OVERVIEW OF CQL ONLINE DATA SECURITY

CQL | The Council on Quality and Leadership is pleased to provide users of the Personal Outcome Measures® (POM) access to the newly developed online, expanded POM database. The database allows 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 document outlines the data security protocols for the online data collection tool as well as CQL's internal protocols to ensure data security. Lastly, the document provides an overview of steps users of the database should take when downloading the data to ensure security on their end.

Data Collection Platform Security

CQL's new data collection system is built using FluidSurveys. FluidSurveys is an online, customizable survey software used to collect information across industries. The system is used by organizations such as Ikea, BMW, and Southwest Airlines to develop customizable surveys for data collection. FluidSurveys offers the ability to not only customize the survey type and scope, but also the ability to securely store and manage large databases using bank grade SSL security. Below provides an overview of FluidSurveys' data security protocol for meeting HIPAA compliance.

Physical Security

FluidSurveys' servers are located in data centers which provide biometric access controls, constant surveillance, redundant power feeds and generators, robust fire suppression, and carefully monitored climate control to protect the servers that store data.

Login Protection

All accounts are password protected and all passwords are encrypted and never stored in clear text. Account logins also have brute-force login protection by preventing individuals/bots from attempting to guess a password too many times.

Secure Socket Layer Encryption (SSL)

FluidSurveys login (i.e. when a user logs in by typing their username/password) is protected using Secure Socket Layer Encryption (SSL). This is a default feature of all accounts. SSL will encrypt communications (256 bit) between the respondent's browser and our server.

Threat Scanning and Firewall Protection

FluidSurveys' servers are scanned for threats and vulnerabilities by McAfee secure scan and are protected with firewalls to prevent unauthorized connections.

Redundant Servers and Data Centers

FluidSurveys infrastructure uses redundant storage and servers to keep the application and your data available in the case of hardware failure - and another set of servers and storage in a geographically separate data center in case our primary data center is made unavailable by a disaster or other disruption.

FluidSurveys uses iWeb.com as its primary data center. iWeb's data centers are equipped with a wide range of security, power management, cooling and network access equipment. Biometric sensors, security cameras and secure access are the first items encountered on-site. In addition to thousands of servers, power regulation systems, diesel generators and air conditioning systems are vital aspects of the facilities. All of these infrastructures are fully controlled and managed by iWeb's team of hosting infrastructure experts.

Connectivity to the internet is assured by multiple black fibers getting into the building's telecom rooms through diverse entry points. Multi-gigabit connectivity is used to link iWeb's data centers to each other and to connect upstream providers to iWeb's own network. iWeb's team monitors the data center and network operations 24 horus a day, 7 days a week, 365 days per year.

Backups

The data in your FluidSurveys account is replicated across multiple database servers in two locations to prevent a single failure from causing data loss. Additionally, that data is backed up nightly and stored in a secure offsite location to ensure that, even in the event of a catastrophe like a tornado or flood, your information will be safe and your records can be quickly restored. FluidSurveys maintain all backups for a period of 30 days. If you delete your data from our system, it will remain in FluidSurveys' backups for the next 30 days and after that point will be permanently deleted.

Accessibility Compliance

Surveys developed through FluidSurveys.com are section 508 compliant and W3c – Priority I and II compliant.

CQL Security Protocols

Data entered into the online data system will occasionally be downloaded by CQL staff for use in reports and research to identify trends and key findings in the POM 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. FluidSurveys allows CQL to set up unique user accounts with unique passwords and unique hyperlinks (access points) for an organization's individual dataset. To manage this or our end, CQL works directly with the organization after they have purchased access to the database to set up the core operating account to the survey system. At that time, CQL assigns only one username and password for full access to the account. The organization can provide multiple users the hyperlink for data input, but CQL will advise on the importance of limiting access to the backend data system. Should the individual whose name and contact information is used to initiate the account 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.

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.

Nightly Backups

Along with its servers being stored offsite, CQL's files and data are backed up nightly to ensure continuity of information in the case of data or files being accidently deleted.

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® 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 FluidSurveys 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 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 data internally.

Organizations with questions about FluidSurveys' or CQL's data security procedures or those with questions about security for internal POM data collection should review the 'Additional Resources' links below or contact CQL's research and data team.

ADDITIONAL RESOURCES

More About FluidSurveys

http://fluidsurveys.com/about/

http://fluidsurveys.com/university/health-insurance-portability-accountability-act-hipaa-privacy-act-online-survey-research/

http://fluidsurveys.com/wp-content/uploads/2013/08/FluidSurveys_Security_Document.pdf

More About HIPAA Compliance And Data Security

http://www.hhs.gov/ocr/privacy/hipaa/administrative/index.html

http://www.healthit.gov/providers-professionals/security-risk-assessmentb

CONTACT US

To learn more, contact:

CQL | The Council on Quality and Leadership
100 West Road, Suite 300
Towson, Maryland 21204
410.583.0060
www.c-q-l.org
data@thecouncil.org

CQL's Mission:

CQL is dedicated to the definition, measurement and improvement of personal quality of life for people receiving human services and supports.