100 West Road Suite 300
Towson, MD 21204
www.c-q-l.org

# OVERVIEW OF PORTAL DATA SECURITY

The PORTAL Data System from CQL | The Council on Quality and Leadership offers users a secure platform for inputting and storing data as well as the ability to run statistical reports to withdraw information from the data. However, given the type and scope of information being collected, it is critical to ensure data remains secure at all times. This page outlines the data security protocols for the PORTAL Data System as well as CQL's internal protocols to ensure data security. Lastly, this provides an overview of steps users of the database should take when downloading the data to ensure security on their end.

CQL's new data collection system, PORTAL, is built using the Rennroc database system. The Rennroc system is designed with a highly-configurable security model in that every user, site object, and data point has a specific and customizable security profile. This allows for any security access requirement to be applied at any level within the site.

## PORTAL (RENNROC) SYSTEM SECURITY

All interface features and objects, which can vary from an entire section, to a specific web form, to a single form field, action button, or navigation element, can be identified and isolated within the security layer. By applying a user and user group security policy, the system administrators can define point-specific security definitions that link an individual or a group with a specific interface object; then a specific permission can be applied, defining what level of access is available. This model can also be applied at the data level. A specific data-point within the system can be identified and secured using this same method as outlined above. This allows for the secure protection of highly-sensitive information. Even if a user has access to the interface object that displays the data, the data itself will be masked or omitted if the user does not have the appropriate security clearance to review that data point. Additionally, this robust security model will always protect your data at the Organization level as well. Not only is the data filtered through the user/user group permission definitions, but it is also filtered against the subset of Organizations to which the user is assigned. A user that has been assigned to manage and maintain admin-level information for a specific Organization will inherently see only the appropriate data for that Organization and any inherited child Organization beneath it.

In terms of physical security, the Rennroc datacenter is a top-tier facility with the following:

- SSAE16 & PCI Compliance
- Network Security monitoring
- N + 1 Power system
- High availability redundant internet connectivity
- 5+ levels of physical security
- Fully climate controlled
- 24x7 uptime and physical access
- 24x7 human monitoring

100 West Road Suite 300
Towson, MD 21204
www.c-q-l.org

Other security features of the Rennroc (PORTAL) system also include:

- Password complexity requirements
- Auto-user disable due to inactivity
- Domain restrictions built in email address limitations
- Audit controls built in including - Logging and auditing of all activity in the site and security report templates for regularly scheduled checks
- All data transmissions via Secure Sockets Layer (SSL)
- Incident reporting (logs) available in the admin interface real-time as well as security reports
- Datacenter includes automated and 24x7 human monitoring systems

## CQL SECURITY PROTOCOLS

Data entered into the PORTAL Data System will occasionally be downloaded by CQL staff for use in reports and research to identify trends and key findings in the POM and BA data. Given this, CQL has set up additional procedures for internal data management and security. It is important to note that any data used by CQL in national reporting or for research purposes outside of contracted agreements with its clients is de-identified at both the provider and individual level. Below, brief descriptions of CQL's internal data security procedures are outlined.

### LIMITED ACCESS: INTERNAL

A key component to ensuring data remains secure is to first make sure that only those who need access to the data have access to the data. At CQL, all downloaded POM data is stored on the company's servers in password and user protected files. This means that only individuals who are given the password or whose computer is granted permission to access the server files can in fact access the data. CQL limits this access to the research and data team to ensure fewer interactions with the data.

### LIMITED ACCESS: EXTERNAL

Similar to CQL's approach to limiting access to data internally, we are also working directly with organizations to maintain constraints on who is able to gain access to the online databases. In PORTAL, every user has their own account with a unique password which increases security. We are able to control what each user has access to, by setting them as a standard user (can enter interviews and only see their own interviews for security purposes) or power user (can enter interviews, see interviews for the entire organization, can run reports and analytics). Should the individual leave the organization, the organization can contact CQL and we can modify the account settings so that individual no longer has access to the data.

100 West Road Suite 300
Towson, MD 21204
www.c-q-l.org

### OFF-SITE STORAGE

CQL's servers are located and monitored in offsite, secure locations. This approach provides enhanced security to the servers (cyber security and climate control) as well as diversion of risk to ensure a reduced likelihood that the servers could be destroyed due to natural or unnatural circumstances.

All in all, the approach to ensuring data remains secure at CQL is always a top priority. CQL takes proactive steps to ensure that the valuable information collected through the Personal Outcome Measures® and Basic Assurances® is safe, secure, and accessible to our clients. Although there is always some risk to data being collected electronically, we believe the steps taken significantly reduce the risk to marginal at best.

## TIPS FOR DATA USERS

Although both Rennroc and CQL maintain tight data security procedures to ensure data is protected, there is still risk associated with the data collection and management at the individual provider level. It is important that agencies utilizing this database consider the internal procedures and protections needed if this data is to be downloaded and stored on local computers or servers. It is recommended that agencies takes steps similar to those outlined in CQL's process above any time POM or BA data is downloaded from the data collection system. For example, agencies should limit access to identifiable data to reduce the number of interactions individuals have with the data. Meaning, the more access people have to the data, the greater the potential for risk (data manipulation, data sharing, data deletion, HIPAA violations). Organizations should also assess their internal IT capabilities to ensure that there is adequate storage and security in place to house the POM and BA data internally.

### MORE ABOUT HIPAA COMPLIANCE AND DATA SECURITY

- http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html
- https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment