HealthFacts RI (APCD) Standard Extracts
RI APCD Data Management Plan Template

IMPORTANT INFORMATION

Prior to completing this template, we strongly recommend reviewing the RI APCD Data Security and Privacy Guidance, available below or at http://www.health.ri.gov/data/healthfactsri/.

As part of the RI APCD Data Management Plan, the Requesting Organization agrees to:

- Comply with all applicable federal and state laws and regulations regarding privacy and security of confidential health information, as described in the RI APCD Data Use Agreement.
- Comply with organizational privacy and security policies for protecting confidential health information and electronic health information.
- Adhere to the RI APCD Data Display and Reporting Policy, as described in Exhibit B of the RI APCD Data Use Agreement, when disclosing any data outputs (including interim analyses and publications) to any individual outside the project personnel specified in this Data Management Plan.
- Bind third party contractors who will have access to the RI APCD Data to this Data Management Plan and the RI APCD Data Use Agreement.

For the purposes of this Data Management Plan, "RI APCD Data" refers to the RI APCD data extracts, claims line level data, or any data outputs that do not follow the RI APCD Data Display and Reporting Policy, as described in Exhibit B of the RI APCD Data Use Agreement.

Please complete the questions below regarding the requested RI APCD Data ("RI APCD Data") and attach to your application. This RI APCD Data Management Plan should be completed by the project personnel who will be responsible for ensuring data security in everyday use, with assistance from a security or privacy officer or staff who has sufficient understanding of the Receiving Organization's internal privacy and security policies and procedures. *This RI APCD Data Management Plan will not be publicly posted.*

DATA MANAGEMENT PLAN

Project Title (should appear the same as on the application):

Requesting Organization (should appear the same as on the application):

1. **Project Personnel**

   a. Please identify the following individuals within your organization:

   The individual who will serve as the "Data Custodian", responsible for organizing, storing, and archiving the RI APCD Data, and who will notify the Rhode Island Department of Health (RIDOH) of any breaches of the RI APCD Data Use Agreement or this Data Management Plan.

Name:	
Organization:	
Title:	
Phone:	
Email:	

The individual responsible for ensuring that all project personnel have signed a confidentiality agreement, will access and use only the minimal data necessary to achieve the project purpose, will only access the RI APCD Data via the secure methods described in this plan, and will no longer have access if their involvement in the project is terminated.

Name:	
Organization:	
Title:	
Phone:	
Email:	

The individual responsible for ensuring the RI APCD Data is destroyed upon termination of the RI APCD Data Use Agreement, and per the terms of the RI APCD Data Use Agreement.

Name:	
Organization:	
Title:	
Phone:	
Email:	

b. Please list any project personnel who will have access to RI APCD Data (excludes aggregate outputs that comply with RI APCD Data Reporting and Display policy).

Name:	
Organization:	
Title:	
Phone:	
Email:	

Name:	
Organization:	
Title:	
Phone:	
Email:	

Name:	
Organization:	

Title:	
Phone:	
Email:	

Name:	
Organization:	
Title:	
Phone:	
Email:	

Name:	
Organization:	
Title:	
Phone:	
Email:	

2. RI APCD Data Delivery, Storage and Access

a. Please provide the delivery address for the RI APCD Data, and for any location where the RI APCD Data will be stored.

Delivery Location

Organization:		
Address:		
Phone:		

Storage Location

- Same as delivery location

Organization:		
Address:		
Phone:		

b. How would you like the RI APCD Data transferred to your organization?
- SFTP
- External hard drive with encrypted data

c. Please describe the data management environment where project personnel will work with the RI APCD data, from the IT storage infrastructure to end users' workstations.

d. Please describe the security features of this architecture and the IT policies and procedures that will ensure RI APCD data is secure. Supplemental documents may be provided but please provide a summary addressing the points raised in the RI APCD Data Security and Privacy Guidance.

e. Within this data management environment, please describe how project personnel work with the RI APCD Data. Please include a typical workflow addressing how personnel interact with the data via the described architecture, how intermediate data products are managed and how collaboration occurs within the confines of the managed environment.

f. How will access to the RI APCD Data be restricted to only the individuals who require access?

g. Please describe the team's review process to ensure any data products to be exported from the data management environment meet the RI APCD Data Display and Reporting Policy (as described in the Data Use Agreement).

3. Personnel/Staffing Safeguards

a. Please describe the training on confidential and electronic health information that the project personnel who will have access to the RI APCD Data have received.

b. How often is this training required?

c. Have all individuals who will have access to the RI APCD Data signed a confidentiality agreement?

- Yes
- No

4. Information Security

a. Does your organization have security policies that are followed and accessible to all staff accessing the RI APCD Data?

- Yes (if yes, attach these policies to the application)

- No

b. When were your organization’s security policies last updated?

c. How do staff/users notify your organization of security problems?

d. What are your organizational procedures for handling a suspected or actual data breach?

e. Has your organization or any of the project personnel listed in question 1 ever been involved with a project that experienced any unauthorized use, reuse or disclosure of protected or confidential data?

- Yes
- No

f. If yes to 4(e), describe the incident, whether the incident included Protected Health Information (PHI), the response procedures that were followed and any subsequent changes in protocols to mitigate the risk of future events.

5. Technical and Physical Safeguards

a. What is the minimum password length and character complexity (uppercase, lowercase, numeric, and special characters) required for passwords on user accounts logging on to the systems to access RI APCD Data?

b. How often are user account passwords required to be changed?

c. How will project personnel with access to the RI APCD Data store user passwords and data encryption keys (e.g. password management tool, memory, etc.)?

d. Is there an audit log of all user log-ons to the system hosting the RI APCD Data?

- Yes

- No

e. Please describe any additional authentication controls your organization uses to defend against unauthorized logon (e.g. maximum failed login attempts, two factor authentication, lock-out period, etc.)

f. Please describe your organization's procedures for maintaining and updating anti-virus and anti-malware software.

g. How will RI APCD Data at rest be encrypted on storage media (must use encryption at least AES-256 or stronger)?

h. Are project personnel able to transfer RI APCD Data in bulk from the secure environment where the RI APCD Data will be accessed?

- Yes
- No

i. If yes to 5(i), please describe why transfer of RI APCD Data is necessary.

j. If yes to 5(i), please describe how your organization will limit transfers of RI APCD Data to only secure locations and only when necessary.

k. If yes to 5(i), will RI APCD Data be transmitted by your organization over the Internet?

- Yes
- No

l. If yes to 5(l), how will RI APCD Data be encrypted when in transit (SSL/TLS, SFTP, etc.)?

m. Will hard copies of the RI APCD Data be used?

- Yes
- No

n. If yes to 5(n), please describe why printing RI APCD Data is necessary.

o. If yes to 5(n), how will these hard copies be secured (e.g. locked file cabinet, locked office, etc.)?

p. What additional specific physical or technical safeguards (not yet mentioned) will be used to mitigate the risk of unauthorized access to RI APCD Data?

6. RI APCD Data Destruction

a. Describe the measures you will use to destroy the RI APCD Data upon termination of the RI APCD Data Use Agreement, per the requirements of the RI APCD Data Use Agreement.

b. Describe your procedures for terminating access to the RI APCD Data when staff/researchers terminate participation in the project.

7. Use of Third Party Contractors

Answer the following questions only if using a third party contractor that will be storing the data in a separate location.

a. Describe how you will communicate with the third party about RI APCD data and analyses being conducted.

b. Describe how you will manage the third party to ensure they are properly handling the RI APCD data.

8. Multi-project Subscription

Answer the following questions only if requesting a multi-project subscription for standard extracts.

a. Describe your plan for internally vetting individual applicants and projects..

b. Describe your plan to provide organizational oversight of individual projects and users accessing the RI APCD Data, including how you will ensure all users are adhering to the terms and conditions of the RI APCD Data Use Agreement.

9. Attestation

By signing below, the Requesting Organization attests that the organization and all project personnel will follow the procedures and requirements outlined in this Data Management Plan.

Name:	
Signature:	
Title:	
Organization:	
Phone:	
Email:	
Date:	