

Exhibit B

HISP Specifications and Requirements

General Privacy and Security Standards Compliance Requirements

- HISPs will continue to comply with all Texas and federal laws and other regulations including but not limited to privacy and security, ONC policies, CMS regulations, requirements, etc. as they evolve.
- HISPs will be compliant with HIPAA and HITECH Privacy and Security rules and will execute a contract with Providers that includes appropriate privacy and security obligations.
- HISPs will attest to THSA that it has established a breach notification compliance program consistent with THSA guidelines and will provide a copy of such program at the beginning of the Term and thereafter upon request from THSA..
- HISPs will complete a security audit and penetration test on their technology infrastructure and provide documented results to the THSA and any affected Providers upon request. The security audit and penetration test must be repeated i) at least quarterly, and ii) any time there are significant technology infrastructure changes to HISP's solution.
- At least one time per calendar year, HISP shall submit to a third party security audit to be performed by a third party of the THSA's choosing. In the event that HISP fails to pass such third party audit, then HISP agrees to submit to THSA a corrective action plan and submit to subsequent audits until a pattern of compliance with security requirements has been satisfied. HISP shall be solely responsible for the reasonable costs of such audits.
- No more than one time per calendar year, HISP shall be subject to a financial audit by the THSA or the THSA's authorized agent with respect to the THSA White Space grant program. If HISP elects to have such financial audit performed by a mutually agreeable independent auditor instead, HISP agrees to pay the costs of such audit. If any discrepancies are found, THSA may require additional audits at HISP's expense in order to rectify any such discrepancies.

Implementation Methodology Requirements:

- HISP will clearly outline to Providers the extent, types and hours of availability of any free technical support, as well as any ongoing support, before Provider selects a Qualified HISP with which to contract.

Technical Architecture Requirements:

- Qualified HISP shall support exchange within the HISP, but also bidirectional exchange between other HISPs using S/MIME and XD* protocols, and bidirectional exchange between EMRs using S/MIME and XD*.

- Qualified HISPs must be able to sign, encrypt, decrypt, and verify the payload using S/MIME as well as support SMTP, S/MIME, and X.509v3 certificates to securely transport health information over the internet as defined by the Applicability Statement for Secure Health Transport: (<http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport>)
- Additionally, Qualified HISPs must support use both i) one x.509v3 certificate for signing and encryption, and ii) optional use of two x.509v3 certificates (one for encrypting and one for signing).
- Qualified HISPs must provide a web-based email client that supports SMTP/TLS protocols and a gateway for desktop-based email clients (such as Outlook) that support POP-S and IMAP-S interfaces. In both cases, x509 certificate or certificates must be issued and employed at the individual provider level. The qualified HISP is not expected to profile a desktop email client application, although it may provide such.
- Qualified HISPs that manage private keys must perform specific risk assessment and risk mitigation to ensure that the private keys have the strongest protection from unauthorized use. That risk assessment must address the risk of internal personnel or external attackers gaining unauthorized access either to the keys or to the health information functions for which the keys enforce trust. HISPs must have a defined policy for notification and handling of a breach of private key stores. Qualified HISP shall provide access to such policy to the THSA upon request.
- Qualified HISPs must be able to format the “payload” as an RFC5322-compliant email message with a valid MIME body (RFC2045, RFC2046). The delivery of messages must be agnostic of attachment type or format.
- Qualified HISPs may not retain patient data for purposes other than processing and delivering the message, or use or store of message payload beyond what is explicitly required by its contract with Providers. Additional access to content must be governed by a separate contract between the Qualified HISP and Provider. Secondary use of any patient data received by the Qualified HISP during the Term of this Agreement is strictly prohibited.
- Qualified HISPs must retain record counts of provider-level (by Direct address) sent, received, failed and pending messages at a minimum of weekly counts and provide such counts to THSA on the first of each month.
- QVs must supply a monthly transaction volume report to the THSA showing, at a minimum, the number of inbound and outbound messages transmitted by the HISP using S/MIME and using XD* protocols.
- Qualified HISPs must route messages to any other well-formed Direct address, regardless of destination HISP provider.

- Qualified HISPs must have the ability to support automatic forwarding of messages from one Direct address to another Direct project address to enable transition of HISP services.
- Qualified HISPs must support the ability for providers to use a custom address domain (e.g. drjohn@direct.mypractice.com) either by forwarding or by native hosting.
- Qualified HISPs must have a defined disaster recovery and backup plan, including offsite hosting and ability to recover from disasters such as primary hardware failure, long-term power outage, flood, etc. A copy of such plan shall be submitted to THSA at the beginning of the Term and later on request of THSA.
- Qualified HISPs must have a defined process and set of policies for testing and deploying production updates to ensure compliance with its service level agreements with Providers.
- Qualified HISPs shall immediately inform THSA about suspected breaches and shall keep the THSA updated regarding such breaches until they have been resolved to the THSA's satisfaction.
- Qualified HISPs will comply with the THSA CP and will issue a public (summary) and a private CP or CPS or similar document explaining how the Qualified HISP will implement the THSA CP. Such CP or CPS shall be subject to the approval of THSA. The CP or CPS should address key life cycle management.
- Qualified HISP CA/RA/VA requirements. The Qualified HISP shall:
 - Qualified HISP, when federal policy and operational procedures are completed to allow for such, must issue all new certificates in such a way as to be interoperable with the federal government (e.g. issuing federal bridge cross-certified certificates, or similar). At this time, Qualified HISP must also re-issue (upgrade) existing HISP Direct Project users and organizations with new federal interoperable certificates in an orderly, efficient, free, and simple process (such as via an automatic update).
 - Have principal subjects (subscribers) of keys acknowledge a security best practices document covering topics, including, but not limited to, password hygiene, keeping their systems patched, an understanding of the liability and harm if a their credentials are compromised, agreeing to notify the HISP immediately if a password or key seems to be compromised, agreeing not to share passwords, using two factor authentication periodically, etc. as part of their subscriber agreement
 - Prohibit, in the subscriber agreement, the use of keys for purposes other than healthcare related data exchange with the Qualified HISP.
 - Issue keys under a new single trust anchor dedicated to THSA HISP operations

- Use NIST level 3 identity proofing for initial key issuance (requiring validation of a person's credentials)
- Operate a Certification Authority, Registration Authority, and Simple Certificate Enrollment Protocol (SCEP) service
- Support batch enrollment, subject to THSA policy
- Support the Online Certificate Status Protocol (OCSP - RFC2560 and RFC5019), including AIA-extension
- Support RFC4387 for distribution of CA certificates and CRLs over HTTP
- Support a Validation Authority service serving OCSP responses (RFC2560/5019), CA certificates and CRLS (RFC4387) with a maximum latency as per THSA policy
- Store Certificates and CRLs in a data source that can be published to, or responds to inquiries from, a provider directory using web services or a RESTful interface
- Key recovery module to store private keys for recovery for selected users and certificates.
- Highly available deployment architecture
- Long term key escrow, key recovery, services (this provision shall survive contract termination) as per THSA policy
- Use the x.509 v3 "Policy Mappings Extension" to indicate the policy compliance OID
- Issue a v3 x.509 certificate with a policy statement OID for the THSA, and one for the HISP, and optimally a policy for any organization affiliated with the principal of the certificate
- Maintain an audit log of all significant activity. Significant activity means, at a minimum, an audit log containing at least the information as required by federal and state guidelines, including accounting for disclosures.
- Respond to a "health check" inquiry by the THSA to allow for operational monitoring
- Support ONC S&I Framework, or other THSA to-be-determined methods of supporting a Provider Directory, and x.509v3 cert distribution, including both organizational and individual end-user (provider) certificates.
- Issue x.509v3 certificates to each provider organization, and to each human end-user of the HISP
- Issue "machine" certificates for THSA approved automated systems

- Provide 24x7x365 help desk support for the duration of the HISP operations for end users. The first month of support will be provided at no charge to Providers from the first date of HISP connectivity with the Provider.
- Subject to THSA policy, issue certificates for roles within organizations such as to the “ED department of xyz facility”
- Issue two x.509v3 certificates for each end point; one to be used for digital signature and non-repudiation purposes, the second to be used for encryption
- Conduct periodic security and HIPAA training for their staff
- Support external RA, CA, and VA service providers as required in the future.
- Provide an "easy" method for non-technical end users to manage their certificates
- Disable or temporarily suspend HISP access in near real time to end-user or organizational accounts with revoked or suspended credentials or where the end-user or organization appears to be breached (subject to THSA policy)
- Provide a reasonable transition plan, subject to THSA approval, in the event that this contract is terminated either by the Qualified HISP or the THSA to avoid an interruption in service to HISP end-users or organizations

Email Account Configuration Requirements:

- Qualified HISPs must provide a configuration guide to Providers who want to manually set-up their e-mail accounts in the web-based mail client provided by the HISP and desktop-based mail clients such as Outlook
- Qualified HISPs must provide to Providers online access to mailbox and account management including:
 - Basic account demographics
 - Trust store manipulation
 - Message forwarding

Best Practice Compliance Requirements:

- Qualified HISPs must follow HISP Best Practices in regard to HIPAA and Legal Agreements, Security, and Transparency and Data Handling/Retention as recommended by HISP Best Practices as published by the Direct project. This information is currently located at the following URL:
<http://wiki.directproject.org/Best+Practices+for+HISPs>.

- Qualified HISPs must include all data collection, use, retention and disclosure policies (including rights reserved but not exercised) in BAAs or other service agreements. Qualified HISPs must minimize data collection, use, retention and disclosure to that minimally required to meet the level of service required of the HISP. Minimal use may require retention of data for security, audit, logging and other required operation; such use must be included in BAAs and service agreements, and must capture the minimal amount of data to fulfill those requirements. Audit logs should contain records related to both: i) sent messages, and ii) failed messages.
- Qualified HISPs agree to participate in the development of and to adopt new industry-consensus approved best practices with respect to HISP “rules of the road”.