Rhode Island All-Payer Claims Database (APCD)

Data Privacy and Security Guidelines

These guidelines are meant to assist data requesters of RI APCD data to develop a comprehensive data management plan for safeguarding RI APCD data and protecting members' privacy. Thinking about how your organization follows these guidelines will help you complete the data management plan template and Data Release Review Board and Data Security Committee review process.

For additional best practices for guiding your own organizational security policies and procedures, we recommend reviewing the Centers for Medicare and Medicaid Services Information Security and Privacy Best Practices.

Data Storage and Access

1. Store RI APCD data in a separate location from other sensitive data, and that only designated project personnel can access
2. Protect all computers and devices on which RI APCD Data will be accessed via:
    a. Firewalls
    b. AES-256 or stronger encryption for data at rest on storage media
    c. Strong network and/or wireless password, that is on a need to know only basis
    d. Anti-malware and anti-virus software that is updated whenever a new update is available
3. Restrict access to RI APCD data to the least number of people possible necessary to access that information to perform their job duties
4. Restrict the ways in which data can be accessed to:
    a. Desktop computers on a closed network with no ability to download or transfer data
    b. Desktop or laptop computers on a secure network. If remote access is necessary, use a secure method like VPN
5. Do not allow access to RI APCD through personal devices.

Personnel Safeguards

1. Use a unique logon or account for designated project personnel to access RI APCD data
2. Use strong passwords and establish a policy as to how often passwords need to be changed
    a. Establish a process and designate personnel to manage password updates Communicate to project personnel that encryption keys and passwords should be treated like access to the data itself. Update all project personnel on who their designated IT personnel are.
3. You may:
    a. Have a "clean desk" policy in which project personnel cannot keep any sensitive information on their desk, including passwords.
    b. Use password management systems to help manage passwords, or establish policies that project personnel memorize passwords
4. Ensure all project personnel receive training on confidential data and organization security policies.
5. Educate project personnel on how they can personally help prevent data security breaches by:
    a. Keeping their password secured, or memorizing it

    b. Locking their screen when they leave their desk
    c. Recognizing and reporting any suspicious activity, messages, or potential attempts at intrusion
6. Have a policy in place for project personnel to report suspected security breaches, and how to handle them

Technical Safeguards

2. Put in place user account controls, such as:
    a. Maximum failed login attempts
    b. Lockout periods after idle time
    c. User audit logs
    d. Two-factor authentication
3. Restrict transfer of RI APCD data to only when necessary, or do not allow it at all:
    a. Have policies around when data transfer is and is not allowed
    b. Use physical controls to restrict transfer, like flagging any transfers for review
4. Restrict use of hard copies of RI APCD data to only when necessary, or do not allow it at all. If using hard copies:
    a. Have a designated secure printing area
    b. Store hard copies in locked drawers in locked offices
    c. Collect any hard copies that are handed out
    d. Shred any hard copies that are no longer needed
5. Establish a peer review process for ensuring any data outputs that leave the secure environment adhere to the RI APCD Data Display and Reporting policy, e.g. data is reviewed by the data custodian and a security officer.
6. Secure data on an encrypted drive.
    a. Restrict access to the drive to authorized users in accordance with the organization's IT security policy.
    b. Provide access via user account to log access and use a single password sign on (Access to encrypted storage controlled via LDAP or Domain vs an external drive(s) with a separate password the user must remember).
    c. If using third-party storage or hosting services, ensure the third-party service only has access to encrypted bites.

7. Use active monitoring alerting systems for security intrusion detections