REQUEST FOR PROPOSALS FOR

PA Health Information Exchange Community Shared Services Implementation

ISSUING OFFICE

Office of Administration, Office for Information Technology
PA eHealth Partnership Authority
311 Finance Building
Harrisburg, PA 17020

RFP NUMBER

6100021471

DATE OF ISSUANCE

August 7, 2012
REQUEST FOR PROPOSALS FOR
PA Health Information Exchange Community Shared Services Implementation

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CALENDAR OF EVENTS</td>
<td>iv</td>
</tr>
<tr>
<td>Part I—GENERAL INFORMATION</td>
<td>1</td>
</tr>
<tr>
<td>Part II—PROPOSAL REQUIREMENTS</td>
<td>11</td>
</tr>
<tr>
<td>Part III—CRITERIA FOR SELECTION</td>
<td>17</td>
</tr>
<tr>
<td>Part IV—WORK STATEMENT</td>
<td>22</td>
</tr>
<tr>
<td>APPENDIX A, CONTRACT TERMS AND CONDITIONS</td>
<td></td>
</tr>
<tr>
<td>APPENDIX B, DOMESTIC WORKFORCE UTILIZATION CERTIFICATION</td>
<td></td>
</tr>
<tr>
<td>APPENDIX C, PROPOSAL COVER SHEET</td>
<td></td>
</tr>
<tr>
<td>APPENDIX D, TRADE SECRET/CONFIDENTAL PROPRIETARY INFORMATION NOTICE</td>
<td></td>
</tr>
<tr>
<td>APPENDIX E, LOBBYING CERTIFICATION</td>
<td></td>
</tr>
<tr>
<td>APPENDIX F, PROJECT REFERENCES</td>
<td></td>
</tr>
<tr>
<td>APPENDIX G, PROPOSED PERSONNEL REFERENCE TEMPLATE</td>
<td></td>
</tr>
<tr>
<td>APPENDIX H, COST MATRIX</td>
<td></td>
</tr>
<tr>
<td>APPENDIX I, ACRONYMS AND GLOSSARY</td>
<td></td>
</tr>
<tr>
<td>APPENDIX J, PROJECT CHARTER</td>
<td></td>
</tr>
<tr>
<td>APPENDIX K, GOVERNANCE STRUCTURE</td>
<td></td>
</tr>
<tr>
<td>APPENDIX L, CHANGE MANAGEMENT TEMPLATE</td>
<td></td>
</tr>
</tbody>
</table>
The Commonwealth will make every effort to adhere to the following schedule:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Responsibility</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deadline to submit Questions via email to <a href="mailto:kashaffer@pa.gov">kashaffer@pa.gov</a></td>
<td>Potential Offerors</td>
<td>August 17, 2012 1:00 PM EST</td>
</tr>
<tr>
<td>Pre-proposal Conference—Pennsylvania Emergency Management Agency, 2605 Interstate Drive, Room 230, Harrisburg, PA 17110</td>
<td>Issuing Office/Potential Offerors</td>
<td>August 23, 2012 1:00 PM EST</td>
</tr>
<tr>
<td>Answers to Potential Offeror questions posted to the DGS website <a href="http://www.dgsweb.state.pa.us/RTA/Search.aspx">http://www.dgsweb.state.pa.us/RTA/Search.aspx</a> no later than this date.</td>
<td>Issuing Office</td>
<td>August 24, 2012 4:00 PM EST</td>
</tr>
<tr>
<td>Deadline to submit second round of questions via email to <a href="mailto:kashaffer@pa.gov">kashaffer@pa.gov</a></td>
<td>Potential Offerors</td>
<td>August 31, 2012 1:00 PM EST</td>
</tr>
<tr>
<td>Answers to second round of questions posted to the DGS website <a href="http://www.dgsweb.state.pa.us/RTA/Search.aspx">http://www.dgsweb.state.pa.us/RTA/Search.aspx</a> no later than this date.</td>
<td>Issuing Office</td>
<td>September 7, 2012 4:00 PM EST</td>
</tr>
<tr>
<td>Please monitor website for all communications regarding the RFP.</td>
<td>Potential Offerors</td>
<td>Ongoing</td>
</tr>
<tr>
<td>Sealed proposal must be received by the Issuing Office at Kay Shaffer, Bureau of IT Procurement c/o Commonwealth Mail Processing Center 2 Technology Park (rear) Attn: IT Procurement 506 Finance Harrisburg, PA 17110</td>
<td>Offerors</td>
<td>September 21, 2012 1:00 PM EST</td>
</tr>
</tbody>
</table>
PART I

GENERAL INFORMATION

I-1. Purpose. This request for proposals (RFP) provides to those interested in submitting proposals for the subject procurement (“Offerors”) sufficient information to enable them to prepare and submit proposals for the Office of Administration’s (“OA’s”) consideration on behalf of the Commonwealth of Pennsylvania (“Commonwealth”) to satisfy a need for the PA Health Information Exchange Community Shared Services Implementation (“Project”).

I-2. Issuing Office. The OA (“Issuing Office”) has issued this RFP on behalf of the Commonwealth. The sole point of contact in the Commonwealth for this RFP shall be Kay Shaffer, 311 Finance Building, Harrisburg, PA 17120, kashaffer@pa.gov, the Issuing Officer for this RFP. Please refer all inquiries to the Issuing Officer.

I-3. Scope. This RFP contains instructions governing the requested proposals, including the requirements for the information and material to be included; a description of the service to be provided; requirements which Offerors must meet to be eligible for consideration; general evaluation criteria; and other requirements specific to this RFP.

I-4. Problem Statement. During July to November 2011 the PA eHealth Collaborative Office (“eHCO”), an office within OA, initiated a stakeholder engagement process, which included more than 150 individuals representing the Pennsylvania healthcare community. Information about, and work products resulting from, that stakeholder engagement process may be found at this location: http://www.paehealthcollab.com/community_shared_svcs.html. The input from that process informed Act 121 of 2012, which is designed to support existing health information exchange (HIE) networks with an overarching HIE-Network governing entity, the Pennsylvania eHealth Partnership Authority. It is anticipated that the Authority will take up the work of the PA eHCO, and will either become the signatory of the Contract resulting from this RFP or will be the Contract’s assignee.

The HIE-Network is conceived as a network-of-networks connected by a thin layer of community shared services (CSS). These services will enable secure, confidential information exchange from one certified Health Information Service Provider (HISP) to another as well as one certified HIE organization to another. The HISPs and HIEs will be certified by the Authority. HIE certification requirements are in the early draft stages. HISP certification has been defined and further information can be found at: http://www.paehealthcollab.com/health_care_prof_minigrant.html. Further, the CSS will support HISP to HIE and HIE to HISP exchanges. The CSS represents the suite of registries, indexing services and security functions that will create a cost-effective pathway between the various certified entities. The CSS is intended to support the common needs of health care providers, patients, HISPs, HIEs, payers, and other stakeholders by facilitating communication across entity boundaries for improved health care quality, cost and efficiency. The CSS is being procured via this RFP as a supplier hosted solution. Additional detail is provided in Part IV of this RFP.
The following vendors are precluded from proposing or acting as subcontractors on this RFP: Virtual Performance, LLC, Dynamed Solutions, LLC, PRworks Inc, and SCFoster, LLC. In addition, should the Commonwealth issue a separate procurement for Independent Verification and Validation Services (IV&V), the selected Offeror of this RFP and any subcontractors would be precluded from the IV&V procurement.

I-5. **Type of Contract.** It is proposed that if the Issuing Office enters into a contract as a result of this RFP, it will be a **fixed price** contract containing the Contract Terms and Conditions as shown in **Appendix A**. The Issuing Office, in its sole discretion, may undertake negotiations with Offerors whose proposals, in the judgment of the Issuing Office, show them to be qualified, responsible and capable of performing the Project.

I-6. **Rejection of Proposals.** The Issuing Office reserves the right, in its sole and complete discretion, to reject any proposal received as a result of this RFP.

I-7. **Incurring Costs.** The Issuing Office is not liable for any costs the Offeror incurs in preparation and submission of its proposal, in participating in the RFP process or in anticipation of award of the contract.

I-8. **Pre-proposal Conference.** The Issuing Office will hold a Pre-proposal conference as specified in the Calendar of Events. The purpose of this conference is to provide opportunity for clarification of the RFP. Offerors should forward all questions to the Issuing Office in accordance with **Part I, Section I-9** to ensure adequate time for analysis before the Issuing Office provides an answer. Offerors may also ask questions at the conference. In view of the limited facilities available for the conference, Offerors should limit their representation to **two (2) individuals per Offeror**. The Pre-proposal conference is for information only. Any answers furnished during the conference will not be official until they have been verified, in writing, by the Issuing Office. All questions and written answers will be posted on the Department of General Services’ (DGS) website as an addendum to, and shall become part of, this RFP. Attendance at the Pre-proposal Conference is optional.

I-9. **Questions & Answers.** If an Offeror has any questions regarding this RFP, the Offeror must submit the questions by email (with the subject line “RFP 6100021471 Question”) to the Issuing Officer named in **Part I, Section I-2** of the RFP. Two rounds of questions are being permitted, per the Calendar of Events. If the Offeror has questions, they must be submitted via email **no later than** the date indicated on the Calendar of Events. The Offeror shall not attempt to contact the Issuing Officer by any other means. The Issuing Officer shall post the answers to the questions on the DGS website by the date stated on the Calendar of Events. An Offeror who submits a question **after** the final deadline date for receipt of questions indicated on the Calendar of Events assumes the risk that its proposal will not be responsive or competitive because the Commonwealth is not able to respond before the proposal receipt date or in sufficient time for the Offeror to prepare a responsive or competitive proposal. When submitted after the final deadline date for receipt of questions indicated on the Calendar of Events, the Issuing Officer **may** respond to questions of an administrative nature by directing the questioning Offeror to
specific provisions in the RFP. To the extent that the Issuing Office decides to respond to a non-administrative question after the final deadline date for receipt of questions indicated on the Calendar of Events, the answer must be provided to all Offerors through an addendum.

All questions and responses as posted on the DGS website are considered as an addendum to, and part of, this RFP in accordance with RFP Part I, Section I-10. Each Offeror shall be responsible to monitor the DGS website for new or revised RFP information. The Issuing Office shall not be bound by any verbal information nor shall it be bound by any written information that is not either contained within the RFP or formally issued as an addendum by the Issuing Office. The Issuing Office does not consider questions to be a protest of the specifications or of the solicitation. The required protest process for Commonwealth procurements is described on the DGS website http://www.dgsweb.state.pa.us/comod/ProtestProcedures.doc

I-10. Addenda to the RFP. If the Issuing Office deems it necessary to revise any part of this RFP before the proposal response date, the Issuing Office will post an addendum to the DGS website at http://www.dgsweb.state.pa.us/RTA/Search.aspx. It is the Offeror’s responsibility to periodically check the website for any new information or addenda to the RFP. Answers to the questions asked during the Questions & Answers period also will be posted to the website as an addendum to the RFP.

I-11. Response Date. To be considered for selection, hard copies of proposals must arrive at the Issuing Office on or before the time and date specified in the RFP Calendar of Events. The Issuing Office will not accept proposals via email or facsimile transmission. Offerors who send proposals by mail or other delivery service should allow sufficient delivery time to ensure timely receipt of their proposals. If, due to inclement weather, natural disaster, or any other cause, the Commonwealth office location to which proposals are to be returned is closed on the proposal response date, the deadline for submission will be automatically extended until the next Commonwealth business day on which the office is open, unless the Issuing Office otherwise notifies Offerors. The hour for submission of proposals shall remain the same. The Issuing Office will reject, unopened, any late proposals. Note: hand-delivered proposals must be delivered to the address set forth in the Calendar of Events and must be time and date stamped by the facility receiving the proposals. Proposals may only be hand-delivered between 6:00 a.m. and 2:45 p.m., Monday through Friday, excluding Commonwealth holidays.

I-12. Proposals. To be considered, Offerors should submit a complete response to this RFP to the Issuing Office, using the format provided in Part II, providing eight (8) paper copies of the Technical Submittal and two (2) paper copy of the Cost Submittal and two (2) paper copies of the Small Diverse Business (SDB) participation submittal. In addition to the paper copies of the proposal, Offerors shall submit two complete and exact copies of the entire proposal (Technical, Cost and Disadvantaged Business Submittals, along with all requested documents) on CD-ROM or Flash drive in Microsoft Office or Microsoft Office-compatible format. The electronic copy must be a mirror image of the paper copy and any spreadsheets must be in Microsoft Excel. The Offerors may not lock or protect any cells or tabs. Offerors should ensure that there is no costing information in the technical submittal. Offerors should not reiterate technical information in the cost submittal. The CD or Flash drive should clearly identify the Offeror and include the name and version number of the virus scanning software that was used to
scan the CD or Flash drive before it was submitted. The Offeror shall make no other distribution of its proposal to any other Offeror or Commonwealth official or Commonwealth consultant. Each proposal page should be numbered for ease of reference. An official authorized to bind the Offeror to its proposals must sign the proposal. If the official signs the Proposal Cover Sheet (Appendix C to this RFP) and the Proposal Cover Sheet is attached to the Offeror’s proposal, the requirement will be met. For this RFP, the proposal must remain valid for 120 days or until a contract is fully executed. If the Issuing Office selects the Offeror’s proposal for award, the contents of the selected Offeror’s proposal will become, except to the extent the contents are changed through Best and Final Offers or negotiations, contractual obligations.

Each Offeror submitting a proposal specifically waives any right to withdraw or modify it, except that the Offeror may withdraw its proposal by written notice received at the Issuing Office’s address for proposal delivery prior to the exact hour and date specified for proposal receipt. An Offeror or its authorized representative may withdraw its proposal in person prior to the exact hour and date set for proposal receipt, provided the withdrawing person provides appropriate identification and signs a receipt for the proposal. An Offeror may modify its submitted proposal prior to the exact hour and date set for proposal receipt only by submitting a new sealed proposal or sealed modification which complies with the RFP requirements.

I-13. Small Diverse Business Information. The Issuing Office encourages participation by small diverse businesses as prime contractors, and encourages all prime contractors to make a significant commitment to use small diverse businesses as subcontractors and suppliers.

A Small Diverse Business is a DGS-certified minority-owned business, woman-owned business, service-disabled veteran-owned business or veteran-owned business, or United States Small Business Administration-certified 8(a) small disadvantaged business concern, that qualifies as a small business.

A small business is a business in the United States which is independently owned, not dominant in its field of operation, employs no more than 100 full-time or full-time equivalent employees, and earns less than $20 million in gross annual revenues ($25 million in gross annual revenues for those businesses in the information technology sales or service business).

Questions regarding this Program can be directed to:

Department of General Services
Bureau of Small Business Opportunities
Room 611, North Office Building
Harrisburg, PA 17125
Phone: (717) 783-3119
Fax: (717) 787-7052
Email: gs-bmwbo@state.pa.us
Website: www.dgs.state.pa.us

The Department’s directory of BSBO-certified minority-, women-, veteran- and service disabled veteran-owned businesses can be accessed from:
I-14. **Economy of Preparation.** Offerors should prepare proposals simply and economically, providing a straightforward, concise description of the Offeror’s ability to meet the requirements of the RFP. **Page limits are set by response sections and are further detailed in Part II of this RFP.Responses must be in a readable font size, preferably Verdana 10 point or Times New Roman 12 point.**

I-15. **Alternate Proposals.** The Issuing Office has identified the basic approach to meeting its requirements, allowing Offerors to be creative and propose their best solution to meeting these requirements. The Issuing Office will not accept alternate proposals.

I-16. **Discussions for Clarification.** Offerors may be required to make an oral or written clarification of their proposals to the Issuing Office to ensure thorough mutual understanding and Offeror responsiveness to the solicitation requirements. The Issuing Office will initiate requests for clarification. Clarifications may occur at any stage of the evaluation and selection process prior to contract execution.

I-17. **Prime Contractor Responsibilities.** The contract will require the selected Offeror to assume responsibility for all services offered in its proposal whether it produces them itself or by subcontract. The Issuing Office will consider the selected Offeror to be the sole point of contact with regard to contractual matters.

I-18. **Proposal Contents.**

A. **Confidential Information.** The Commonwealth is not requesting, and does not require, confidential proprietary information or trade secrets to be included as part of Offerors’ submissions in order to evaluate proposals submitted in response to this RFP. Accordingly, except as provided herein, Offerors should not label proposal submissions as confidential or proprietary or trade secret protected. Any Offeror who determines that it must divulge such information as part of its proposal must submit the signed written statement described in subsection c. below and must additionally provide a redacted version of its proposal, which removes only the confidential proprietary information and trade secrets, for required public disclosure purposes.

B. **Commonwealth Use.** All material submitted with the proposal shall be considered the property of the Commonwealth of Pennsylvania and may be returned only at the Issuing Office’s option. The Commonwealth has the right to use any or all ideas not protected by intellectual property rights that are presented in any proposal regardless of whether the proposal becomes part of a contract. Notwithstanding any Offeror copyright designations contained on proposals, the Commonwealth shall have the right to make copies and distribute proposals internally and to comply with public record or other disclosure
requirements under the provisions of any Commonwealth or United States statute or
regulation, or rule or order of any court of competent jurisdiction.

C. **Public Disclosure.** After the award of a contract pursuant to this RFP, all proposal
submissions are subject to disclosure in response to a request for public records made
under the Pennsylvania Right-to-Know-Law, 65 P.S. § 67.101, et seq. If a proposal
submission contains confidential proprietary information or trade secrets, a signed written
statement to this effect must be provided with the submission in accordance with 65 P.S.
§ 67.707(b) for the information to be considered exempt under 65 P.S. § 67.708(b)(11)
from public records requests. (See Appendix D, Trade Secret/Confidential Proprietary
Information Notice). Financial capability information submitted in response to Part II,
Section II-7 of this RFP is exempt from public records disclosure under 65 P.S. §
67.708(b)(26).

I-19. **Best and Final Offers.**

A. While not required, the Issuing Office reserves the right to conduct discussions with
Offerors for the purpose of obtaining “best and final offers.” To obtain best and final
offers from Offerors, the Issuing Office may do one or more of the following, in any
combination and order:

1. Schedule oral presentations;
2. Request revised proposals;
3. Conduct a reverse online auction; and
4. Enter into pre-selection negotiations.

B. The following Offerors will **not** be invited by the Issuing Office to submit a Best and
Final Offer:

1. Those Offerors, which the Issuing Office has determined to be not responsible or
whose proposals the Issuing Office has determined to be not responsive.
2. Those Offerors, which the Issuing Office has determined in accordance with **Part III,
Section III-5**, from the submitted and gathered financial and other information, do
not possess the financial capability, experience or qualifications to assure good faith
performance of the contract.
3. Those Offerors whose score for their technical submittal of the proposal is less than
70% of the total amount of technical points allotted to the technical criterion.

The Issuing Office may further limit participation in the best and final offers process to
those remaining responsible Offerors which the Issuing Office has, within its discretion,
determined to be within the top competitive range of responsive proposals.
C. The Evaluation Criteria found in Part III, Section III-4, shall also be used to evaluate the Best and Final offers.

D. Price reductions offered through any reverse online auction shall have no effect upon the Offeror’s Technical Submittal. Dollar commitments to Small Diverse Businesses can be reduced only in the same percentage as the percent reduction in the total price offered through any reverse online auction or negotiations.

I-20. News Releases. Offerors shall not issue news releases, Internet postings, advertisements or any other public communications pertaining to this Project without prior written approval of the Issuing Office, and then only in coordination with the Issuing Office.

I-21. Restriction of Contact. From the issue date of this RFP until the Issuing Office selects a proposal for award, the Issuing Officer is the sole point of contact concerning this RFP. Any violation of this condition may be cause for the Issuing Office to reject the offending Offeror’s proposal. If the Issuing Office later discovers that the Offeror has engaged in any violations of this condition, the Issuing Office may reject the offending Offeror’s proposal or rescind its contract award. Offerors must agree not to distribute any part of their proposals beyond the Issuing Office. An Offeror who shares information contained in its proposal with other Commonwealth personnel and/or competing Offeror personnel may be disqualified.

I-22. Issuing Office Participation. Offerors shall provide all services, supplies, facilities, and other support necessary to complete the identified work, except as otherwise provided in this Part I, Section I-22. It is expected that the contracted services resulting from this RFP will be hosted by the selected Offeror. The Commonwealth will provide only project staff as needed to ensure a successful implementation and project management. No office space or equipment will be provided. The Commonwealth will provide conference rooms as needed as well as access to the staff necessary for the requirements described in this RFP.

I-23. Term of Contract. The term of the contract will commence on the Effective Date and will end in five (5) years with five (5) optional one year renewals. The renewals may be exercised in single or multiple year terms at the Commonwealth’s discretion, by letter signed by the Contracting Officer. The Issuing Office will fix the Effective Date after the contract has been fully executed by the selected Offeror and by the Commonwealth and all approvals required by Commonwealth contracting procedures have been obtained. The selected Offeror shall not start the performance of any work prior to the Effective Date of the contract and the Commonwealth shall not be liable to pay the selected Offeror for any service or work performed or expenses incurred before the Effective Date of the contract.

I-24. Offeror’s Representations and Authorizations. By submitting its proposal, each Offeror understands, represents, and acknowledges that:

A. All of the Offeror’s information and representations in the proposal are material and important, and the Issuing Office may rely upon the contents of the proposal in awarding the contract(s). The Commonwealth shall treat any misstatement, omission or
misrepresentation as fraudulent concealment of the true facts relating to the Proposal submission, punishable pursuant to 18 Pa. C.S. § 4904.

B. The Offeror has arrived at the price(s) and amounts in its proposal independently and without consultation, communication, or agreement with any other Offeror or potential Offeror.

C. The Offeror has not disclosed the price(s), the amount of the proposal, nor the approximate price(s) or amount(s) of its proposal to any other firm or person who is an Offeror or potential Offeror for this RFP, and the Offeror shall not disclose any of these items on or before the proposal submission deadline specified in the Calendar of Events of this RFP.

D. The Offeror has not attempted, nor will it attempt, to induce any firm or person to refrain from submitting a proposal on this contract, or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal.

E. The Offeror makes its proposal in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive proposal.

F. To the best knowledge of the person signing the proposal for the Offeror, the Offeror, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any governmental agency and have not in the last four years been convicted or found liable for any act prohibited by State or Federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding or proposing on any public contract, except as the Offeror has disclosed in its proposal.

G. To the best of the knowledge of the person signing the proposal for the Offeror and except as the Offeror has otherwise disclosed in its proposal, the Offeror has no outstanding, delinquent obligations to the Commonwealth including, but not limited to, any state tax liability not being contested on appeal or other obligation of the Offeror that is owed to the Commonwealth.

H. The Offeror is not currently under suspension or debarment by the Commonwealth, any other state or the federal government, and if the Offeror cannot so certify, then it shall submit along with its proposal a written explanation of why it cannot make such certification.

I. The Offeror has not made, under separate contract with the Issuing Office, any recommendations to the Issuing Office concerning the need for the services described in its proposal or the specifications for the services described in the proposal.
J. Each Offeror, by submitting its proposal, authorizes Commonwealth agencies to release to the Commonwealth information concerning the Offeror’s Pennsylvania taxes, unemployment compensation and workers’ compensation liabilities.

K. Until the selected Offeror receives a fully executed and approved written contract from the Issuing Office, there is no legal and valid contract, in law or in equity, and the Offeror shall not begin to perform.


A. Contract Negotiations. The Issuing Office will notify all Offerors in writing of the Offeror selected for contract negotiations after the Issuing Office has determined, taking into consideration all of the evaluation factors, the proposal that is the most advantageous to the Issuing Office.

B. Award. Offerors whose proposals are not selected will be notified when contract negotiations have been successfully completed and the Issuing Office has received the final negotiated contract signed by the selected Offeror.

I-26. Debriefing Conferences. Upon notification of award, Offerors whose proposals were not selected will be given the opportunity to be debriefed. The Issuing Office will schedule the debriefing at a mutually agreeable time. The debriefing will not compare the Offeror with other Offerors, other than the position of the Offeror’s proposal in relation to all other Offeror proposals. An Offeror’s exercise of the opportunity to be debriefed does not constitute nor toll the time for filing a protest (See Section I-27 of this RFP).

I-27. RFP Protest Procedure. The RFP Protest Procedure is on the DGS website at http://www.dgsweb.state.pa.us/comod/ProtestProcedures.doc. A protest by a party not submitting a proposal must be filed within seven days after the protesting party knew or should have known of the facts giving rise to the protest, but no later than the proposal submission deadline specified in the Calendar of Events of the RFP. Offerors may file a protest within seven days after the protesting Offeror knew or should have known of the facts giving rise to the protest, but in no event may an Offeror file a protest later than seven days after the date the notice of award of the contract is posted on the DGS website. The date of filing is the date of receipt of the protest. A protest must be filed in writing with the Issuing Office. To be timely, the protest must be received by 4:00 p.m. on the seventh day.

I-28. Use of Electronic Versions of this RFP. This RFP is being made available by electronic means. If an Offeror electronically accepts the RFP, the Offeror acknowledges and accepts full responsibility to insure that no changes are made to the RFP. In the event of a conflict between a version of the RFP in the Offeror’s possession and the Issuing Office’s version of the RFP, the Issuing Office’s version shall govern.

I-29. Information Technology Bulletins. This RFP is subject to the Information Technology Bulletins (ITB’s) issued by the Office of Administration, Office for Information Technology.
ITBs may be found at:
http://www.portal.state.pa.us/portal/server.pt?open=512&objID=416&PageID=210791&mode=2

All proposals must be submitted on the basis that all ITBs are applicable to this procurement. It is the responsibility of the Offeror to read and be familiar with the ITBs. Notwithstanding the foregoing, if the Offeror believes that any ITB is not applicable to this procurement, it must list all such ITBs in its technical submittal, and explain why it believes the ITB is not applicable. The Issuing Office may, in its sole discretion, accept or reject any request that an ITB not be considered to be applicable to the procurement. The Offeror’s failure to list an ITB will result in its waiving its right to do so later, unless the Issuing Office, in its sole discretion, determines that it would be in the best interest of the Commonwealth to waive the pertinent ITB.
PART II

PROPOSAL REQUIREMENTS

Offerors must submit their proposals in the format, including heading descriptions, outlined below. To be considered, the proposal must respond to all requirements in this part of the RFP. Offerors should provide any other information thought to be relevant, but not applicable to the enumerated categories, as an appendix to the Proposal. All cost data relating to this proposal and all Small Diverse Business cost data should be kept separate from and not included in the Technical Submittal. Each Proposal shall consist of the following three separately sealed submittals:

A. Technical Submittal, which shall be a response to RFP Part II, Sections II-1 through II-8;

B. Small Diverse Business Submittal, in response to RFP Part II, Section II-9; and

C. Cost Submittal, in response to RFP Part II, Section II-10.

The Issuing Office reserves the right to request additional information which, in the Issuing Office’s opinion, is necessary to assure that the Offeror’s competence, number of qualified employees, business organization, and financial resources are adequate to perform according to the RFP.

The Issuing Office may make investigations as deemed necessary to determine the ability of the Offeror to perform the Project, and the Offeror shall furnish to the Issuing Office all requested information and data. The Issuing Office reserves the right to reject any proposal if the evidence submitted by, or investigation of, such Offeror fails to satisfy the Issuing Office that such Offeror is properly qualified to carry out the obligations of the RFP and to complete the Project as specified.

II-1. Statement of the Problem. State in succinct terms your understanding of the problem presented or the service required by this RFP. Offerors must also describe the three to five characteristics, conditions, or variables they believe will have a direct and critical impact on the effectiveness, efficiency, and viability of their proposed solution. Offerors must describe their approach to mitigating risks and ensuring these critical factors are successful. This section of the response should be limited to no more than five (5) pages.

II-2. Management Summary. Include a narrative description of the proposed effort and an overview of how each of the pieces of your response will come together, to form an, efficient, interoperable, and cost effective solution for the CSS. This section of the response should be limited to no more than two (2) pages.

II-3. Approach and Work Plan. Describe in narrative form your technical plan for accomplishing the work. Use the requirements descriptions in Part IV of this RFP as your reference point. Responses must address all functionality required in Part IV of this RFP and
include the technical architecture proposed to support the solution. Modifications of the task descriptions are permitted; however, reasons for changes should be fully explained. Indicate the number of person hours allocated to each task. Include a Program Evaluation and Review Technique (PERT) or similar type display, time related, showing each event (as an attachment to your response, which will not count towards the page limit). If more than one approach is apparent, comment on why you chose this approach. This section of the response should not contain any marketing materials, and should be limited to no more than 150 pages.

II-4. Prior Experience. Include experience in implementing large scale HIE deployments, management of large, complex systems, security infrastructure services, ITIL v3, testing and datacenter hosting services. All experience shown should indicate the degree to which individuals and/or your company were serving participants across business entities, and must emphasize the applicability of the experience to the HIE arena. Experience shown should be work done by individuals who will be assigned to this project as well as that of your company. Studies or projects referred to must be identified and the name of the customer shown, including the name, address, and telephone number of the responsible official of the customer, company, or agency who may be contacted.

Offerors must provide a minimum of three (3) client references similar in size, scope and complexity to the requirements of this RFP. These may be the same client references used to satisfy the Mandatory Requirements in Part III-1, however Offerors must use the applicable Appendix. Please reference and complete Appendix F, Project References, for each of the three references. This section of the response should be included as an appendix, and does not have a page limitation.

II-5. Personnel. Include the number of executive and professional personnel, analysts, auditors, researchers, programmers, consultants, etc., who will be engaged in the work. Show where these personnel will be physically located during the time they are engaged in the Project. Identify proposed key personnel, include the employee’s name and, through a resume or similar document, the Project personnel’s education and experience in implementing large scale HIE deployments, management of large complex projects, security infrastructure, ITIL v3, testing, and datacenter hosting services. Indicate the responsibilities each individual will have in this Project and how long each has been with your company. Identify by name any subcontractors you intend to use and the services they will perform. The Offeror must certify that all personnel named in their proposal shall actually work on the project in the manner described in their proposal.

Resumes are not to include personal information that will, or will be likely to, require redaction prior to release of the proposal under the Right to Know Law. This includes home addresses and phone numbers, Social Security Numbers, Drivers’ License numbers or numbers from state ID cards issued in lieu of a Drivers’ License, financial account numbers, etc. If the Commonwealth requires any of this information for security verification or other purposes, the information will be requested separately and as necessary. Please reference and complete Appendix G, Proposed Personnel Reference Template for each of the key personnel being proposed.
The individuals named in the selected Offeror’s proposal shall continue to perform services for the duration of the Contract, except in the event of resignation or death. No changes, substitution, additions or deletions shall be made unless approved in advance by the Commonwealth, which approval shall not be unreasonably withheld. In such event, the selected Contractor must notify the Commonwealth’s Project Manager at least thirty (30) days prior to replacing a member of its staff assigned to the project. The selected Contractor must provide the name, qualifications and background check of the person who will replace the staff member. Within ten (10) days of receiving notice, the Commonwealth’s Project Manager will notify the selected Contractor of whether the replacement candidate is acceptable and whether the replacement is approved.

The Commonwealth’s Project Manager may request that the selected Contractor remove one or more of its staff from this project at any time. In the event that a staff member is removed from the project, the selected Contractor will have ten (10) days to fill the vacancy with an individual deemed by the Commonwealth’s Project Manager to have acceptable experience and skills.

This section of the response should be included as an appendix, and does not have a page limitation.

II-6. Training. Indicate recommended training of agency personnel. Include the agency personnel to be trained, the number to be trained, duration of the program, place of training, curricula, training materials to be used, number and frequency of sessions, and number and level of instructors. Use the requirements descriptions in Part IV of this RFP as your reference point. This section of the response should be limited to no more than five (5) pages.

II-7. Financial Capability. Describe your company’s financial stability and economic capability to perform the contract requirements. Provide your company’s financial statements (audited, if available) for the past three fiscal years. Financial statements must include the company’s Balance Sheet and Income Statement or Profit/Loss Statements. Also include a Dun & Bradstreet comprehensive report if available. If your company is a publicly traded company, please provide a link to your financial records on your company website in lieu of providing hardcopies. The Commonwealth reserves the right to request additional information it deems necessary to evaluate an Offeror’s financial capability. This section of the response should be included as an appendix, and does not have a page limitation.

II-8. Objections and Additions to Contract Terms and Conditions and SLAs. The Offeror will identify which, if any, of the terms and conditions (contained in Appendix A) and SLAs (contained in Appendix T) it would like to negotiate and what additional terms and conditions the Offeror would like to add to the contract terms and conditions. The Offeror’s failure to make a submission under this paragraph will result in its waiving its right to do so later, but the Issuing Office may consider late objections and requests for additions if to do so, in the Issuing Office’s sole discretion, would be in the best interest of the Commonwealth. The Issuing Office may, in its sole discretion, accept or reject any requested changes to the SLAs and contract terms and conditions. The Offeror shall not request changes to the other provisions of the RFP, nor shall the Offeror request to completely substitute its own terms and conditions for Appendix A or Appendix T. All terms and conditions must appear in one integrated contract. The Issuing
Office will not accept references to the Offeror’s, or any other, online guides or online terms and
conditions contained in any proposal.

Regardless of any objections set out in its proposal, the Offeror must submit its proposal,
including the cost proposal, on the basis of the terms and conditions and SLAs set out in
Appendix A and Appendix T. The Issuing Office will reject any proposal that is conditioned
on the negotiation of the terms and conditions or SLAs set out in Appendix A, Appendix T, or
to other provisions of the RFP as specifically identified above. This section of the response
should be included as an appendix, and does not have a page limitation.


A. To receive credit for being a Small Diverse Business or for subcontracting with a
Small Diverse Business (including purchasing supplies and/or services through a
purchase agreement), an Offeror must include proof of Small Diverse Business
qualification in the Small Diverse Business participation submittal of the proposal, as
indicated below:

   1. A Small Diverse Business certified by BSBO as an MBE/WBE/VBE/SDVBE
      must provide a photocopy of their active BSBO certificate. A Small Diverse
      Business certified by BSBO in more than one category should indicate for which
      category it wishes its participation to be counted for program recordkeeping
      purposes.

   2. Businesses certified by the U.S. Small Business Administration pursuant to
      Section 8(a) of the Small Business Act (15 U.S.C. § 636(a)) as an 8(a) Small
      Disadvantaged Businesses must submit proof of U.S. Small Business
      Administration certification. The owners of such businesses must also submit
      proof of United States citizenship.

   3. All businesses claiming Small Diverse Business status, whether as a result of
      BSBO certification, or U.S. Small Business Administration certification as an 8(a)
      small disadvantaged business, must attest to the fact that the business has no more
      than 100 full-time or full-time equivalent employees. This can be accomplished
      by including copies of IRS Form 941s or a letter from the small diverse business
      attesting to the number of employees.

   4. All businesses claiming Small Diverse Business status, whether as a result of
      BSBO certification, or U.S. Small Business Administration certification as an 8(a)
      small disadvantaged business, must submit proof that their gross annual revenues
      are less than $20,000,000 ($25,000,000 for those businesses in the information
      technology sales or service business). This can be accomplished by including a
      recent tax return, audited financial statement or a letter from a CPA attesting to
      the annual revenues.
B. In addition to the above verifications, the Offeror must include in the Small Diverse Business participation submittal of the proposal the following information:

1. All Offerors must include a numerical percentage which represents the total percentage of the work (as a percentage of the total cost in the Cost Submittal) to be performed by the Offeror and not by subcontractors and suppliers.

2. All Offerors must include a numerical percentage which represents the total percentage of the total cost in the Cost Submittal that the Offeror commits to paying to Small Diverse Businesses (SDBs) as subcontractors. To support its total percentage SDB subcontractor commitment, Offeror must also include:
   a. The dollar amount of each subcontract commitment to a Small Diverse Business;
   b. The name of each Small Diverse Business. The Offeror will not receive credit for stating that after the contract is awarded it will find a Small Diverse Business.
   c. The services or supplies each Small Diverse Business will provide, including the timeframe for providing the services or supplies.
   d. The location where each Small Diverse Business will perform services.
   e. The timeframe for each Small Diverse Business to provide or deliver the goods or services.
   f. A signed subcontract or letter of intent for each Small Diverse Business. The subcontract or letter of intent must identify the specific work, goods or services the Small Diverse Business will perform and how the work, goods or services relates to the project.
   g. The name, address and telephone number of the primary contact person for each Small Diverse Business.

3. The total percentages and each SDB subcontractor commitment will become contractual obligations once the contract is fully executed.

4. The name and telephone number of the Offeror’s project (contact) person for the Small Diverse Business information.

C. The Offeror is required to submit two copies of its Small Diverse Business participation submittal. The submittal shall be clearly identified as Small Diverse Business information and sealed in its own envelope, separate from the remainder of the proposal.

D. A Small Diverse Business can be included as a subcontractor with as many prime contractors as it chooses in separate proposals.

E. An Offeror that qualifies as a Small Diverse Business and submits a proposal as a prime contractor is not prohibited from being included as a subcontractor in separate proposals submitted by other Offerors.
II-10. Cost Submittal. The information requested in this Part II, Section II-10 shall constitute the Cost Submittal. The Cost Submittal shall be placed in a separate sealed envelope within the sealed proposal, separated from the technical submittal. The total proposed cost shall be broken down as indicated in Appendix H, Cost Matrix. In an effort to maximize the opportunity for Offerors to price their proposals based upon their own proprietary costing methods, while ensuring that the Commonwealth can meaningfully compare pricing, costs are to be submitted in the following manner: Offerors are to propose only their total costs for each year of the contract term, including the optional renewal years, along with the completed rate card. The rate card will be included in the cost scoring. Those Offerors selected for Best and Final Offers will be required to provide a detailed breakout of their costs at that time. Detailed information presented at Best and Final Offers may include, but will not be limited to, the pricing for each of the functional service components, implementation/on boarding, licensing, maintenance/support, service support fees. These breakouts will be, or will result in, deliverables based on the provided rate card, but will not contain any time and materials based pricing. The rate card will also be used as the basis for the creation of deliverables in the future, insofar as enhancements to the CSS may be required.

Offerors should not include any assumptions in their cost submittals. If the Offeror includes assumptions in its cost submittal, the Issuing Office may reject the proposal. Offerors should direct in writing to the Issuing Office pursuant to Part I, Section I-9, of this RFP any questions about whether a cost or other component is included or applies. All Offerors will then have the benefit of the Issuing Office’s written answer so that all proposals are submitted on the same basis.

The Issuing Office will reimburse the selected Offeror for work satisfactorily performed after execution of a written contract and the start of the contract term, in accordance with contract requirements, and only after the Issuing Office has issued a notice to proceed.

II-11. Domestic Workforce Utilization Certification. Complete and sign the Domestic Workforce Utilization Certification contained in Appendix B of this RFP. Offerors who seek consideration for this criterion must submit in hardcopy the signed Domestic Workforce Utilization Certification Form in the same sealed envelope with the Technical Submittal.
PART III

CRITERIA FOR SELECTION

III-1. Mandatory Responsiveness Requirements. To be eligible for selection, a proposal must be:

A. Timely received from an Offeror;

B. Properly signed by the Offeror;

C. Provide at least one (1) reference to validate that the solution components proposed in response to this RFP are currently functional and have been in production for at least one (1) other client. Use the Appendix X Solution Component Attestation to provide verification and a wet ink signature from the referenced client(s); and

D. Have at least one (1) operational Tier 3 Datacenter with a minimum of five (5) clients hosted, functional and in production for at least one (1) year. Use the Appendix Y Datacenter Client Verification to provide verification and a wet ink signature from each of the referenced clients.

III-2. Technical Nonconforming Proposals. The four (4) Mandatory Responsiveness Requirements set forth in Section III-1 above (A-D) are the only RFP requirements that the Commonwealth will consider to be non-waivable. The Issuing Office reserves the right, in its sole discretion, to (1) waive any other technical or immaterial nonconformities in an Offeror’s proposal, (2) allow the Offeror to cure the nonconformity, or (3) consider the nonconformity in the scoring of the Offeror’s proposal.

III-3. Evaluation. The Issuing Office has selected a committee of qualified personnel to review and evaluate timely submitted proposals. Independent of the committee, BSBO will evaluate the Small Diverse Business Participation Submittal and provide the Issuing Office with a rating for this component of each proposal. The Issuing Office will notify in writing of its selection for negotiation the responsible Offeror whose proposal is determined to be the most advantageous to the Commonwealth as determined by the Issuing Office after taking into consideration all of the evaluation factors.

III-4. Evaluation Criteria. The following criteria will be used in evaluating each proposal:

A. Technical: The Issuing Office has established the weight for the Technical criterion for this RFP as 50% of the total points. Evaluation will be based upon the following: Understanding the Problem, Responsiveness to Project, Functional, and Technical Requirements, Soundness of Approach, Offeror Qualification, and Personnel Qualifications. The final Technical scores are determined by giving the maximum number of technical points available to the proposal with the highest raw technical score.
The remaining proposals are rated by applying the Technical Scoring Formula set forth at the following webpage:
http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124.

B. Cost: The Issuing Office has established the weight for the Cost criterion for this RFP as 30% of the total points. The cost criterion is rated by giving the proposal with the lowest total cost the maximum number of Cost points available. The remaining proposals are rated by applying the Cost Formula set forth at the following webpage:
http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124.

C. Small Diverse Business Participation:
BSBO has established the weight for the Small Diverse Business (SDB) participation criterion for this RFP as 20% of the total points. Each SDB participation submittal will be rated for its approach to enhancing the utilization of SDBs in accordance with the below-listed priority ranking and subject to the following requirements:

- A business submitting a proposal as a prime contractor must perform 60% of the total contract value to receive points for this criterion under any priority ranking.
- To receive credit for an SDB subcontracting commitment, the SDB subcontractor must perform at least fifty percent (50%) of the work subcontracted to it.
- A significant commitment is a minimum of five percent (5%) of the total contract value.
- A commitment less than five percent (5%) of the total contract value is considered nominal and will receive reduced or no additional SDB points depending on the priority ranking.

**Priority Rank 1:** Proposals submitted by SDBs as prime offerors will receive 150 points. In addition, SDB offerors that have significant subcontracting commitments to additional SDBs may receive up to an additional 50 points (200 points total available).

Additional subcontracting commitments to SDBs are evaluated based on the proposal offering the highest total percentage SDB subcontracting commitment. All other Offerors will be scored in proportion to the highest total percentage SDB subcontracting commitment within this ranking. See formula below.

**Priority Rank 2:** Proposals submitted by SDBs as prime contractors, with no or nominal subcontracting commitments to additional SDBs, will receive 150 points.

**Priority Rank 3:** Proposals submitted by non-small diverse businesses as prime contractors, with significant subcontracting commitments to SDBs, will receive up to 100 points. Proposals submitted with nominal subcontracting commitments to SDBs
will receive points equal to the percentage level of their total SDB subcontracting commitment.

SDB subcontracting commitments are evaluated based on the proposal offering the highest total percentage SDB subcontracting commitment. All other Offerors will be scored in proportion to the highest total percentage SDB subcontracting commitment within this ranking. See formula below.

**Priority Rank 4:** Proposals by non-small diverse businesses as prime contractors with no SDB subcontracting commitments shall receive no points under this criterion.

To the extent that there are multiple SDB Participation submittals in Priority Rank 1 and/or Priority Rank 3 that offer significant subcontracting commitments to SDBs, the proposal offering the highest total percentage SDB subcontracting commitment shall receive the highest score (or additional points) available in that Priority Rank category and the other proposal(s) in that category shall be scored in proportion to the highest total percentage SDB subcontracting commitment. Proportional scoring is determined by applying the following formula:

\[
\frac{SDB\ %\ Being\ Scored}{Highest\ %\ SDB\ Commitment} \times \frac{Points/Additional}{Points\ Available*} = \frac{Awarded/Additional}{SDB\ Points}
\]

*Priority Rank 1 = 50 Additional Points Available
*Priority Rank 3 = 100 Total Points Available

Please refer to the following webpage for an illustrative chart which shows SDB scoring based on a hypothetical situation in which the Commonwealth receives proposals for each Priority Rank:

http://www.portal.state.pa.us/portal/server.pt/community/rfp_scoring_formulas_overview/20124

**E. Domestic Workforce Utilization:** Any points received for the Domestic Workforce Utilization criterion are bonus points in addition to the total points for this RFP. The maximum bonus points for this criterion is 3% of the total points for this RFP. To the extent permitted by the laws and treaties of the United States, each proposal will be scored for its commitment to use domestic workforce in the fulfillment of the contract. Maximum consideration will be given to those Offerors who will perform the contracted direct labor exclusively within the geographical boundaries of the United States or within the geographical boundaries of a country that is a party to the World Trade Organization Government Procurement Agreement. Those who propose to perform a portion of the direct labor outside of the United States and not within the geographical boundaries of a party to the World Trade Organization Government Procurement Agreement will receive a correspondingly smaller score for this criterion. Offerors who seek consideration for this criterion must submit in hardcopy the signed Domestic Workforce Utilization Certification Form in the same sealed envelope with the Technical Submittal. The certification will be included as a contractual obligation when the contract is executed.
III-5. Offeror Responsibility. To be responsible, an Offeror must submit a responsive proposal and possess the capability to fully perform the contract requirements in all respects and the integrity and reliability to assure good faith performance of the contract.

In order for an Offeror to be considered responsible for this RFP and therefore eligible for selection for best and final offers or selection for contract negotiations:

A. The total score for the technical submittal of the Offeror’s proposal must be greater than or equal to 70% of the available technical points; and

B. The Offeror’s financial information must demonstrate that the Offeror possesses the financial capability to assure good faith performance of the contract. The Issuing Office will review the Offeror’s previous three financial statements, any additional information received from the Offeror, and any other publicly-available financial information concerning the Offeror, and assess each Offeror’s financial capacity based on calculating and analyzing various financial ratios, and comparison with industry standards and trends.

An Offeror which fails to demonstrate sufficient financial capability to assure good faith performance of the contract as specified herein may be considered by the Issuing Office, in its sole discretion, for Best and Final Offers or contract negotiation contingent upon such Offeror providing contract performance security for the first contract year cost proposed by the Offeror in a form acceptable to the Issuing Office. Based on the financial condition of the Offeror, the Issuing Office may require a certified or bank (cashier’s) check, letter of credit, or a performance bond conditioned upon the faithful performance of the contract by the Offeror. The required performance security must be issued or executed by a bank or surety company authorized to do business in the Commonwealth. The cost of the required performance security will be the sole responsibility of the Offeror and cannot increase the Offeror’s cost proposal or the contract cost to the Commonwealth.

Further, the Issuing Office will award a contract only to an Offeror determined to be responsible in accordance with the most current version of Commonwealth Management Directive 215.9, Contractor Responsibility Program.

III-6. Final Ranking and Award.

A. After any best and final offer process conducted, the Issuing Office will combine the evaluation committee’s final technical scores, BSBO’s final small diverse business participation scores, the final cost scores, and (when applicable) the domestic workforce utilization scores, in accordance with the relative weights assigned to these areas as set forth in this Part.

B. The Issuing Office will rank responsible offerors according to the total overall score assigned to each, in descending order.
C. The Issuing Office must select for contract negotiations the offeror with the highest overall score; PROVIDED, HOWEVER, THAT AN AWARD WILL NOT BE MADE TO AN OFFEROR WHOSE PROPOSAL RECEIVED THE LOWEST TECHNICAL SCORE AND HAD THE LOWEST COST SCORE OF THE RESPONSIVE PROPOSALS RECEIVED FROM RESPONSIBLE OFFERORS. IN THE EVENT SUCH A PROPOSAL ACHIEVES THE HIGHEST OVERALL SCORE, IT SHALL BE ELIMINATED FROM CONSIDERATION AND AWARD SHALL BE MADE TO THE OFFEROR WITH THE NEXT HIGHEST OVERALL SCORE.

D. The Issuing Office has the discretion to reject all proposals or cancel the request for proposals, at any time prior to the time a contract is fully executed, when it is in the best interests of the Commonwealth. The reasons for the rejection or cancellation shall be made part of the contract file.
PART IV
WORK STATEMENT

IV-1. Problem Statement and Background. During July to November 2011 the PA eHealth Collaborative Office (“eHCO”), an office within OA, initiated a stakeholder engagement process, which included more than 150 individuals representing the Pennsylvania healthcare community. Information about, and work products resulting from, that stakeholder engagement process may be found at this location: http://www.paehealthcollab.com/community_shared_svc.html. The input from that process informed Act 121 of 2012, which is designed to support existing health information exchange (HIE) networks with an overarching HIE-Network governing entity, the Pennsylvania eHealth Partnership Authority. It is anticipated that the Authority will take up the work of the PA eHCO, and will either become the signatory of the Contract resulting from this RFP, or will be the Contract’s assignee.

The HIE-Network is conceived as a network-of-networks connected by a thin layer of community shared services (CSS). The CSS services are the services/solutions being procured via this RFP as a supplier hosted solution. These services will enable secure, confidential information exchange from one certified Health Information Service Provider (HISP) to another as well as one certified HIE organization to another. Further, the CSS will support HISP to HIE and HIE to HISP exchanges. The CSS represents the suite of registries, indexing services and security functions that will create a cost-effective pathway between the various certified entities. The CSS is intended to support the common needs of health care providers, patients, HISPs, HIEs, payers, and other stakeholders by facilitating communication across entity boundaries for improved health care quality, cost and efficiency.

IV-2. Objectives.

A. General. The Commonwealth is seeking to engage a supplier to implement a Community Shared Services (CSS) to enable Health Information Exchange (HIE) across the Commonwealth. The CSS will be comprised of tools and services which will support and enable a federated model for HIE. It will include such services as a Public Key Infrastructure (PKI), security certificate services supporting HISP and HIE interoperability and testing, auditing/logging, an authoritative participant services directory, record locator service and system notifications, among others. The CSS is also expected to support and enable the interoperability between the (commercial) HISP and HIE organizations and the prospective Commonwealth internal HIE (CI-HIE), which is to be made up of several Commonwealth agencies including the Department of Health, Department of Public Welfare, etc. that store and/or use health information. To enable the interoperability with the CI-HIE, the Commonwealth will build out a proof of technology for the bidirectional flow of information between the (commercial) HIEs and the CI-HIE, using the Department of Health’s Electronic Laboratory Reporting system for the pilot. Although the strategic direction of the CI-HIE is still evolving, the Proof of Technology is a requirement of this RFP.
The diagram below shows the overarching structure of the HIE Network and its associated participants:

B. **Specific.** The vision for HIE in Pennsylvania is to strengthen the healthcare system and improve both healthcare delivery and healthcare outcomes through the timely, secure and authorized exchange of patient health information among all healthcare providers willing to participate, including those providers who serve vulnerable, underinsured and uninsured patients, those on Medicare and Medicaid, and those who live in rural and urban settings. In support of this vision, the following goals have been established:

- Pennsylvania’s HIE-Network will support the meaningful use of health information technology (as defined by the Centers for Medicare and Medicaid Services), patient-centered healthcare and continuous improvements in access, quality, outcomes and efficiency of care.
- Pennsylvania will adopt an HIE model that considers the needs of stakeholders, such as various HIE communities and Commonwealth agencies, and achieves stakeholder support to enable the use of health information technology and advance secure HIE.
- The privacy and security of all Pennsylvanians’ health information is a priority of paramount importance to the Commonwealth. Therefore, every effort will be made to address the concerns of stakeholders and patients.
- It is our objective to significantly reduce preventable medical errors, lessen the likelihood of redundant tests and procedures, support healthcare delivery innovation, and diminish overall healthcare costs.
- The HIE-Network will adhere to federal standards and specifications for exchange and will connect entities offering HIE services, integrated delivery networks, health
systems, community hospitals, providers, labs and other systems that have patient
data needed to make treatment and transition of care decisions.

The following assumptions are the foundation and principles for which the functional and
technical requirements were developed, and are considered critical to the success of the
CSS implementation:

- The CSS shall support the exchange of information across Pennsylvania certified
  HIEs, HISPs, state agencies (via the CI-HIE), integrated delivery networks,
  accountable care organizations and the federal government.
- The CSS shall provide services at the statewide level that can be performed in a more
cost-effective and efficient manner than at the individual local HIE level.
- The CSS shall support a federated architecture of the HIEs in the Commonwealth.
- The CSS shall not unnecessarily duplicate the services and functions of the local
  health information exchanges.
- The CSS shall not store clinical or claims data.
- The CSS shall support all exchanges securely over the internet via standards based
  internet support protocols (HTTPS, WS-* , SOAP, SAML, etc.)
- The CSS shall be appropriately secured to meet all applicable state and federal laws.
- The CSS shall support all functional and technical requirements as defined in this
  RFP to fulfill the vision of the Strategic Plan as refined by the Participant Workgroup.
  The Strategic Plan can be found at:
  http://www.paehealthcollab.com/general_info.html


A. Project Scope. The scope of services of this RFP is to provide the technical and support
services necessary to fulfill the aforementioned Objectives, which are built in large part
upon Act 121 of 2012. This Scope includes, but is not limited to, the following:

- Develop and maintain a directory of health care provider’s contact information to
  enable participants to share health information electronically.
- Develop and maintain standards to ensure interoperability.
- Develop and maintain a registry of patients choosing to opt out of the health
  information exchange, and procedures to re-enroll into the health information
  exchange

The Project Scope includes managing and fulfilling the technical and support service
requirements associated with Project change, growth and enhancement.

It is important to note that all clinical data will reside within the source of origin. The
CSS shall not store clinical data, nor shall it store any data beyond the minimum
necessary to support CSS functionality. Use cases have been developed and are included
in Appendix V.

B. Affected Organizations. There are approximately nine (9) local/regional HIEs in the
Commonwealth: Allied Health Information Exchange Company (AlliedHIE), Clinical
Connect, HealthShare of South Eastern Pennsylvania, Highmark Health Information
Exchange, Keystone Health Information Exchange (KeyHIE), Lehigh Valley Health Network, St. Luke’s University Health Network, Vale-U-Health and Vantage Health Information Exchange. Most of the HIEs are in the planning and start-up phase. Five of these HIEs (AlliedHIE, Clinical Connect, KeyHIE, St. Luke’s University Health Network and Vantage HIE) have existing operational HIE systems. Two are currently implementing HIE technology and planning to be live in 2012 (Highmark HIE and Vale-U-Health).

Most of the HIEs have prioritized meaningful use functions as their start-up functionality, such as clinical summary exchange, lab results delivery/exchange and secure clinical messaging. Multiple HIEs will be providing Health Information Service Provider (HISP) services.

All HIEs currently support or envision being the conduit for delivering clinical results and reports to ordering providers’ electronic health record (EHR) systems as well as facilitating summary document (or continuity of care document (CCD)) exchange. Most HIEs will be phasing in the capability to query the exchange for historical patient information.

Connecting to CSS services will be entirely in the discretion of individual entities. All HIEs indicated that they plan to connect to the CSS for patient privacy management. Connecting for other services will be dependent upon the affordability of a set of common services including (but not limited to) directory services, patient consent management, and cross-boundary exchange (inter- and intra-state connectivity).

The Commonwealth Internal HIE (CI-HIE) is also in the planning phase, and is to be made up of the following state agencies:

- Department of Health
- Department of Public Welfare
- Department of State
- Department of Corrections
- Department of Labor and Industry
- Department of Military and Veterans Affairs
- PA Board of Probation and Parole
- PA Department of Aging
- PA Insurance Department
- PA Department of Education
- Justice Network

The CI-HIE is expected to support health information exchanges across state agencies and is conceived to provide an HIE-like gateway connection to the HIE-Network (via CSS) to allow providers and HIEs access to state resources for both consumption of those resources where appropriate and permissible (e.g., registry information), and for reporting purposes.
PA Certified HIE-Network Participants ("Participants") are those entities that have been certified to meet all of the required technical and operational standards set forth by the eHCO. Individuals authorized to access information and services from the CSS will be members of a Participant organization, regardless of size or functionality. For example, a physician (or his/her authorized staff) may have a need to report to and/or query data from the CSS. His/her access will be accomplished via his/her membership in a Participant organization. This relationship will ensure the integrity of the HIE-Network’s trust framework, data, and patient privacy.

Additionally, patients will have secure web-enabled access to the CSS in order to manage their privacy preferences as well as to request an audit report from the HIE-Network.

C. **Constraints.** In order for the Authority to support and maintain the CSS, financial sustainability is critical. The current financial model focuses on the collection of fees from the CSS Participants. Therefore, cost optimization must be considered a priority for all of the RFP requirements.

**IV-4. Requirements.**

A. **Project Requirements.** As part of its response, Offerors must describe their level of familiarity in performing project management in accordance with PMBOK best practices.

1. **Project Management.** The management of this project is expected to be a shared responsibility between the selected Offeror and the Commonwealth Project Manager, with final authority resting with the Commonwealth. Offerors must propose a detailed project management approach that aligns with the eHCO’s project charter (see Appendix J) with the following items/documents, at a minimum, included in their RFP response:

   a. **Responsibility Matrix/RACI Chart.** Offerors must propose a responsibility matrix/RACI chart listing all major project activities along with who will be responsible.

   b. **Governance Structure.** The Authority’s governance structure is included as Appendix K. Offerors must propose their governance structure. Where staff have not yet been named, please provide a job title instead.

   c. **Detailed Project Work Plan/Work Breakdown Structure.** Offerors must propose a detailed work plan depicting all project tasks with estimated start and completion dates, work products and deliverables, task dependencies, and assigned resources. This plan must also highlight the critical path to project completion. Please submit this in Microsoft Project 2007 format. For purposes of your response, assume a project start date of March 1, 2013. The actual start date will be dependent upon the date of Contract execution.
d. **Change Management Plan.** A change management plan template is included as Appendix L, along with a Change Request Form Template as Appendix M. Offerors may accept these formats, suggest changes to the formats, or propose different formats. Provide an explanation for suggested changes, or the reason for using a different format entirely. Also, provide a narrative description of your approach to change management.

e. **Risk Management Plan.** A risk management plan template is included as Appendix N. Offerors may accept this format, suggest changes to this format, or propose a different format. Provide an explanation for suggested changes, or the reason for using a different format entirely. Also, provide a narrative description of your approach to risk management.

f. **Communication Plan.** A communication management plan template is included as Appendix O. Offerors may accept this format, suggest changes to this format, or propose a different format. Provide an explanation for suggested changes, or the reason for using a different format entirely. Also, provide a narrative description of your approach to communication. Address the communications necessary to provide a feedback loop for evaluation and assessment of systems functionality and opportunities for improvement.

g. **Requirements Management Plan.** A requirements traceability matrix template is included as Appendix P. Offerors may accept this format, suggest changes to this format, or propose a different format. Provide an explanation for suggested changes, or the reason for using a different format entirely. Also, provide a narrative description of your approach to requirements management.

h. **Alignment with ITIL v3.** The selected Offeror must use ITIL v3 processes to manage the delivery of the services provided. This includes ensuring that all staff hired by the selected Offeror are at least ITIL v3 foundations certified – copies of ITIL v3 certificates must be provided to the Commonwealth within six months of an employee’s hire date. This requirement also applies to any sub-contractors hired by the selected Offeror. In addition, team leads assigned to this project must have ITIL v3 Expert Certification. For the purposes of any contract which may result from this RFP, the selected Offeror must implement and report on rollout of the following ITIL processes to meet the requirements of this statement of work:

- Service Level Management
- Availability Management
  - Specifically, the Contractor will need to specify how it will manage planned downtime to implement required patches and maintenance.
- Financial Management
- Capacity Management
- Access Management
- Information Security Management
- Incident Management
- Change Management
- Problem Management
- Configuration management
- Release & Deployment Management
- Service Operation
- Continuous Service Improvement

i. **Annual Planning.** To ensure that the CSS implementation project remains on schedule and accommodates the functional services required at each phase, the Commonwealth and the selected Offeror will hold annual planning sessions. These sessions are designed to review the previous year’s work, outline lessons learned, and to further detail the project plan for the upcoming year. Offerors must describe their approach to these planning sessions, including timing, personnel required, and critical outcomes. The annual planning sessions will not preclude the ability to approach the implementation in an agile methodology. The ongoing iterative processes and related management are separate from the annual planning.

2. **Project Reporting**

   a. **Task Plan.** As part of the project initiation activities (preferably within 30 days of contract execution), the selected Offeror will be required to update the proposed project work plan submitted in response to this RFP (preferably in Microsoft Project 2007). This represents a plan for each task that identifies the work elements of each task, the resources assigned to the task, and the time allotted to each element and the deliverable items to be produced. Where appropriate, a PERT or GANTT chart display should be used to show project, task, and time relationship.

   b. **Status Report.** The selected Offeror will be required to submit weekly progress reports covering activities, problems and recommendations throughout the implementation period of this project. During the annual planning sessions, it may be decided to change this to a monthly status report if approved by the Commonwealth and the selected Offeror. These reports should be keyed to the work plan the Offeror developed in its proposal, as amended or approved by the Commonwealth Project Manager.

   c. **Incident Report.** The selected Offeror will be required to submit an “as required” report, identifying incidents. The report should describe the incident and its impact on system usability and/or functionality. This report must be delivered to the Commonwealth within one hour of when an incident occurs. Updates must be provided every two (2) hours for critical incidents until the incident is resolved to the satisfaction of the Commonwealth. This report must be tied to both your Risk Management Plan and your Change Management Plan. An incident reporting template is included as Appendix Q. Offerors may accept this
format, suggest changes to this format, or propose a different format. Provide an explanation for suggested changes, or the reason for using a different format entirely. Also, provide a narrative description of your approach to incident management.

d. Performance Reporting. On an ad hoc basis, the selected Offeror may be asked to provide performance related reporting as required by Act 121 of 2012 as well as requirements related to ARRA funding.

e. Meetings. The selected Offeror is required to meet with the Commonwealth’s Project personnel, or other designated representatives, to resolve technical or contractual problems that may occur during the term of the Contract. Meetings will occur as problems arise and will be coordinated by the Commonwealth Project Manager. The selected Offeror will be given reasonable and sufficient notice of meeting dates, times, and locations. Face to face meetings are desired. However, at the selected Offeror’s option and expense, and with the approval of the Commonwealth, a conference call meeting may be substituted. Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Contract.

f. Deliverable Walkthroughs. To promote effective Deliverable submission, review, and sign-off, the selected Offeror will facilitate sessions for early, informal reviews of interim Deliverables between selected Offeror Project team leaders and Commonwealth project staff. This technique will allow deficiencies to be identified and corrected early in the process, ultimately conserving time and resources. It also helps to maintain quality; by the time a Deliverable reaches the formal review stage it has already undergone much scrutiny. This approach provides a high level of confidence in the Deliverable’s accuracy. By Deliverable signoff time, the Commonwealth’s project staff will be familiar with the Deliverable through ongoing evaluation.

3. Initiation. Offerors must propose their approach to project initiation, including resources and length of time, approach to collaboration, kickoff meeting participation, and goals.

4. Development. Describe process for determining system configuration specifications, and anticipated time to system readiness. For any portions of your response which require software development, configuration and/or customization, the following information shall apply. Design work associated with custom development, configuration and customization is expected to be iterative, meaning it will be repeated for each release and/or project phase. See Appendix R Priorities, Phasing and Pilot Participants, for a breakdown of the services required for each phase and their associated timing. In response to this requirement, provide the following, at a minimum:
a. **Requirements Gathering.** Describe your proposed requirements gathering process, including expectations of the Commonwealth project team, timeframe needed for completion, and any other resources needed for successful delivery.

b. **As-Is Documentation.** Where appropriate, describe your approach to define the as-is process, including expectations of the Commonwealth, HISPS, HIEs, etc.

c. **To-Be Documentation.** Describe your proposed to-be process, including expectations of the Commonwealth, HISPs, HIEs, etc.

d. **Gap Analysis.** Describe your proposed gap analysis process, including expectations of the Commonwealth, HISPs, HIEs, etc.

e. **General Systems Design.** Describe your approach to building the General Systems Design (GSD) including staffing and hours, Commonwealth participation (along with any other resources necessary), review and validation, and acceptance criteria.

f. **Detailed Systems Design.** Describe your approach to handing off the GSD to a Detailed Systems Design (DSD) team, including reviews and walkthroughs, staffing and hours, Commonwealth project team participation, and acceptance criteria. Describe the DSD process, including participation and staffing levels, review and validation, and acceptance criteria.

g. **Build.** Describe your approach to building each release for deployment to the test environment. Include, at a minimum, review and validation of requirements and use cases as needed, interaction expected with the Independent Verification and Validation (IV&V) Contractor, Commonwealth and HIE project team reviews and participation, staffing levels and hours, and acceptance criteria to be met prior to deployment to the production environment.

5. **Delivery**

a. **Execute** - Offerors must propose a strategy to deploy the release into the testing environment and, if testing and training (if needed) are completed and fully approved, certify the release as ready for use. Describe how, upon successful completion of testing and training, the release will be deployed to the production environment. Also address the feedback mechanism to support lessons learned.

b. **Test** - Describe your approach to testing the release including, at a minimum, the following:

- Interoperability Testing
- Regression Testing
- Penetration Testing
- Vulnerability Testing
- Load Testing
- User Acceptance Testing

The selected Offeror must provide a test environment in which all functionality will be fully tested prior to deployment in the production environment. Prior to testing, the selected Offeror will develop test cases for any functionality to be deployed. Test cases will be developed collaboratively with the IV&V Contractor (should the Commonwealth select an IV&V Contractor), with final approval resting with the Commonwealth. All testing must be approved by the Commonwealth Project Manager before the functional release can be migrated to production. Sign off by both the selected Offeror's Project Manager and the Commonwealth’s Project Manager will indicate that the release is certified as ready for use.

Any patches or changes to functions must be fully tested prior to deployment in the production environment. Additionally, the selected Offeror shall test the connectivity and interoperability of all approved entities with the CSS. While it is not the selected Offeror's responsibility to solve the technical problems on the entity's side that prevent it from connecting to the CSS, the selected Offeror shall provide any available testing feedback (including problem or failure notification and resolution and/or facilitation) to the entity that will facilitate the connectivity. The selected Offeror will also be required to provide, in the same environment, a "sandbox" for certification testing (and re-certification) of HIEs and HISPs.

c. **Training** – Describe your approach to training Commonwealth Staff as well as HIE staff. Offerors must provide the numbers and types of HIE and Commonwealth staff to be trained, with the understanding that Commonwealth staff numbers approximately 15. Assume the Commonwealth will provide training locations. Include a list of all training required, including technical training, business and administrative training, etc to support your proposed solution. Offerors must include in their proposal the approach, which may include but not be limited to classroom based training, virtual training, etc. Offerors will be required to deliver all training materials to the Commonwealth. The selected Offeror will be required to provide hard copy training materials at training sessions.

6. **Support**

a. **Maintenance and Support** - Once a release has been successfully moved into production, the selected Offeror will be required to warranty the release for a period of 90 days, after which it will move to a maintenance and support phase. Describe your approach to maintenance and support, including your approach to bug fixes, performance optimization, storage and capacity requirements, backups, support services, and refresh schedules.
b. **Enhancements** - The selected Offeror shall be responsible for the project management, development, testing, and implementation of system enhancements upon request of the Commonwealth. System Enhancements will include the addition of any feature or function within the Project Scope but not specified in this RFP which is requested by the Commonwealth and that has not been mandated. Any changes mandated by Federal, State, or local regulations will be considered maintenance and support and not an enhancement. All other system maintenance activities as described in section IV-4.A.6 Maintenance and Support shall be included as part of maintenance and support and will not be considered a system enhancement. System enhancements will be performed as deliverables negotiated based upon the rates specified in the rate card in Appendix H, Cost Matrix.

c. **Disaster Recovery** - Describe your approach to providing disaster recovery and/or backup services for this project. The approach must support 24 x 7 x 365 availability. For further details, see Appendix S Hosting Requirements.

d. **Service Support.** Describe your approach to providing product, service and datacenter support for Participants and Commonwealth staff which meets the SLAs in Appendix T. Include staffing levels, definition of service tiers and support levels, and escalation processes.

e. **Service Level Agreements** - The Commonwealth has drafted Service Level Agreements (SLAs) for this project, which are attached to this RFP as Appendix T. Offerors must propose assuming the applicability of Service Level Agreements in Appendix T, however, Offerors are invited to propose additions and alterations to Appendix T for Commonwealth consideration. Offerors will describe individual SLAs that establish minimum operating and availability metrics for all services. It is expected that multiple service tiers and associated service levels will be provided within each service offered.

7. **Turnover**

a. **Turnover and Turnover Plan.** Describe your approach to transitioning the services at the end of the contract to either Commonwealth project staff or their designee(s). Include, at a minimum, staffing levels with roles and hours, Commonwealth or Contractor roles, hours, and skill sets, materials necessary, length of time to complete, and acceptance criteria. Consideration must be given to ensuring continued operation and services, without disruption, during the turnover period. The turnover plan shall include, as applicable:

1) Responsibilities by resource for operational support during the turnover services period.
2) Identification of any deliverables that have not been delivered, that have been delivered but not accepted, or that have been rejected, and a proposed resolution for all such identified deliverables.
3) A list of detailed documentation about the technical infrastructure and applications to be provided during the transition services period to support ongoing support and maintenance of the CSS. Include provision for delivery of all documentation, configurations, design assumptions, manuals, business logic and other such informational records necessary for continued operation of the CSS.

4) A work plan for each stage of the transition services.

5) Plans for coordination and transition of specific responsibilities from the selected Offeror to the Commonwealth or its designee.

6) Application and technical service support.

7) A list of operational statistics to be provided during the transition services period, including resource consumption, system performance, and application activity in both aggregated and trended forms.

8) An inventory of third party products for which the licenses will be transferred (if applicable) from the selected Offeror to the Commonwealth or its designee. This inventory shall be delivered together with full executed copies of all license agreements and assignments therefore acceptable to the Commonwealth or its designee.

9) Any work in process or to be performed under any work order in operation at the time the Commonwealth requests transition.

10) Return of Commonwealth data & other property; and destruction and verification for confidential records, software, scripts.

In addition, the turnover plan will, at a minimum, specifically provide for turnover of the following functions to the Commonwealth or its designee:

1) Training Support - Knowledge and Process Transition
2) Project Management Support: Knowledge and Process Transition, Management Tool Transition.
5) Training
6) Production Hardware Infrastructure Transition: Server Based systems, Network Based systems, Database systems, Web Based systems, Data Migration.
7) Development Environment Hardware Infrastructure Transition: Server Based systems, Network Based systems, Database systems, Web Based systems.
8) Data Migration
9) Hardware Infrastructure Test Plan
14) Operations Transitions

b. **Closeout.** Describe your project closeout approach, including a final report which must be submitted to the Commonwealth as part of the project closeout activities. The final report must be submitted in draft form for Commonwealth approval prior to final submission. At a minimum, the final report must include the following:

1) An abstract or summary of the project services, goals, and accomplishments presented in a way that will be meaningful to management and others only generally familiar with the subject area.
2) A description of the methods used during the project to ensure success, cost savings and efficiencies realized as a result of the initiative.
3) A summary of the goals and objectives of the project, stating how well each was met, including completion of activities within time, budget and scope.
4) A summary of the service level agreements used for this project, including any changes made, how often and why any service levels were not met, and any actions taken to correct missed service levels.
5) A summary of lessons learned during this project, including how the procurement process could have been improved to further ensure project success, level of success of communications, risk and change management, and effectiveness of the project management approach between Contractor and the Commonwealth.

**B. Functional Requirements.** The CSS represents the suite of registries, indexing services and a trust framework that will create a cost-effective pathway to support the common needs of health care providers, patients, HISPS, HIEs, payers, and other stakeholders by facilitating communication across entity boundaries for improved health care quality, cost and efficiency.

CSS services may be accessed via web-based services or through interfaces between the CSS and Participants. Web-based services primarily support secure patient access to manage their privacy preferences as well as request audit reports. Participants will be required to connect to the CSS based upon a set of standard interfaces to support the exchange of information in a bi-directional manner with the CSS. This connectivity supports automated reporting to and discovery from the CSS to support automated interaction between the CSS and Participants, and their members.

The CSS services are broken into two sets: core and menu. The core services are intended to be those services which form the framework of the CSS, and will be offered to the Participants as part of a package deal. The menu services are those services which some,
but maybe not all, of the Participants may select based on their needs, lower operational costs, and/or maximum value.

The functional requirements have been separated into service components for ease of description. Your response should consider these requirements, but also allow for some of the components to be combined if doing so will provide for a more efficient and effective solution at a lower cost. Responses must outline how these services may evolve over the course of the five year base contract and beyond, into the optional years, if exercised. For a breakout of the timing/phase in which each of these requirements will need to be met, please refer to Appendix R, Priorities, Phasing and Pilot Participants.

**B.1 Core Services.** CSS core services create a foundation for Participants to exchange health information. Core services support them so that they can:

- Identify and locate each other and their authenticated users in a trusted environment;
- Enable the reconciliation of the identity of the individual patient to whom the information pertains;
- Exchange information in a secure manner that supports both authorization decisions and the appropriate logging of transactions;
- Patient self-registration and administration and management of their ability to deny access to their information;
- Establish relationships among providers, patients and their data;
- Facilitate the provision of HIE-Network-wide audit reporting; and
- Measure, monitor and report system performance and service levels.

Core services will also support both push and pull transactions. Push transactions enable provider messaging and referrals; and pull services use indexing services to support query and retrieval of patient and clinical information across multiple and disparate sources of data.

The Authoritative Participant Services Directory (APSD) is a critical portion of the functional requirements for the CSS. It manages the authentication, authorization and account administration of the HIE-Network. It also identifies relationships between all users and related health care entities. The APSD amalgates and augments the functions of a Provider Directory and a CSS Level Master Patient Index (MPI); and enables interfaces among other functions to include, for example, Record Locator Services, and Patient Consent Services. The APSD includes the following services, described in more detail below:

- Federated Trust Services
- Batch Upload and Download
- Patient Privacy Management Services
- White Pages Look-up
- Patient Discovery
- Profile Management
- Provider Directory Services
- Individual Level Provider Directory
Entity Level Provider Directory

a. **Federated Trust Services.** Federated Trust Services is a set of processes that make identity and authentication portable across disparate security domains and provide support for a universal set of identity attributes which should make a Participant recognizable and acceptable to all HIE-Network systems and Participants. To facilitate federated trust services, a set of published assurance criteria and common protocols for sharing identity information must be defined. The identity trust service of the CSS will enable the trust of multiple identity managers within the Participants who will be facilitating access to CSS services. The federated trust will provide local autonomous HIEs the ability to make local policy access decisions based upon their independent governance models. This process supports and includes multi-level mapping to define and establish trust – at the domain and individual level, not only within an HIE but also between the HIE and the CSS and by implication within the HIE-Network. This process will therefore also support extended attribute functionality that will be shared between the HIE and the CSS to allow the CSS to keep track of and identify who is authorized to which services and at what type of access level.

2. **Public Key Infrastructure.** The security infrastructure must be fully interoperable among all components of the CSS. These services will include the Certificate Authority (CA), the Registration Authority (RA), the supporting directories (DNS, LDAP), and the Identity/Profile Management. All components must fully integrate with the Profile Management. In essence, the main objective is to promote secure interoperability with the following stakeholders that will interact with the CSS:
   - All HIE or HIE-like certified entities that participate in the HIE-Network
   - All HISP or HISP-like certified entities that participate in the HIE-Network
   - The NwHIN gateway
   - The CI-HIE gateway
A dependable and reliable ecosystem of trust within the HIE-Network predicates on a strong security infrastructure that needs to be in place. Such infrastructure will support a diverse array of different security services such as, but not limited to:
   - Identity/trust verification
   - Certificate validation
   - Certificate signing
   - Certificate revocation
   - Authenticating and validating users
   - Registering and on-boarding users
   - Assigning certificates to users
   - Discovering certificates
The security infrastructure and services must support both HISP (DIRECT Project) as well as HIE (NwHIN) security protocols and services.

3. **Master Patient Index (MPI).** The MPI contains a list of patients and unique identifiers for each patient who has received services, which are available in any of
the local HIEs. Each local HIE is expected to maintain a local MPI. The CSS level MPI supports patient discovery and privacy management services. Using the patient identifier information located in the CSS level MPI, a provider can locate a patient’s identifier number and use this to submit a request via their EHR system to locate and retrieve a patient’s health records (i.e. clinical summaries) which are located in the HIE-Network.

4. **Reporting Registry.** The overall goal of the Commonwealth’s Evaluation and Performance Framework is to assess adoption and use of various components of the HIE program, measure perceived value by various participants, and to analyze cost and quality impact of Commonwealth initiatives. The CSS Reporting Registry supports these goals by providing a centralized mechanism whereby all Participants can submit reports that contain the necessary data and information to support this Framework.

5. **Federated Audit Reporting and Logging.** In accordance with HIPAA, all Participants and the CSS must maintain a log of audits that identifies users who have viewed a patient’s data. These audits must be made available to patients upon request. The HIE-Network seeks to streamline this process by making the CSS the centralized point for responding to patient audit requests. Therefore, the CSS must have a federated audit reporting and logging function by which it can make a request to all Participants to return a standardized accounting of disclosures for a given patient’s record at any Participant.

6. **Batch Upload and Download.** This function will allow an authorized directory administrator or user the ability to batch upload or download a list of records. For uploads, this function would require a standard upload name-value pair format and will manage data validation and duplicate entries. For downloading, this function will provide the data in a standard downloadable format.

7. **Record Locator Service.** The Record Locator Service (RLS) is the application component that uses a Document Registry to receive and store information regarding the location of a particular set of data and/or reports on a given patient identified in the MPI. The RLS’ Document Registry does not contain clinical data. It receives key identifier information (i.e. MPI patient identifier and unique record location) about new or updated patient records created by Participants. In the CSS, this service allows authenticated and authorized providers who participate in Participant organizations to determine the existence and location of patient documents from the source. Therefore, this service must also be able to support extended attribute functionality to allow the Profile Management service to correlate requestors’ profiles with access authorization.

8. **Patient Opt-Out Registry.** The patient Opt-Out Registry supports the HIE-Network privacy framework and Patient Privacy Management Services. This registry stores the denial of release request form that has been registered by the patient or on the patient’s behalf by a provider. The database also must support the immediate
termination of the request for denial upon the patient’s request to cancel the denial (i.e. their previously registered opt-out request).

9. Patient Privacy Management Services. Patient privacy management services support the enforcement of the HIE-Network’s privacy policy with regard to patient’s ability to decline their information from being shared in the HIE-Network. Patients may choose to “opt-out” or “deny release” of their health information within the HIE-Network. Doing so “hides” all of their data from query viewing by any Participant. The patient’s privacy preferences are stored in the Patient Opt-Out Registry. Every time the CSS receives a request for either opt-out or cancellation of opt-out it will notify the patient.

Both providers and patients will have the capability to register in a secured website, become authenticated, and register a denial of release or cancel a denial of release. If the patient chooses to deny release of their data in the HIE-Network before they have been identified in the CSS level MPI, the Commonwealth must have the capability to manually enter a patient record in the CSS level MPI in order to support the denial of release. Such cases will need to be processed by the Commonwealth according to a set of defined procedures.

It must be noted that at no time shall an opt-out request hinder or prevent the continued storing and recording within the CSS Document Registry (managed and maintained by the RLS) of documents’ index references (key identifier information) pertaining to the opted out patient.

a. Processing Denial of Release Form. Denial of release may be logged in any of four ways:

1) **Provider Initiated - Automated:** Provider receives patient authorized request to deny access to their PHI and logs into a secure website (in which he/she has been previously authenticated through the federated trust framework) and enters the denial which is saved in the Opt-Out Registry. The electronic submission must include an attestation that the provider received a signed form from the patient or the patient’s authorized representative and has provided a copy to the patient for his/her records; or

2) **Provider Initiated - Manual:** Provider receives patient denial request and submits the signed denial form to the Commonwealth; Commonwealth staff enter the denial into the Opt-Out Registry; or

3) **Patient Initiated – Automated:** The Patient (or the patient’s authorized representative) logs into a secure website, registers and is authenticated (using two-factors). Once authenticated and securely logged in, the patient registers a denial of release to prevent access to their personally identified health information in the HIE-Network. The denial is saved in the Opt-Out Registry and makes the patient’s personally identified health information unavailable for query viewing across the HIE-Network; or
4) **Patient Initiated – Manual:** Patient completes and signs the denial of release form and sends to the Commonwealth; Commonwealth staff enter the denial in the Opt-Out Registry.

b. **Patient Discovery and Opt-Out.** All queries for personally identified health information to or from any Participant must first identify the patient’s opt-out status via a query of the CSS Opt-Out Registry. If a patient has registered a denial of release, the query will result in a denial of access to any patient identifiable information from any HIE-Network domain. A standard message, as defined by the Commonwealth, will be returned to the requestor for denial of access.

c. ** Cancelling a Denial of Release.** A patient may choose to cancel their denial of release and therefore allow query viewing of their health information by any HIE-Network Participant’s authenticated and authorized user. The cancellation may be completed in any of the following ways:

1) **Provider Initiated – Automated:** Provider receives the authorized cancellation of denial release and in order to immediately access the patient’s data they enter the cancellation into the secure website, which logs the cancellation in the Opt-Out Registry. The electronic submission must include an attestation that the provider received a signed form from the patient (or the patient’s authorized representative) and has provided a copy to the patient for his/her records; or

2) **Provider Initiated – Manual:** Provider receives patient cancellation request and submits the signed form to the Commonwealth; Commonwealth staff enter the denial cancellation into the opt-out registry and notify the patient; or

3) **Patient Initiated – Automated:** If the patient registered with the CSS to complete the denial, then those credentials can be used to cancel the denial of release. If the patient used a manual process or their provider to submit the denial of release, then the patient must first register, be authenticated and gain log-on credentials. The patient then logs into a secure website using their login credentials and cancels the denial of release of their data. The automated process must be followed by receipt of the patient’s signed cancellation of denial of release by the Commonwealth within a predetermined timeframe; or

4) **Patient Initiated – Manual:** Patient (or authorized patient representative) completes the cancellation of opt-out form and sends the signed form directly to the Commonwealth; Commonwealth staff enters the denial cancellation into the opt-out registry and notifies the patient.

10. **White Pages Directory Lookup.** White Pages Directory Lookup provides a subset of the Provider Directory Services Individual Level Provider Directory (ILPD – see
below) and offers early phase CSS functionality that makes it easier for Participants to locate and validate DIRECT email addresses. This lookup service will provide an API that will allow authorized Participants (HISPs as well as HIEs) access to the following user and system functions:

a. Global Address List for Web Mail provides DIRECT email users with the basic search function to locate and validate other DIRECT users via first name, last name, organization or DIRECT email based lookup.

b. Locate/Validate User Endpoint interoperates with different mail solutions (DIRECT, Web mail, and EHR) to enable the CSS global address list function to locate a user’s valid DIRECT email address using a number of different user search fields.

11. Intra-Network Capabilities Directory. The Intra-Network Capabilities Directory serves as the white pages of Participants and their capabilities for exchanging data. This directory is a subset of the Profile Management Services and supports the exchange of data across disparate security and participant domains and utilizes the federated trust framework to support health information exchange between and among Participants.

12. Patient and Document Discovery. This service in the CSS allows authenticated and authorized users within Participant domains to determine the existence of a patient at any HIE-Network domain. A query to the CSS by a trusted and authorized user leverages the RLS to return a list of documents and its electronic “location” for the given patient who has been previously identified in the CSS level MPI and who has not registered a denial of release. The document list includes a link or pointer to the source of the data. The user may then view selected documents via the link/pointer and import or download for display or import needed information into their own electronic health systems. This service must also be able to support extended attribute functionality to allow the Profile Management service to correlate requestors’ profiles with access authorization to prevent inadvertent access to flagged (sensitive) documents that the requestor may not be privy to view. The service must be able to support returning a denial of release message.

13. Patient Directed Audit Report Request and Viewing. All Participants and the CSS must maintain a log of audits that identifies users who have viewed and/or accessed a patient’s records. These audits must be made available to patients upon request. The HIE-Network seeks to streamline this process by making the CSS the centralized point for responding to patient audit requests. Therefore, the CSS must have a federated audit reporting and logging function by which it can make a request to all Participants to return a standardized accounting of disclosures for a given patient’s records at any PA Certified HIE-Network Participant.

14. Authoritative Participant Services Directory (APSD) – The APSD is encapsulated by Profile Management Services, which uses and/or harmonizes a number of
directories and services. The Profile Management Services is the fabric and glue that allows applicable subordinate services and directories of the APSD to work together in a seamless fashion, when and as needed. The Profile Management Services supports individual and entity level matching and resolution of data received from multiple data sources, validates the accuracy of participants’ data, positively identifies and certifies the individual or entity, stores DIRECT addresses, and cross-references data from disparate sources. It supports the creation and maintenance of individual to entity relationships as well as seamless interoperability with other directories external to the APSD, such as the State Board of Licensing, local HIEs and HSPs, the PA Medical Society, etc.

15. Provider Directory Services. The Provider Directory is a subset of the APSD and, under the direction of the Profile Management, maintains a collection of registered provider and entity addresses and exchange information, such as port information, formats supported, security credential locations, etc. Important components of the Provider Directory Services are the:

1. **Entity Level Provider Directory (ELPD).** The ELPD supports a federated exchange, discoverability of the entity as well as of information exchange capabilities (i.e., CCD, HL7, etc.) and security credentials. The ELPD consists of the following entities/users: health care provider organizations (i.e. hospitals, clinics, nursing homes, pharmacies, labs, etc.); other health care organizations (i.e., health plans, public health agencies); health information organizations (i.e. regional HIE organizations, health information service providers); and other organizations involved in the exchange of health information (business associates, clearinghouses).

2. **Individual-Level Provider Directories (ILPD).** The ILPD supports federated exchange and discoverability of an individual provider, the individual provider’s practice location(s), associations with entities and their security credentials. The ILPD will “communicate” through the profile management services with the ELPD for basic information regarding the relationship with entries in the ELPD and the exchange capabilities of the entity under which the individual provider is affiliated.

3. **Provider Verification Services.** A subset of information in the Provider Directory shall include information that can assist Participants with authenticating and authorizing providers to access patient information within the Participant’s organization, which is an important component in ensuring CSS federated trust. Having a streamlined mechanism to obtain information in support of the provider verification processes will provide a common set of information, including professional licensing status (suspension or sanctions), and potentially, credentialed provider lists from other sources such as health plans and hospitals/health systems.
B.2 Menu Services. Menu services are those functions that can be provided by the CSS to minimize operational costs and maximize value to Participants. These services may be purchased from the CSS if they add value to the Participant.

1. Public Health Services. Public health services is conceived as making available data from public health systems through the CSS. This function will support the capability of a participant to submit, query and view (as appropriate) specific patient data via the CI-HIE, such as that of the State’s Immunization Registry or Newborn Screening Program. This functionality will be heavily dependent upon the CI-HIE’s ability to establish gateway services to support the bi-directional flow of information.

To accomplish this, a proof of technology will be required for the CI-HIE gateway that supports the bi-directional flow of information. This will require an assessment of Public Health Indexing and Public Health Reporting. This service will stand up the communication between the CI-HIE and the Participants, with the PA Department of Health’s Electronic Laboratory Reporting (ELR) System as the test application. This service must be scalable, and if it is successful, must be capable of building out separately to support the CI-HIE in a later phase and under a separate procurement to support the additional public health services needs. This solution will be a reusable prototype, and will be considered a developed work. Specific information on the current DOH data formats and standards for the ELR System is contained in Appendix U, PA Department of Health Electronic Laboratory Reporting Guidelines. This gateway must be standards based and support efficient and effective interoperability for all Participants’ native systems, including RODS (a disease surveillance and reporting system), PA-HAN (Health Alert Network), Cancer Registry and Immunizations. Applicable standards and requirements vary according to each program area and their respective data.

2. Provider Coordinated Patient Privacy Management. The Core Service for Patient Privacy Management allows a provider to log into a secured website to support a denial of release or cancellation of denial of release upon a patient's request. This value-add service supports Participants who wish to offer providers the ability to remain in their native environment and/or Participant system to complete the patient requested denial of release or cancellation of denial of release. The Participant then passes this transaction, including attestation of a signed form, to the CSS to populate the registry.

**Automated Denial of Release:** Provider receives patient request to deny access to their PHI and in his/her native system, enters the denial, which is passed to the Opt-Out Registry via a Participant. The electronic submission must include an attestation that the provider received a signed form from the patient and has provided a copy to the patient for his/her records.

**Automated Cancellation of Denial of Release:** Provider receives the cancellation of denial of release and in order to immediately access the patient's data, he/she enters the cancellation into their native system, which sends the cancellation notice to the
Opt-Out Registry. The electronic submission must include an attestation that the provider received a signed form from the patient and has provided a copy to the patient for his/her records.

3. **Inter-Network/NwHIN Communications Gateway.** The gateway enables trusted communication, utilizing the federal trust framework and standards, to support health information exchange with the federal government and with HIEs residing across state lines and/or outside the HIE-Network.

4. **Provider Look-up and Referral Requirements Discovery (Transitions of Care Facilitation).** Supported by the APSD, the referral component enables transitions of care and allows providers to select the provider to which he/she wishes to send a patient referral. The referral may be electronically generated allowing the provider to document the reason for the referral request, notate the level of urgency, include any necessary supporting continuity of care documentation along with recent results from lab or diagnostic tests, and send directly to the referred-to provider for appointment. Conversely, a provider may also post his/her specifications when receiving referrals, including required diagnostic testing, lab work, patient notifications, scheduling preferences, etc. (see APSD)

B. **Technical Requirements** – the following sections define the technical requirements for each of the core and value-add functions of the CSS.

It should be noted that the Profile Management Services will span and/or interact with most of the services listed below, in some form or another. Therefore, the Profile Management Services must establish and maintain its own relational database management system (RDBMS). Offerors must provide their ability to normalize the RDBMS) and APIs to harmonize business rules and seamless support of the technical requirements of the following:

- Federated Trust Services
- Master Patient Index
- Reporting Registry
- Federated Audit Reporting and Logging
- Provider Batch Upload and Download
- Record Locator Services (including Document Registry)
- Patient Opt-Out Registry
- Patient Privacy Management Services
- White Pages Directory Lookup
- Intra-Network Capabilities Directory
- Patient Discovery
- Patient Directed Audit Report Request and Viewing
- Provider Directory Services
- Public Health Services
- Inter-Network Communications Gateway
C.1 Core Services

1. **Federated Trust Services.** A robust trust service is needed at the CSS that will mature over time as the local and national trust framework continues to evolve. Federated trust services must align cross-certification on a Participant (PKI) level with that of the federal bridge and any other appropriate government-recognized certificate granting bodies. The federated trust will support certificate discovery and ongoing harmonization as well as accept pass-through user and service authentication from trusted Participants to support access to CSS services. The Commonwealth requires an easy-to-use federated solution based upon OASIS SAML TLS standards identified below. This solution needs to be able to support identity provider and service provider functions and provide an administrative database/application to manage the receipt, creation and generation of SAML tokens as well as support SAML decoding and policy enforcement including any necessary URL rewriting functions. Additionally, the federated solution needs to support certificates and support immediate granting and revocation of a Participant's access to the CSS.

For users who will directly access CSS services through a web-based application to support functions such as patient privacy management, audit report requests, provider directory maintenance and upload and other administrative services the following functions must be supported:

a. **Account Lockout.** Provide identification of “brute force” attacks and automatic disabling of accounts. This function ensures that user accounts will not be compromised by rogue users or machines. At a minimum, after an invalid attempt at entering an incorrect user name or password, the system will log the failed attempt. This will be done for some preset number of times. Once this preset number of times has been met the account will be locked and the user will be informed that their account has been locked. Additionally, the user will be given the link and instructions for unlocking their account.

b. **Change Password Notification.** The change password notification function alerts an internet connected and previously registered CSS user of current password expiration. The user will be notified at defined intervals and the user will be provided with sufficient time and directions to change their password before expiration. If the password is not changed, this function will expire the user’s password in accordance with HIE-Network security policies and specifications.

2. **Public Key Infrastructure.** Please refer to Appendix W, Security Infrastructure Requirements for details on the technical requirements for this section.

3. **Master Patient Index.** The CSS level MPI must:

   a. Support both probabilistic and deterministic matching algorithms
b. Have configurable and tunable matching algorithms and reports that provide metrics on matching rates and exceptions

c. Include a patient reconciliation tool that provides the capability to perform administrative functions such as manually addressing mismatches and unmatched records

d. Be able to adapt to the CSS level MPI match level policy, which will be a minimum of 99% assurety.

e. Support manual creation of a patient in the CSS level MPI when an opt-out is received but the patient does not currently have a CSS level MPI record in the CSS

f. At a minimum, have the capability to create patient identities in the CSS level MPI via reconciliation with Participant’s MPIs.

g. Offerors to provide a response which includes a Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis of the solution presented.

Offerors must provide their approach to the appropriate data elements to be used. These elements must be reviewed and approved by the Commonwealth.

4. **Reporting Registry.** The CSS must include a mechanism by which the Participants' reports are received in a format designated by the Commonwealth (e.g., comma separated, delimited text, etc.), who will then synthesize them for aggregate analysis, viewing and reporting to third-party entities and funding organizations. This reporting includes receipt of reporting files from Participants, including via secure file transfer protocol (FTP). Contents for reporting will be defined based on frameworks established in the Strategic Plan and shall include at a minimum:

- Transaction Volumes (unique transactions) by use case and demographics
- Use Volumes (unique providers) by use case and demographics
- Re-Admissions Rates (from hospitals and/or payers; possibly from HIEs)
- Provider contact information
- Complaints and/or breach reporting
- Legal, privacy and security reporting
- Other HISP-specific reporting

Reporting needs may change over the course of the contract term. Changes will be discussed during the annual planning process. Furthermore, the CSS must have capabilities for reporting at the CSS on: adoption, use and impact of data, and administrative reporting on CSS functions, services and activities.

5. **Federated Audit Reporting and Logging.** The CSS must support a broadcast query to each Participant, which will result in a response received in the format of an accounting of disclosures report from each Participant, which contains ATNA specified data elements. This process must allow for responses to be received in a manner consistent with the technology capabilities of the responding Participant and will evolve as the Participants' capabilities are enhanced over time. For example, a
responding Participant could post the audit data to an FTP site or deliver a standards-based electronic response that is consumed and aggregated by the CSS.

6. **Batch Upload and Download.** An automated and manual mechanism for updating and editing directory entries must be provided to support new and changed records. Offerors must propose their approach for managing the manual and automated updates to the White Pages Directory, the MPI, the RLS and any other directory that will be used in a federated fashion. This function must provide an administrative tool to support the reconciliation between Participant uploads, as well as error handling and exception reports. A download request will create files from a directory based on user-identified filters and formats (e.g., comma separated, delimited text, PDF, etc.). An application view is needed to submit a request for a directory report.

7. **Record Locator Service.** The RLS must have the capability to:
   
   - Receive document registrations, queries, updates (changes to metadata) from Participants
   - Identify documents using the Participants local identifiers
   - Support non-required static extensions to the XDS standard (e.g. DOS)
   - Support federated logging and auditing in response to a patient's request
   - Receive batch uploads from the Participants' RLS at time of on-boarding to the CSS with the record creation date reflecting the date of the encounter, not the date of the upload

8. **Patient Opt-out Registry.** A relational store for dynamic queries and integration with the CSS level MPI/RLS is essential. Initially the Commonwealth requires the function to support an "On/Off" switch whereby a patient's denial of release prevents any and all of their data in the HIE-Network from being available for query and viewing. The solution must have the capacity to support potential future requirements for more granular opt-out services. The registry shall:
   
   - Hold a record of the denial of release/cancellation of denial transaction and start/end dates of each
   - Hold all data collected on the denial of release form and the cancellation of denial of release form
   - Provide capability to attach electronic files (e.g., scanned image of signed denial of release form) in the patient's opt-out record in the registry
   - Support denial of release for super protected data (HIV/AIDS, mental health, and substance abuse) only
   - Support override of the opt-out indicator where applicable by law (e.g., Correctional Health Services patients)
   - Support override of the opt-out indicator when the individual has specifically authorized a given access (e.g., SSA disability determination)
   - Queue in a work list all denial of release and cancellations electronically registered, pending receipt of the signed form; automatically reverse the action if the signed form is not received after a predetermined timeframe.
• Generate confirmation that is manually or electronically sent to the patient
• Generate notice to the patient when the "opted-out" patient turns 18; notices may be generated in batch and mailed or emailed to the patient(s)

The Opt-Out Registry must be robust and scalable to support all current and future Participants and all queries generated by their users. Consideration must be given to the growth of adoption based on the Commonwealth's population of providers and entities.

9. **Patient Privacy Management Services.** The CSS shall support a public facing website with mobile access capabilities, which includes secure registration, identity-proofing capabilities, and account creation to allow a patient to login via multi-factor authentication to submit a denial of release as well as login at a future date using the same login credentials to cancel the denial of release. (This website and user authentication process also will support the patient-directed audit report request process.) Upon completion of the denial of release/cancellation of denial of release process, Privacy Management Services will generate a confirmation based on the patient's preferences. The confirmation presentation may include printing and mailing via US mail, electronically delivering via the patient's secure user account or via email or fax.

10. **White Pages Directory Look-up.** The CSS shall support a query by any set or combination of demographic data stored in the directory and allowable by a Participant. Only those who have registered for a DIRECT-enabled email address will be included in the White Pages.

11. **Patient and Document Discovery.** Upon a Participant’s query for a patient and their records in the HIE-Network, a patient demographic query or MPI unique identifier query returns a patient list of matching responses. If more than one patient is returned, the user must select the correct patient upon which a document list with link/pointer is returned. By clicking on the link, the provider generates a query for which the source acts upon for document retrieval. This function does not require a presentation from the CSS. The CSS must be capable of supporting both gateway connectivity and XDS options. If a patient is opted out, this query must be prevented from returning the document list of that patient and must return a message that will be provided by the Commonwealth.

12. **Patient Directed Audit Report Request and Viewing.** The CSS must provide a user interface via portlet with mobile access capabilities that can be integrated into any Participant's portal that supports the standards. All user interface designs and layouts are subject to Commonwealth approval. The report output methodology must support a request from any point of entry, including directly from the patient via phone, via secure website or via a request referred by a Participant. Additionally, display mechanisms must include options (in compliance with state and federal laws) for the patient to download from the secure website, receive as an electronic attachment to electronic mail or be printed and annually mailed by Commonwealth staff.
13. **Provider Directory Services.** The provider directory services must use federal definitions and build on the CSS-implemented White Pages Directory. Directory Services must also build upon the process for populating the White Pages through batch upload from authorized and trusted organizations and databases holding valid provider information. Capability for reconciling the presentation of provider information is necessary when the NPI or license number match (required data elements), but any combination of the provider name, address, phone number, etc. from contributing organizations is different. A linkage between Directory Services and Trust Services is essential to support more interactive provider upload and update functionality; this must be harmonized via the Profile Management Services. Furthermore, in support of enhancing Federated Trust, the Provider Directory Services, under the direction of the Profile Management Services, must support a variety of provider verification purposes, whereby a Participant may understand where a provider is credentialed, for what purpose, if there are sanctions issued against him/her, etc. Provider directory services may be accessed via an API with the Participants or directly through a CSS Provider Directory website.

C.2 **Menu Services** (services which must be implemented by the Selected Vendor, but which need not be purchased by system Participants)

1. **Public Health Services.** The CI-HIE Gateway Proof of Technology will require an “As-Is” assessment and “To-Be” design work. This Proof of Technology must consider the following:
   - API for HIE’s to exchange to CSS and for CSS to exchange to Public Health
   - Translation and transformation interactions
   - Public Health’s use of Orion Health’s Rhapsody Integration Engine
   - Handling of problem or failure notification and resolution
   - Format required by HIEs to exchange data with initial focus on Electronic Lab Reporting
   - Support and compliance with public health requirements and exchange standards such as the S&I Framework
   - Potential to leverage the Commonwealth’s JNET infrastructure as opposed to a direct connection from the CSS to DOH

2. **Provider Coordinated Patient Privacy Management.** The CSS must have the capability to do the following in support of a provider communicating a patient’s privacy management preferences:
   - Accept pass-through user authentication from Participants
   - Support portlet or transactional-based updates to the Opt-Out Registry from Participants
   - Support providers in native environment and/or Participant system to support the patient's requested denial of release or cancellation of denial of release, which is
electronically passed to the CSS to populate the registry. Provide acknowledgement back to the provider that the transaction has been received

- Support a provider attestation that they have received a signed form from patient and have provided a copy of the form to the patient
- Support scanning and uploading of denial of release/cancellation of denial of release forms to the patient’s record in the Opt-Out Registry. Offerors must include the type of document management system they would propose to handle this functionality

3. **Inter-Network Communications Gateway.** The Gateway shall serve as a relay function to translate and convert a request for information from a NwHIN participant into a federated request for information of the HIE-Network. The CSS will generate an aggregated response to the NwHIN query. The CSS will retrieve documents from applicable Participants and pass the information on to the NwHIN requester without opening and/or storing the corresponding PHI. The CSS acts in a proxy gateway capacity following the NwHIN proxy standards.

4. **Intra-Network Capabilities Directory.** A directory of CSS participating entities and their capabilities for exchanging data will be provided by the CSS. The Capabilities Directory will be supported by an administrative console tool and non-interactive certificate protected configuration transaction. Each Participant will have an "On/Off" switch for each exchange service indicating their capabilities. A staging/test environment will be provided to all Participants to ensure that changes in the Participant's system are verified as working and updated in the directory.

5. **Provider Look-up and Referral Requirements Discovery (Transitions of Care Facilitation).** This function supports provider-to-provider referrals, utilizing the Provider Directory Services, to enhance transitions of care. This service allows providers to submit and update referral requirements which referring providers can query, view and act upon to streamline the patient referral process and provider-to-provider communication. This service requires an API so that providers may remain in their native systems or the Participant's system to enter referral preferences and also to query CSS Provider Directory Services to identify providers meeting specific criteria for which they may refer their patients.

C.3 **Datacenter/Hosting Environment Requirements.** Datacenter Services will be required to host and support all CSS functionality. The Commonwealth seeks to contract with an Offeror that currently owns, maintains and operates a world-class (Tier 3) datacenter. The proposed solution must be hosted in the selected Offeror’s (Tier 3) datacenter. The Datacenter services will provide the following:

- A reliable, flexible, secure, and robust IT infrastructure to support the CSS
- Established processes, tools, and service catalog necessary to ensure consistent and predictable pricing models to facilitate accurate budget projections
- Engineering support that will anticipate changes in business and technical requirements and stay current with industry best practices
Adhere to the Commonwealth's contractual, regulatory, and policy compliance requirements for security, architecture, and systems development

The capability to support high-availability hosting, backup, and disaster recovery (DR) services to maintain continuity of operations

The Commonwealth requires that the Offeror's service management practices be based on the ITIL v3 framework and guidance. A service-oriented structure as prescribed by a service framework is required. The Offeror must provide a set of IT services in the following areas:

- Project & Service Management - This level defines the overall Datacenter management structure, including interactions with the Commonwealth. Examples include project management, service level agreement (SLA) management, incident management, release management, change management, and service desk.

- Technical Services - This level defines the Datacenter architecture, and prescribes standards for Datacenter continuity and security. Examples include capacity management, DR planning and testing, security management, and performance management.

- Facilities Management - This level defines day-to-day Datacenter operations and maintenance.

- Managed Hosting Services - This level defines a set of managed services such as operating system support, storage management, database services, network, and security services.

- Capacity On demand Services - This level defines a set of Infrastructure as a Service (IaaS) offerings, each designed to provide just-in-time resources to the Commonwealth. Examples include server, storage, and DR services on demand.

The Offeror must meet the following requirements:

- Be a company registered in the United States
- Be ISO 27001 and 9001, ISO-IEC/ 2000 certified or with equivalent certification for Quality Management Standards
- Have valid SSAE 16 audit findings
- Have valid security certification including CISSP and Comp TIA
- Must be compliant with Federal and State mandated policies
- Be an established firm in providing hosted services for a period exceeding three years
- The proposed datacenter environment must have a valid CMMI certificate (minimum level 3)
- Have had consistent availability of 99.9% in the past six months
- Understand and adhere with applicable federal, state and local regulations, as they pertain to the Commonwealth

C.4 Performance and Interoperability Requirements The following items apply to all functions and corresponding requirements for the CSS.
1. Data Integrity. Data integrity ensures that the data being exchanged across Participants is accurate and is presented as intended by the source. In order to ensure data integrity, stringent and specific test plans must be developed, implemented and maintained. This includes both interface testing and monitoring. Interface testing will ensure that prior to production deployment, interfaces between the CSS and Participants are working to specification and outputs are accurate. Interface monitoring will ensure the continued accuracy of those interfaces after deployment. For the CSS, the primary risk for data integrity is in the CSS level MPI and RLS. Testing and monitoring of these interfaces and systems will drive data integrity for all Participants.

2. System Availability and Planned Downtime. The CSS shall have a schedule (defined in the SLAs) and maximum duration for planned (routine) outages as well as a remediation and communication plan for unplanned outages. Scheduled maintenance should be performed during a set time period on a set day each week. Notice of non-scheduled (non-routine) maintenance should be given to all Participants at least 2 weeks prior to the expected system downtime.

System availability measurements apply to un-planned downtime. Un-planned downtime is defined as downtime (or system un-availability) for which a change control notice was not provided with advance notice of at least two (2) weeks. Planned downtime for maintenance or enhancement migration is defined as downtime for which at least two (2) weeks' notice was provided within the formal change control approval process.

3. System Scalability. The CSS scalability will be highly dependent upon the rate in which Participants grow. Today, HIE in the Commonwealth is in its infancy and the growth is expected to be exponential in the next three years. As such, the CSS must be capable of scaling to accommodate a rapid growth in patients submitted to the CSS level MPI and their corresponding metadata, encounters submitted to the RLS, average daily message load, average daily query load (especially those to the Opt-Out Registry). Furthermore, the system must accommodate compounding stored transactions and data generated over future years.

Scalability needs may be estimated using historical encounter data collected by the hospital and medical associations, the Commonwealth's population and expected growth over time and the number of Commonwealth licensed providers. According to the Pennsylvania eHealth Collaborative Strategic Plan for Health Information Exchange, Pennsylvania has 12.7 million citizens; nearly 41,000 medical and osteopathic doctors, over half of whom (21,740) are primary care providers. There are 268 hospitals, 155 of them are general acute care hospitals, covering over 1.6 million annual discharges. Many of these hospitals are gathered into 24 health systems but several remain independent and/or are relatively small with 84% of all hospitals having fewer than 300 beds.
4. Failover and Disaster Recovery Requirements. The Commonwealth shall maintain disaster avoidance provisions for the CSS that are designed to safeguard any data in the CSS databases and registries. Disaster recovery plans shall be developed and used during unexpected events, which may affect the ability of the CSS to perform its obligations to the Participants. The plans shall be successfully tested and updated on an annual basis or as needed based on changes in the CSS environment.

The Commonwealth shall obtain from its contractor a SAES-16 version of its Business Recovery Plan on an annual basis beginning at the time of contract execution. A continuous improvement process of CSS business recovery processes shall be implemented to facilitate the continuity of CSS services, including actively reviewing new technology in the industry, hardware and uninterruptible power supplies. Business continuity and disaster recovery services shall utilize offsite data storage and a hot site across multiple time zones, which has the necessary hardware to back-up the data center. Such disaster recovery services are designed to achieve and attain resumption of on-line services in the production environment with minimal down time.

Contracts for business continuity of server and network equipment should provide spare equipment on an as needed basis, which could be plugged into the network and attached to the primary or secondary SAN for recovery.

5. Systems Integration and Interface Requirements. System integration and interfaces are an essential part of the CSS infrastructure and must support the functions defined in this document. The following integration and interface requirements will support interoperability between the CSS and Participants to support the planned CSS functionality:

- Master Patient Index harmonization
- Record Locator Service harmonization - document registrations, queries and updates
- Security certificate discovery and harmonization
- Reporting registry update (to CSS)
- Application Programming Interface
- Opt-Out Registry query response from CSS (real-time)
- Audit log query response from Participant
- Batch upload of provider directory (to CSS) and query response download (from CSS)
- Exchange service capabilities (to CSS) and query response (from CSS)
- Patient discovery query (from CSS) and pointer to source data (from Participant)
- Patient and information queries and responses via the NwHIN Gateway (to/from CSS)
- Interface and integration specifications will be defined by the selected CSS Offeror(s) and will consider the systems and applications supported by each Participant
6. **Adherence to Federal Regulations.** It is expected that the Offeror’s proposed solution will be maintained consistently with changes and updates to federal regulations. Within 90 days of a new or updated regulation or standard, the selected Offeror will be required to meet with the Commonwealth staff to discuss the plan and requirements necessary to maintain compliance.

7. **Documentation.** The Offeror must provide solution documentation sufficient to enable an in depth understanding of all components of the proposed solution, including but not limited to system documentation, installation documentation, screen maps and data dictionaries, support documentation, training documentation, and user documentation. Documentation must be delivered in an editable electronic format, to be approved by the Commonwealth.

8. **Browser Types.** The solution must support browsers in use by over 95% of web users, such as Internet Explorer, Firefox, Safari, Chrome, and Opera (compliant with Section 508 requirements) in the current and most recent prior release and must produce the same user experience independent of browser and platform. The platform must adhere to World Wide Web Consortium (W3C) recommendations and other standards of interoperability. Public facing portals must have the ability to support the branding chosen by the Commonwealth. Offerors must address the following items in their response, at a minimum:
   a. browsers and versions supported
   b. browser compatibility testing strategy, including when they decide to add or drop a browser from active support
   c. how the platform development strategy either enhances content using newer browser capabilities, or degrades presentation for older browsers
   d. minimum and recommended screen resolution (e.g., 1024 x 768) for their user interface
   e. policies and use of plug-ins or applications; the Offeror shall limit their use of browser plug-ins or applications to those that are either free online or provided by the vendor at no additional charge
   f. how the components handle browsers where JavaScript is not enabled

C.5 Database and Repository Components

1. **CSS Level Master Patient Index.** The CSS level MPI contains a list of patients, demographics, and unique identifiers for each patient who has received services, which are available from any of the Participants. Each Participant is expected to maintain a local MPI. The CSS level MPI supports patient discovery and privacy management services.

2. **Record Locator Services.** The RLS will provide directory and registry services for the HIE-Network, which supports the interoperability within and between Participants regardless of their architecture and software platforms. In the CSS, this service allows authenticated and authorized providers who participate in Participant organizations to determine the existence and location of patient documents that are located within the
HIE-Network and to query and retrieve chosen documents from the source. This must be integrated with the Profile Management Services to ensure the appropriate levels of privacy and security of protected information.

3. **Reporting Registry.** The overall goal of the Commonwealth Evaluation and Performance Framework is to assess adoption and use of various components of the HIE program, measure perceived value by various participants, and to analyze cost and quality impact of Commonwealth initiatives. The CSS Reporting Registry supports these goals by providing a centralized mechanism whereby all Participants can submit reports that contain the necessary data and information to support this Framework.

4. **Patient Opt-Out Registry.** The patient Opt-Out Registry supports the HIE-Network privacy framework and Patient Privacy Management Services. This Registry stores the denial of release request form and associated data and affective dates registered with the Commonwealth by the patient or on the patient's behalf by a provider. A Registry entry of a patient's denial of release (or opt-out request) "hides" all of the patient's data from query viewing by a Participant. The registry is used to support the management of the patient's opt-out by suppressing the release of the patient's data upon a query for data at any level of the HIE-Network. Patients may also cancel their denial of release, which re-opens their data to query viewing by authorized Participants. The database also must support the immediate termination of the request for denial upon the patient's request to cancel the denial (i.e., their previously registered opt-out request).

### C.6 Systems Architecture and Security Requirements

Offerors are responsible for investigating and proposing the most effective and efficient technical configuration. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of their ability that the proposed approach is not short lived. Several approaches may exist for hardware configurations, other products and any software. Offerors must provide a justification for their proposed hardware, product and software solution(s). Offerors are to present explanations of benefits, merits and limitations of their proposed solutions together with any accompanying services, maintenance, warranties, value added services or other criteria identified herein.

Specifications developed for the long-term solution for the CSS should address the planned technical architecture and security requirements. The following sections do not prescribe these requirements, but rather provide a basis for which Offerors should provide detailed specifications, including detailed network diagrams of the physical architecture that will be used to support the CSS.

1. **Software Architecture**
   - Software language
   - Services profile (i.e., Web services XML scheme x.x, SOAP x.x, WSDL, WDI)
   - Services registry (Services architecture)
• Interoperability standards
• API description

2. Logical architecture
• ESB
• WSBPEL engine
• Rules engine
• Forms engine
• Routing engine
• Transformation engine
• Binding SPI (WSI, SFTP, JMS, SMTP, HTTP, SOAP)
• Additional APIs
• Databases - included clustering and disaster recovery replication
• Application server - include clustering and high availability
• Additional utilities (document management, data warehouse, business intelligence)

3. Physical Architecture Preferences
• Network (load balancing, routers, switches firewalls) if running on your cloud service, or dependencies on the selected Offeror’s data center
• Other physical appliance dependencies (Power Edge), firewall(s), and XML security appliance(s)
• Servers (web, application, database, utility services)
• Building/Facility requirements (space, cooling, electrical)

4. Federated Trust Services. The stakeholder community has a wide, diverse and distributed user base. They have constructed their own registration processes, authentication mechanisms and authorization for securely allowing users and services access to their services. In order to effectively use and build upon these security systems, the CSS will support a federated trust model using OASIS SAML TLS (refer to the Federated Trust Services sections IV-4.B.1.1 and IV-4.C.1.1). Federated trust services must align cross-certification on a Participant (PKI) level with that of the federal bridge and any other government recognized certificate granting bodies.

• Network security
• Intrusion detection
• Vulnerability assessments
• Security certifications and assessments
• Data encryption
• Authentication, authorization, access controls, audit and compliance functions
• External connections and interface security model (Web Services, encryption of data in motion, SAML assertions, other)
C.7 Hardware/software refresh. Offerors are to provide their approach to a hardware refresh schedule, taking into consideration scalability, security, interoperability, and growth over a minimum of five (5) years.

IV-5. Tasks and Deliverables. Offerors are to propose appropriate tasks, deliverables and milestones which reflect their response to the functional and technical requirements. For those Offerors selected for Best and Final Offers, these tasks and deliverables will be expected to align with the detailed cost structure to be provided at that time.

IV-6. Contract Requirements—Small Diverse Business Participation. All contracts containing Small Diverse Business participation must also include a provision requiring the selected contractor to meet and maintain those commitments made to Small Diverse Businesses at the time of proposal submittal or contract negotiation, unless a change in the commitment is approved by the BSBO. All contracts containing Small Diverse Business participation must include a provision requiring Small Diverse Business subcontractors to perform at least 50% of the subcontracted work.

The selected contractor’s commitments to Small Diverse Businesses made at the time of proposal submittal or contract negotiation shall, to the extent so provided in the commitment, be maintained throughout the term of the contract and through any renewal or extension of the contract. Any proposed change must be submitted to BSBO, which will make a recommendation to the Contracting Officer regarding a course of action.

If a contract is assigned to another contractor, the new contractor must maintain the Small Diverse Business participation of the original contract.

The selected contractor shall complete the Prime Contractor’s Quarterly Utilization Report (or similar type document containing the same information) and submit it to the contracting officer of the Issuing Office and BSBO within 10 workdays at the end of each quarter the contract is in force. This information will be used to determine the actual dollar amount paid to Small Diverse Business subcontractors and suppliers. Also, this information will serve as a record of fulfillment of the commitment the selected contractor made and for which it received Small Diverse Business participation points. If there was no activity during the quarter then the form must be completed by stating “No activity in this quarter.”

NOTE: EQUAL EMPLOYMENT OPPORTUNITY AND CONTRACT COMPLIANCE STATEMENTS REFERRING TO COMPANY EQUAL EMPLOYMENT OPPORTUNITY POLICIES OR PAST CONTRACT COMPLIANCE PRACTICES DO NOT CONSTITUTE PROOF OF SMALL DIVERSE BUSINESS STATUS OR ENTITLE AN OFFEROR TO RECEIVE CREDIT FOR SMALL DIVERSE BUSINESS UTILIZATION.