Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
1.0	Audit and Logging	Mandatory	Solution Provider shall maintain audit logs (Source, Destination, Message Type/Protocol, Date, Time, Status, Count)for all routing actions, all data access, all applicable proxy actions, and all administrative functions within the HISP.	
2.0	Audit and Logging	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.	
3.0	Authentication	Mandatory	Solution Provider must support signature, encryption, decryption and payload verification directly or as proxy using S/MIME.	
4.0	Certification Granting/Resolution	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.	
5.0	Certification Granting/Resolution	Mandatory	Certificate generated in previous requirement must be associated with Direct Address of the form as established by WISHIN (e.g. userx@direct.wishin.org or entityx@direct. wishin.org).	
6.0	Certification Granting/Resolution	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).	http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport
7.0	Certification Granting/Resolution	Mandatory	Solution Provider must provide a complete participant provisioning and de-provisioning solution that verifies a participants 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.	
8.0	Certification Granting/Resolution	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	
9.0	Certification Granting/Resolution	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	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document: **1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.** **2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.**				
10.0	Certification Granting/Resolution	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.	
11.0	Certification Granting/Resolution	Mandatory	Solution Provider must operationalize the following provisioning process (note that these are minimum requirements. RFP respondents may enhance or expand upon these requirements as long as the resulting process meets the requirements set forth in this section): X.509 certificates cannot be issued unless the following criteria are met: 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) Has paid required fees as established by WISHIN. Solution Provider must be able to accept payment electronically. For individual participants, the identity verification documents include: A notarized copy of two identity documents: a) The identity documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. b) At least one document shall be a valid State or Federal government-issued picture identification (ID). For entity participants, the identity verification process is still being defined. Until this work is completed, a designated official contact at entity will have	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
12.0	Certification Granting/Resolution	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)	http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport healthit.hhs.gov/portal/server.pt/...0.../digital-certificates-021111.ppt
13.0	Certification Granting/Resolution	Mandatory	Must support automated certificate publication and resolution in a directory structure and process that operates intra and inter HISP	
14.0	EHR Connectivity	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 and PDF).	
15.0	General HISP Services	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)	
16.0	General HISP Services	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)	
17.0	General HISP Services	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.	
18.0	General HISP Services	Mandatory	Soluton must be able to format the “payload” as an Internet Message Format (IMF) RFC5322-compliant email message with a valid MIME body (RFC2045, RFC2046).	
19.0	Help Desk/Education	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	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document: **1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.** **2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.**				
20.0	Help Desk/Education	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.	Traditional 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. WISHIN 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
21.0	Help Desk/Education	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.	
22.0	Help Desk/Education	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.	
23.0	Help Desk/Education	Mandatory	Solution Provider shall offer end user training materials in electronic format to facilitate WISHIN education sessions and establishment of on-line education services.	
24.0	Help Desk/Education	Mandatory	Solution Provider shall provide educational material regarding Help Desk Support for technical operations, granting and revocation of certificates.	
25.0	Legal/Privacy/Security	Mandatory	Solution Provider and Solution complies with all applicable federal (including HIPAA) and Wisconsin regulations mandates and rules regarding security and privacy of protected health information. Explain Solution Provider and solution adheres to "Transparency and Data Handling" from Best Practices for HISPs	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
26.0	Legal/Privacy/Security	Mandatory	Solution Provider must address the risk assessments and residual risks as outlined in this link to Direct Project Threat Model Process	
27.0	Legal/Privacy/Security	Mandatory	Solution Provider must execute sub BAA with WISHIN who will in turn have BAA executed with each participating entity and/or provider.	
28.0	Legal/Privacy/Security	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.	
29.0	Legal/Privacy/Security	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).	
30.0	Legal/Privacy/Security	Mandatory	Solution Provider must provide reporting for identification of various attacks (including Denial of Service (DOS) and “brute force”) and initiate defensive actions.	
31.0	Legal/Privacy/Security	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.	
32.0	Legal/Privacy/Security	Mandatory	Solution Provider shall provide a copy of security standards and practices, including upgrade and patching procedures to WISHIN.	
33.0	Legal/Privacy/Security	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.	
34.0	Legal/Privacy/Security	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document: **1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.** **2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.**				
35.0	Legal/Privacy/Security	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 standards of WISHIN.	
36.0	Legal/Privacy/Security	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.	
37.0	Legal/Privacy/Security	Mandatory	Solution Provider must allow for WISHIN to establish security controls for audit logs.	
38.0	Legal/Privacy/Security	Mandatory	Solution Provider shall collaborate with WISHIN to establish and maintain appropriate levels of disaster recovery and regularly tested process for all HISP services. At a minimum, this will include local hot swap/hot fail over redundancy in all critical components as well as hot site operations with database replication.	
39.0	Legal/Privacy/Security	Mandatory	Solution Provider shall provide standard reports and adhoc reporting tools related to the above named Legal/Privacy/Security requirements.	
40.0	Operational/Infrastructure/SLA	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.	
41.0	Operational/Infrastructure/SLA	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document: **1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.** **2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.**				
42.0	Operational/Infrastructure/SLA	Mandatory	Solution Provider data centers selected for hosting services shall meet or exceed the Tier 3 specifications.	Tier Level Requirements 1 Single non-redundant distribution path serving the IT equipment Non-redundant capacity components Basic site infrastructure guaranteeing 99.671% availability 2 Fulfills all Tier 1 requirements Redundant site infrastructure capacity components guaranteeing 99.741% availability 3 Fulfills all Tier 1 and Tier 2 requirements Multiple independent distribution paths serving the IT equipment All IT equipment must be dual-powered and fully compatible with the topology of a site's architecture Concurrently maintainable site infrastructure guaranteeing 99.982% availability 4 Fulfills all Tier 1, Tier 2 and Tier 3 requirements All cooling equipment is independently dual-powered, including chillers and heating, ventilating and air-conditioning (HVAC) systems Fault-tolerant site infrastructure with electrical power storage and distribution facilities guaranteeing 99.995% availability
43.0	Operational/Infrastructure/SLA	Mandatory	Solution Provider and Solution must demonstrate the routing of messages in real time as well as those delivered in a batch process.	
44.0	Operational/Infrastructure/SLA	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document: **1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.** **2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.**				
45.0	Operational/Infrastructure/SLA	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 99.8% uptime 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.	
46.0	Operational/Infrastructure/SLA	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.	
47.0	Operational/Infrastructure/SLA	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.	
48.0	Operational/Infrastructure/SLA	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.	
49.0	Operational/Infrastructure/SLA	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.	
50.0	Operational/Infrastructure/SLA	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.	
51.0	Operational/Infrastructure/SLA	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
52.0	Operational/Infrastructure/SLA	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.	
53.0	Operational/Infrastructure/SLA	Mandatory	Solution Provider hosted and turn key solutions shall offer ability to configure and manage the level of backup requested by WISHIN.	
54.0	Operational/Infrastructure/SLA	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.	
55.0	Operational/Infrastructure/SLA	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.	
56.0	Operational/Infrastructure/SLA	Mandatory	Solution Provider shall provide documentation on source control, versioning protocols, and staging for pre production migration for all system upgrades and functional enhancements.	
57.0	Operational/Infrastructure/SLA	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.	
58.0	Operational/Infrastructure/SLA	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 shall be mutually arranged.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
59.0	Operational/Infrastructure/SLA	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.	
60.0	Operational/Infrastructure/SLA	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, 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.	
61.0	Operational/Infrastructure/SLA	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.	
62.0	Operational/Infrastructure/SLA	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	
63.0	Operational/Infrastructure/SLA	Mandatory	Solution Provider must provide an "Administrative" level user interface for management and maintenance of the HISP services.	
64.0	Operational/Infrastructure/SLA	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	
65.0	Provider Directory	Mandatory	Solution Provider must provide and maintain a provider directory for Direct users that establish accounts directly through the HISP for Direct services.	
66.0	Provider Directory	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	
67.0	Provider Directory	Mandatory	Solution must comply with ASC X12 Transaction 274 – Health Care Provider Information	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
68.0	Provider Directory	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 an standards established through the ONC. The directory must support multiple Direct addresses for an individual or entity.	
69.0	Provider Directory	Mandatory	Solution shall store the certificates; however, certificates may be stored in DNS servers during phase I	
70.0	Provider Directory	Mandatory	Solution shall store audit tracking information on the participant agreement "signature" (e-signature), including but not limited to date and time "signed".	
71.0	Provider Directory	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)	
72.0	Provider Directory	Mandatory	Solution must store key data provided by WMS, used by WISHIN for Phase I services, and participant provisioning, including but not limited to provider specific key, license number, license type, license expiration.	
73.0	Provider Directory	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.	
74.0	Provider Directory	Mandatory	Solution must store in local Provider Directory Direct address issued with the associated Certificate.	
75.0	Provider Directory	Mandatory	Solution must store Direct addresses issued by other Certificate Authorities.	
76.0	Provider Directory	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.	
77.0	Provider Directory	Mandatory	Solution Provider and Solution must demonstrate ability to import HIPAA Provider level data from external sources.	
78.0	Provider Directory	Mandatory	Solution Provider must support ITI-58 Provider Directory Information Query and ITI-59 Provider Directory Information Feed	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
79.0	Provider Directory	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.	
80.0	Standards	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, S-MIME, DNS, X12 274 and S&I Framework. Compliance is defined in the Applicability Statement for Secure Health Transport.	
81.0	Standards	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.	
82.0	User Interface	Mandatory	Solution Provider, through Solution, must offer and operate a web portal supporting enrollment, composition, sending, routing, receiving and reading Direct Secure Messages and allowable attachments to these messages.	
83.0	User Interface	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.	
84.0	User Interface	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
85.0	User Interface	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.	
86.0	User Interface	Mandatory	HISP 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	
87.0	User Interface	Mandatory	Solution Provider shall indicate support of the following: 1) Web-based e-mail clients that offer secure 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.	
88.0	User Interface	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.	
89.0	User Interface	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.	
90.0	User Interface	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).	
91.0	User Interface	Mandatory	Solution web portal must automatically append a WISHIN drafted confidentiality statement to each Direct message sent by an end user.	Obtain input from Policy Committee on language.
92.0	User Interface	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.	

Req. ID	Functional Category	Weight Status (Mandatory/ Optional)	Description	Comment
				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
For the scope of this document:				
1. "Solution Provider" refers to the organization responding to the RFP and their proposed Solution.				
2. "Solution" is that provided by Solution Provider to provide HISP services as defined in these requirements.				
93.0	User Interface	Mandatory	Solution must include a public-facing interface, perhaps integrated with the previously discussed web portal, that supports authorized user searching of the Provider Director in order to locate another participant's Direct address and public certificate.	
94.0	User Interface	Mandatory	Solution Provider Web Portal must support commonly used Internet browsers such as Internet Explorer, Firefox, or Safari.	
95.0	User Interface	Mandatory	Solution Provider must ensure that all health information in transit and at rest 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.	
96.0	User Interface	Mandatory	Solution Provider and Solution must provide for WISHIN branding on all User Interface and Administrative Interface screens. For example: "WISHIN powered by…"	

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment

Committee Member Comment