structure (leadership team, technical team, clinical teams, etc.).
131.0	Mandatory	Describe how you handle change control.
132.0	Mandatory	Describe how you track and resolve issues during implementation. Please describe what will be included on this report (including issue number, description, date first reported, resolved, responsible party, issue escalation, etc.)
133.0	Mandatory	Describe your implementation methodology.
134.0	Mandatory	Describe your project communication methodology. Will a project web site be available?
135.0	Mandatory	How do you provide version control of your applications?
136.0	Mandatory	What FTE resources on our part will you require for implementation and continuing support?
137.0	Mandatory	Provide a sample lessons learned document from a previous installation.
138.0	Mandatory	Describe (or provide a sample) testing plan.
139.0	Mandatory	Describe statistical and trending reports that are available (i.e. Usage of NIMI HISP services by participants authorized users, types and volumes of information accessed by authorized user, volume of demographic and record locator services, etc.)
140.0	Mandatory	Please describe your process for requested system customizations and modifications before and during implementation?

2.16 Phase II Anticipated Functionality

This section begins to address the integration of HISP and HIE services following anticipated functional requirements for Phase 2 of a fully functional Health Information Exchange, establishing a network of networks, connecting/integrating the various existing HIE services in Wisconsin. These responses and related assessments will be applied to finalists as an additional evaluation metric, categorized as Solution Provider Vision for Integration of HISP and HIE services. Bidder will describe current capabilities and 12-18 month planning related to the following:

Req. ID	Weight Status (Mandatory/ Optional)	Description
1.0	**Optional**	**Solution Provider will support routing of messages to/from HIE nodes on the state wide HIN (e.g. a HIE may receive a Direct message statement or question and respond in kind, and a HIE may initiate delivery of message based on internal HIE event).**
2.0	**Optional**	**HIE nodes may perform local, regional or state level value add services which may include:** **1) Duplication of messages supporting addition of new destinations to existing message;** **2) Spawning of new messages to new sources on the basis of: Source; Destination; Message type and/or content;** **3) Offer/support data driven actions from the provider directory.** **Solution Provider will support all such value add services in the context of additional routing requests. Solution Provider will maintain audit log of routing actions and support and/or serve Provider Directory address resolution in support of HIE actions. HIE will maintain context of value add functional actions.**
3.0	**Optional**	**Solution Provider and WISHIN Technical Manager will operate HISP in the context of being an optional "on ramp" to HIE services in the State. Such "on ramp" services will not be impacted by message structure or payload content.**
4.0	**Optional**	**Web Portal Solution must allow for various UI form factors (e.g. workstation screen, iPhone, iPad, etc.?)**
5.0	**Optional**	**HISP services must be managed, messages routed, directories resolved and maintained, etc. to support an environment of value add from messages, beyond fundamental message routing. Discuss how this should align with WISHIN ROI including HISP and HIE clients and strategic growth planning.**

2.17 Price Tables and Schedules

For the following pricing details, assume that NIMI will provide Tier 1 and 2 help desk support. If your help desk support (Tier 3) is not incorporated into your fees please provide those costs separately.

Provide details of pricing based on a per provider structure. List all provider types, provide detail definition and pricing (e.g. one time and ongoing monthly or annually) per provider type. Indicate if there are any price breaks for volumes of providers (e.g. first 500 at a certain level, the next 500 at another level or for sites that are "self administering" certificates to their employees). Indicate methods for tracking and reporting the number of "providers" and the basis of that provider's fees (e.g. differentiate a single provider from a large IDN that is "self managing" provider certificates).

If fees are structured on a per transaction model, provide details of the transaction types, and their ongoing fees. Identify all one time fees separate from the ongoing transaction fees. Indicate all details on a per transaction model (e.g. accounting methods, reporting methods, handling of errors or undeliverable messages and other exceptions). Indicate which transaction accounting application, if any, is integrated with the Solution.

2.17.1 Optional Pricing Element

If offered, please provide pricing on these options. If not offered indicate as such:

2.17.1.1 Addition of Help Desk Tier 1 and Tier 2 as outlined previously in requirements (See # 26 and Definitions Section).

2.17.1.2 Train the Trainer education sessions for WISHIN and other support staff to attend, including the costs of materials. Indicate if classes are offered in WI or only at Solution Provider designated site(s).

2.17.1.3 Offering of End User Support services for integration of EHRs and e-mail clients on per site or per hour basis.

2.17.1.4 Offering of End User Training sessions to be offered in regional areas of the state.

2.17.2 Additional Commitments from RFP

- Contract term will be for a period of 3 years with WISHIN options for 2 additional years.
- Prices must be guaranteed for a period of 3 years from the signing of a contract.
- As stated previously, any statements, pricing or other RFP responses may be used by NIMI for inclusion in any contract with the potential Solution Provider.
- Solution Provider may withdraw proposal before final selection.

- Selected Solution Provider will commit to indemnify and hold harmless WISHIN and NIMI. (See Requirement #51)
- Selected Solution Provider will commit to establishing Wisconsin as State of Law in contract. (See Requirement #52.)

2.18 Bidder Signature Form:

I attest that all statements in this RFP are true.

NAME OF BIDDER: _____

SIGNATURE OF AUTHORIZED PERSON: _____

TYPE IN NAME OF AUTHORIZED PERSON: _____

TITLE OF AUTHORIZED PERSON: _____

STREET NAME AND NUMBER: _____

CITY, STATE, AND ZIP CODE: _____

CONTACT PERSON: _____

TELEPHONE NUMBER: _____

FAX NUMBER: _____

E-MAIL:_____

DATE: _____