access health CT

Connecticut's Health Insurance Marketplace

Data Privacy and Security Subcommittee Meeting

June 26, 2014

Presentation Overview

- Approval of April 1, 2014 Meeting Minutes
- Chairperson’s Update
- Revised Committee Charge Language
- Proposed Broad Outline of Data Governance Process – internal vs. external users
- RFP and RTM Requirements for Data Privacy and Security
- Update and Overview of Preferred Vendor Security Audit
- Next Steps

Revised Committee Charge Language

The overall objective of the Database Privacy, Confidentiality, and Data Security Workgroup is to create effective and transparent processes and policy-to ensure ~~individually identifiable information~~ information is properly protected, while maintaining health information needed to improve healthcare quality and efficiency in Connecticut. To this point, the workgroup will focus on the following initiatives:

- Formulation of a review/approval framework for data release to the research and public health community
- Creation of a data accessibility charter to determine use cases and clearance levels for varying levels of data access
- Preparation of a functional data use agreements between Access Health Analytics and future data requesters
- Ongoing development and evaluation of data protection policies to functionally mitigate data breach and re-identification risks
- Identification of legal limits/boundaries of data reporting, e.g., FTC DOJ requirements for price transparency, HIPAA restrictions on cell size requirement for reporting

Proposed Broad Outline of Data Governance Process – internal vs. external users

Data Governance

- Policy and Procedures document cite a number of data governance issues as below.
  - ➢ Data Collection – legislation mandates data collection from commercial payers
  - ➢ Data Management – legislation enables Access Health Analytics (AHA) to manage All-Payer Claims Database (APCD)
  - ➢ Data Reporting – legislation objective is to use APCD's data to report on healthcare market trends, costs and utilization which may "…improve efficiency, enhance outcomes and improve understanding of healthcare expenditures in public and private sector."
  - ➢ Data Disclosure – legislation allows only deidentified data to be released.

Data Disclosure Process - Internal

- Data will rest at APCD with non-PHI member identification format
- There will be two types of data available for internal analysts
    - ➢ Deidentified data – 18 member-specific identifiers suppressed
    - ➢ Limited Data Set – 16 member-specific identifiers suppressed
- Limited Data Set will be required to support value-added applications – Geocoding (using zip codes), clinical episode or risk groupers (using dates of services)
- No data or report will be published on the web or elsewhere that may lead to risk of reidentification (of members)

Data Disclosure Process - External

- Releasable Data –
  - Member identifiers masked
  - Deidentified data structure, i.e., 18 member-specific information suppressed
  - Claims from facilities (inpatient & outpatient), professionals, pharmacy
  - Diagnoses, procedures, drug codes, providers, financials, types and places of services
- Data requesters – private and public entities
- Data Release Entity – a committee to be created which works with AHA to receive, evaluate and approve requests
- Data Release Committee will apply certain criteria to determine the validity of data requests
- Data Release Committee will weigh risks of reidentification with any request and may deny based on that ground

Data Disclosure Process – Data Release Committee

- Data release Criteria –
  - ➢ Identifying varying levels of data – aggregated vs. detail claims data
  - ➢ "Minimum necessary" standard under HIPAA
  - ➢ Researcher will not be allowed to link with other data sets to reduce reidentification risk
  - ➢ Requestors will need to provide evidence of infrastructural adequacy
  - ➢ Requesters will also have to demonstrate –
    - ✓ Purpose of the data request
    - ✓ Methodology and data elements needed to support research
    - ✓ Qualifications of the researcher and/or the institution (s)he belongs to
    - ✓ Privacy and security measures to protect the data
    - ✓ State how the research will support CT's objective
    - ✓ Requirement that the committee will be given the preview prior to publication
  - ➢ Requester will have to sign a Data USE Agreement (DUA) with AHA

Data Disclosure Process – Data Use Agreement (DUA)

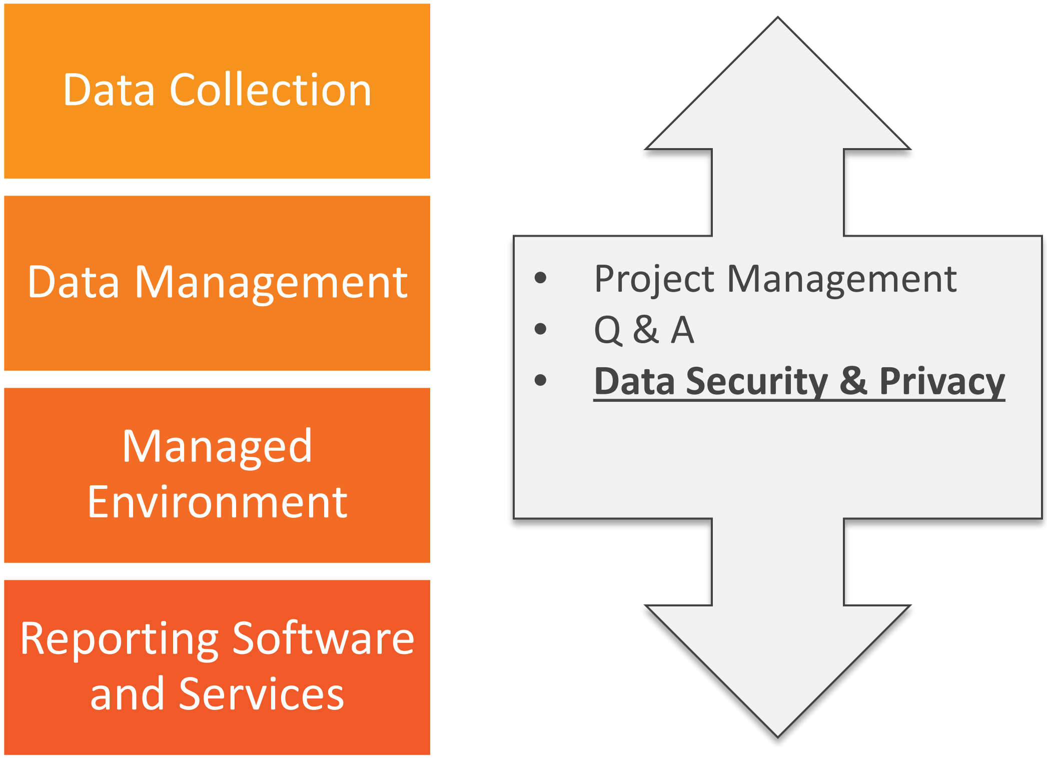
- DUA must include the following –
  - ➢ Ensure that data will be used only for the purpose of the proposed research
  - ➢ Researcher will not attempt to reidentify people from the data they receive
  - ➢ Researcher will not release this data or reuse for other than the stated objective/project
  - ➢ Researcher will have to return data back to AHA or demonstrate that it has erased all such data from its environment
  - ➢ Recipient agrees to defray costs of producing the data in advance of data delivery
  - ➢ Recipient of data must ensure that the data is not used by other(s) not stated in the research proposal
  - ➢ Breaches of DUA may constitute enough grounds to
    - ✓ Immediate cancellation and return of data to AHA
    - ✓ Will result in future denial of any data from APCD
    - ✓ May lead to civil action by the AHA, at State and/or Federal level

Security Related RFP and RTM Requirements For The Data Management Vendor

RFP and RTM Requirements For The Data Management Vendor

Background:

- APCD: Data Management Contractor RFP, issued on January 27, 2014.
- Outlined the vision for the proposed APCD and requested services:



Data Collection

Data Management

Managed Environment

Reporting Software and Services

- Project Management
- Q & A
- **Data Security & Privacy**

RFP and RTM Requirements For The Data Management Vendor

Background:

Project Critical Success Factors & Expectations (Related to PSC):

- Security and protection of PII and PHI data.
- Fully integrated data security and privacy protections consistent with all applicable laws.
- A managed hosted environment that provides controlled access to anonymized data and ensures the maintenance of security protocols.

RFP and RTM Requirements For The Data Management Vendor

Data Collection

RTM Requirement: *"The Contractor shall provide encryption of data during transmission employing FIPS 140-2 compliant cryptographic controls in accordance with NIST Special Publication 800-53."*

Requirements/Specifications*:

- FIPS and HIPAA security standard
- Supports SFTP, FTPS and HTTPS protocols
- 256-bit AES encryption
- Full audit log of file transfer activity
- Immediate/Automated transfer to a secure internal network for further processing
- **Additional Level of Security:**
  - 2nd layer of file encryption & password protection to further reduce vulnerabilities of data at rest (Not a requirement of FIPS)

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Data Management

RTM Requirement: *"The Contractor shall ensure that all sensitive PII and PHI is anonymized and secured."*

Requirements/Specifications*:

- Fully automated identifier encryption process which removes human interaction
- Ensure immediate encryption of identifiers upon receipt from reporting entities
- Proceed with data load phase

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Data Management

RTM Requirement: *"The Contractor shall develop and maintain consistent masking methods for PHI and PII data elements."*

Requirements/Specifications*:

1. The Contractor shall ensure all direct identifiers are encrypted, except:
   a) Zip Code
   b) Dates of Service
2. Strong Encryption shall be maintained

Direct and Indirect Identifiers To Be Removed

1. Names;
~~2. Zip codes~~
~~3. All elements of dates ;~~
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Managed Environment

RTM Requirement: *"The Contractor shall provide role-based security"*

Requirements/Specifications*:

Multi-Layer Authentication shall be managed by the Contractor:

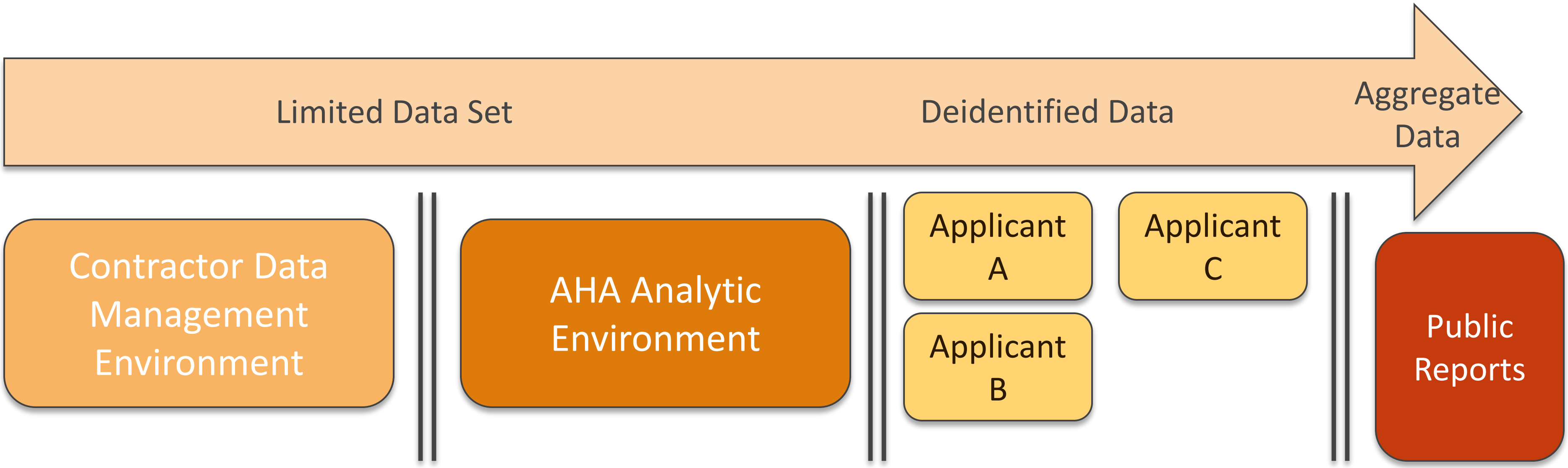
- **Network Authentication**
  - Virtual private network locked to specific inbound IP addresses
  - Multi-factor Authentication
- **Domain / Operating System (OS) Authentication**
  - Password Management
  - Clearance Level User Groups
- **Data Access Authentication**
  - Password Management
  - Data Access Clearance Model

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Managed Environment

Data Access Clearance Model*



Limited Data Set

Deidentified Data

Aggregate Data

Contractor Data Management Environment

AHA Analytic Environment

Applicant A

Applicant B

Applicant C

Public Reports

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Reporting Software and Services

RTM Requirement: *"The Contractor shall develop a process to integrate data, tables and views on the web."*

Requirements/Specifications*:

- **Public Reporting:**
  - Adherence to CMS Cell Suppression Rules

- **Reporting Application:**
  - Comply and provide support for software code review of web portal code

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

Universal Requirements:

RTM Requirement: *"The Contractor shall propose a security plan highlighting vendor implementation to ensure Data remains secure."*

Requirements/Specifications*:

Security Plan shall cover 4 major focus areas:

1. Project Planning & Processes
2. Data Interactions, and Sanitization
3. Security and Privacy Methods
4. Governance

** Subject to security auditor approval and risk assessment*

RFP and RTM Requirements For The Data Management Vendor

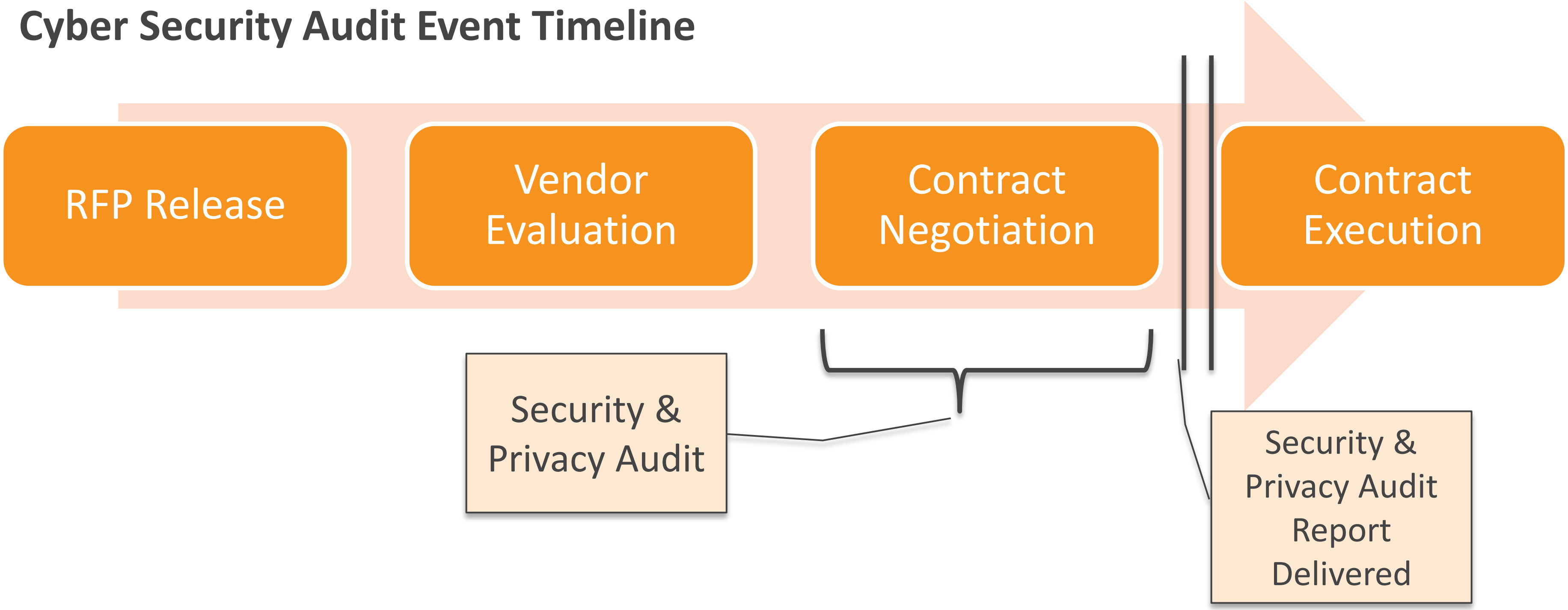
Universal Requirements:

- A single POC Security and Privacy Officer.
- Prohibition on Contractor from releasing or using data or information obtained, for any purposes other than those authorized by AHA.
- Audit and test all aspects of data and software to ensure hardware and data assets remain protected.
- Participation in Data Privacy and Security Subcommittee meetings, whenever necessary.

Update and Overview of Preferred Vendor Security Audit

Overview of Preferred Vendor Security Audit

Cyber Security Audit Event Timeline



RFP Release

Vendor Evaluation

Contract Negotiation

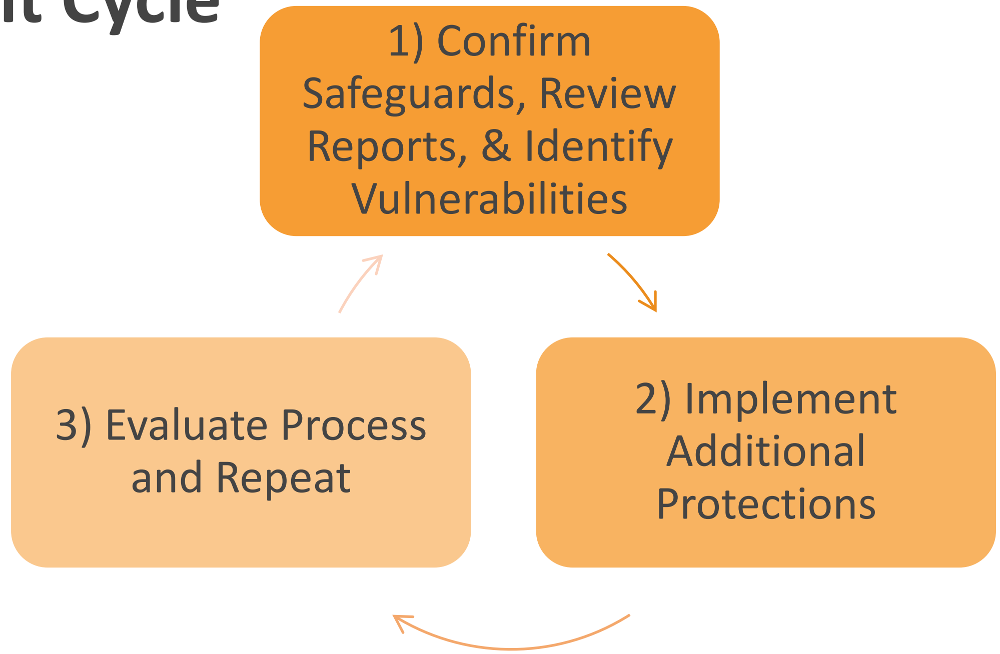
Contract Execution

Security & Privacy Audit

Security & Privacy Audit Report Delivered

Overview of Preferred Vendor Security Audit

Proposed Audit Cycle



1) Confirm Safeguards, Review Reports, & Identify Vulnerabilities

2) Implement Additional Protections

3) Evaluate Process and Repeat

Documentation To Be Utilized:

1. AHA Security Audit Reports
2. Vendor Certifications
3. Vendor Annual Compliance Reports
4. Vendor Attestation

Overview of Preferred Vendor Security Audit

Security Standards and Frameworks To Be Referenced Within Cyber Security Audit:

1. National Institute of Standards and Technology (NIST)
   - 800-53 Rev. 4
   - 800-66
2. Federal Information Processing Standards (FIPS) 140-2
3. **HIPAA Security Rule**
   - Administrative Safeguards:
   - Physical Safeguards:
   - Technical Safeguards:

Overview of Preferred Vendor Security Audit

Task 1: Cyber Security Evaluation of Proposed APCD Data Management Vendor

Goals:

1. Complete an administrative, technical, physical security audit of the proposed APCD data management vendor to identify and document potential vulnerabilities.
2. Assess the proposed vendor's security program against security requirements for the Health Insurance Portability and Accountability Act (HIPAA), using the NIST HIPAA Toolkit, with a mapping to 800-53.

Deliverables:

A Cyber Evaluation Report covering:

1. Background
2. Key Findings of Review, Identified Gaps/Deficiencies, and Risks.
3. Recommended Remediation Activities

Overview of Preferred Vendor Security Audit

Task 1: Cyber Security Evaluation of Proposed APCD Data Management Vendor

Tasks:

1. Review:
   a) Contracts with key third parties
   b) Existing audit and certification reports
2. Collect and review administrative, technical, and protocol documentation
3. Interview targeted personnel (e.g., human resources, legal, IT security and infrastructure, business personnel, finance, and communications)

Overview of Preferred Vendor Security Audit

Task 1: Cyber Security Evaluation of Proposed APCD Data Management Vendor

Tasks:

4. Review of current technical and administrative documentation
5. Review privacy and security with third party vendors and software providers
6. Identify gaps or deficiencies in security program and governance structure
7. Categorize and prioritize risks and recommended remediation measures

Overview of Preferred Vendor Security Audit

Task 2: Proposal and Proposed Methodology Review

Goal:

1. Perform an independent audit of RFP proposal methods and methodology from the proposed contractor.

Deliverables:

1. A report setting forth:
   a) Findings associated with the high-level evaluation of the Vendor's security program and its security practices.
   b) Recommendations for changes to approach, technologies deployed, or controls that would enhance security.

Overview of Preferred Vendor Security Audit

Task 2: Proposal and Proposed Methodology Review

Tasks:

1. Review proposed security processes for receiving, sanitizing, anonymizing, storing, and transmitting health data
2. Assess the adequacy of the proposed approach for managing data for AHA
3. Conduct a high-level evaluation of hosting provisions and incident response
4. Perform an evaluation of the software coding practices

Task 3: Provision of Technical Assistance in Contract Language

Goals:

1. Obtain a 3rd party review and assessment of the security and privacy requirements and SOW from a subject matter expert.
2. Supplement contract language with findings.

Deliverables:

1. Proposed language additions and revisions to the security related subsections of the contract and SOW.

Tasks:

1. Provide recommendations regarding proposed contract language to security approaches, processes, and/or controls.

Task 4: Software Code Review (Future Service)

Goal: Ensure future developed code for APCD products maintain security protocol and mitigate risk of vulnerabilities.

Deliverables:

- TBD

Tasks:

1. Upon request, perform software code review of any web portal code developed by VENDOR to identify weaknesses or vulnerabilities.

Next Steps

Next Steps