Your Health Idaho (YHI)

Privacy Impact Assessment
RFP Questions and Responses

February 19, 2015

The following presents a list of questions Your Health Idaho (YHI) received in response to YHI's Request for Proposals ("RFP") for a Privacy Impact Assessment ("Assessment"):

1. The RFP references PII throughout the document. Other than PII, are there any regulated data types in scope for this assessment (e.g. electronic Protected Health Information)? If so, which regulated data types are in scope?

Answer: Unlikely, but possible. Our Eligibility Shared Services partner stores Federal Tax Information (FTI) data. (Electronic) Protected Health Information (PHI, or ePHI) is not collected, as YHI is not a covered entity or business associate; we do not receive electronic health information as a normal course of our business. We do not anticipate the Vendor will encounter FTI or PHI/ePHI as a part of this Assessment. The Vendor may encounter electronic health information inadvertently provided to us.

2. Has an ISRA (information security risk assessment) and/or SSP (System Security and Privacy Plan) previously been completed for YHI?

Answer: Yes, as required by CMS for all the State Based Marketplaces to receive Authority to Connect (ATC), YHI has completed all the documents in the Minimum Acceptable Risk Standards for Exchanges (MARS-E) document suite and secured the Authority to Connect (ATC). The MARS-E package includes the System Security Plan (SSP) and Workbook as well as the Security Assessment Report (SAR) in addition to PIA and agreements (ISA, CMA).

3. What Exchange functions (e.g. eligibility determinations, submission of notices) will be covered by the Assessment?

Answer: The proposed business functions are on pages 3-5. YHI welcomes additional suggestions in the Proposal, based on Respondent's experience in similar situations.

4. Do overriding State or other agencies' policies and procedures exist that the departmental policies and procedures align with?

Answer: YHI is an independent body corporate and politic established by Idaho Code § 41-6101 et seq; YHI is not a state agency. YHI's policies and procedures are intended to align with Department of Health and Welfare (DHW) and GetInsured as appropriate, and third party vendors are required to comply with MARS-E/FISMA standards.

5. Does YHI integrate with the Federal Data Services Hub? If so, what type of data is sent/received?

Answer: The integrated eligibility system managed by Department of Health and Welfare (DHW) integrates with the Federal Services Hub. YHI has no direct integration with Federal Services Hub. The details on the type of data sent/received will be shared as a part of the Assessment.

6. What standards in addition to MARS-E are required for compliance (e.g. FISMA, IRS Pub 1075)?

Answer: YHI expects the selected Vendor to bring the knowledge necessary for it to identify and validate the applicable standards and to address the requirements of such standards in performing the Assessment. FISMA and Section 155.260 of Final Rule of the ACA along with MARS-E have been identified as applicable standards.

7. Who manages IT security, privacy, and governance? Does the State have a Chief Information Security Officer (CISO or acting security lead)?

Answer: Yes, YHI has a dedicated security team. The details will be shared with the selected Vendor during the Assessment.

8. How is vendor security management performed (e.g. who manages/approves vendor access to systems, data, and/or facilities)?

Answer: The details will be shared with the selected Vendor during the assessment.

9. Do YHI staff (including vendors) have remote access to the system? If yes, how is this access monitored?

Answer: The details will be shared with the selected Vendor during the Assessment.

10. Do YHI staff (including vendors) have access to the system via mobile devices? If yes, how is this access monitored?

Answer: The details will be shared with the selected Vendor during the Assessment.

11. What other forms of access are permitted? E.g. is IP range blocking and port disablement implemented?

Answer: The details will be shared with the selected Vendor during the Assessment.

12. Was the original PIA for ATC done in accordance with MARS-E v3 or v4?

Answer: v3.

13. Was the PIA for ATC accepted as submitted or was a remediation plan required for ATC?

Answer: YHI's PIA document was submitted to CMS and accepted. Any open items are being tracked as a part of Plan of Action and Milestones (POAMs), which will be shared with the selected Vendor during the Assessment.
;
14. If a remediation plan was required, how many tasks were identified and how many have been completed?

Answer: Any open items are being tracked as a part of Plan of Action and Milestones (POAMs), which will be shared with the selected Vendor during the Assessment.

15. As part of the original PIA or current documentation, how complete would you characterize existing data flows?

Answer: YHI expects the selected Vendor to identify and validate this as a part of the Assessment.

16. Do you handle or process any Federal Tax Information (FTI) or Protected Health Information (PHI) and is that part of the scope of this effort?

Answer: Please see response to question 1.

17. Could you provide a list of all parties/agencies external to the Exchange from whom PII/PHI/FTI is received and/or shared?

Answer: The details will be shared with the selected Vendor during the Assessment.

18. You identify that YHI spans multiple entities (YHI, DHW, GI, and multiple third parties), please briefly describe what each of these entities are responsible for.

Answer: Please refer to the RFP on page 3 and 4.

19. Regarding the multiple entities, which ones will require a complete analysis and which ones will the scope stop at the interface (e.g. navigators or broker programs to add boundary business logic or assess within the boundaries)?

Answer: YHI expects the selected Vendor to identify and validate this as a part of the Assessment.

20. Do data flows internal to all of the multiple parties exist?

Answer: The details will be shared with the selected Vendor during the Assessment.

20. Do you handle payment information such as bank account numbers, credit card numbers, etc.?

Answer: No. Payment functions redirect to carrier sites and are outside the system boundary as currently defined.

21. Does the scope include any of the YHI administrative (back office, leadership, office) systems or just the Exchange environment?

Answer: Primarily Exchange Environment. Any supporting processes or administrative systems supporting the Exchange, identified as a part of data flow diagrams, will be considered in scope.

22. Does YHI have a small business element that is within scope? If so, does the small business element interface with the small business exchange?

Answer: No, please refer to the RFP on page 3 and 4.

23. Are there any state (Idaho or other states) privacy laws that are (a) applicable and (b) within the scope of the effort? For example, if an Idaho based family has a student living in California, there is the potential for CA privacy laws to apply? Example 2, if the Exchange is housed in data centers outside of the state, then the state laws where it is located may apply.

Answer: Yes, YHI expects the selected Vendor to identify and validate the applicable privacy laws and to address the requirements of such laws in performing the Assessment.

24. Will there be any consideration to extend the deadline for responses past the stated deadline of February 27th?

Answer: YHI is expecting Proposals to be submitted by the deadline. Please review the RFP to understand the rights reserved by YHI.