Q-global™ Web-based Administration, Scoring & Reporting System Security FAQs

Q-global is a web-based platform for test administration, scoring and reporting. It houses the industry's gold standard in assessment tools and is accessible from any computer connected to the Internet. Secure and affordable, Q-global helps you quickly and efficiently organize examinee information, generate scores, and produce accurate, comprehensive reports.

Frequently Asked Questions

Is there a Privacy Policy for this System?
Yes. The Privacy Policy is also available for download. The Privacy Policy explains how personally identifiable information is collected, handled and used.

How does Q-global protect personal data?
Pearson security for data stored on Q-global complies with the standards established in the HIPAA Security Regulations and in accordance with the HITECH Act applicable to Business Associates. The following types of general safeguards protect your personal data:

- Administrative safeguards,
- Physical safeguards, and
- Technical safeguards.

In addition, your data is secure as follows:

- When you Access the System. The https Q-global site and its database are password protected.
- Through a Secure Transmission. All data transferred from your web browser to Q-global is sent over a secure (industry-standard Secure Socket Layer (SSL) Internet connection.
- With your Stored data. Your data is protected utilizing encryption, physical security, and administrative safeguards.

Why is the data stored in Canada, instead of in the United States?
Pearson's hosting facility in Canada accommodates the security requirements of U.S., Canadian, EU and other global data privacy laws.

How will examinee data be secured?
Examinee data on Q-global is protected through physical security, administrative safeguards and encryption. The examinee data is stored in Canada in a database that is encrypted with industry-standard high-security encryption. When the data is transmitted, the data is encrypted using industry-standard Transport Layer Security (TLS) technology. The system uses a secured data base which separates and segregates a customer's records so that they cannot be seen by other customers. This separation and segregation is confirmed through testing and external auditing.

Customer access to the System and the data is protected by unique usernames and passwords. Customers are responsible for safeguarding their passwords, and to change passwords periodically and whenever there is a concern about a possible compromise. The System frequently undergoes vulnerability and penetration intrusion testing and is subject to audits, both internal and external.

How can I access my examinee's data?
Use your username and password to log into Q-global and retrieve or download your stored data at any time, 24/7.

What happens if an unauthorized user attacks the database and tries to steal my data?
Personally identifiable information, including examinee data, is encrypted on the System. Encryption is utilized to prevent an unauthorized person from being able to access or use the data.

What examinee data can System support people see?
Pearson support personnel do not have access to personally identifiable examinee data. In the unlikely event that such access was needed to address a specific problem, specific procedures would have to be followed, which would entail securing explicit consent from the customer, obtaining a copy of the data from the customer or receiving authorization from the customer and Pearson management to have the data decrypted. System support staff personnel do not have access to, or control over, the encryption keys. The encryption keys are securely held and protected through physical and administrative safeguards in Canada.

Can Pearson use my examinee data for research?
Pearson may statistically aggregate raw data in de-identified non-personally-identifiable form from nonidentifying information collected; and during the testing process for internal quality control, operations management, security, and research to enhance, develop and improve tests and testing processes. Deidentification of data means that the extracted demographics and test responses cannot be identified as belonging to any individual and specifically meets the de-identification standard as required by HIPAA in 45 CFR §164.514(b)(1).

Is Q-global HIPAA compliant?
Pearson and its Q-global application comply with all applicable security and privacy regulations required by HIPAA and the HITECH Act as a Business Associate.

Is Pearson a Business Associate of health care providers that use its services?
If you are a Covered Entity as defined by HIPAA, when you agree to Pearson's Business Associate Addendum, Pearson becomes your Business Associate under HIPAA.

What is Pearson's position on releasing data pursuant to HIPAA requests?
The Business Associate Addendum to the Q-global License agreement addresses the release of data to the Covered Entity pursuant to HIPAA.