Pearson

Privacy Practices: Q-global & Q-interactive

This whitepaper: (a) is for informational purposes only, (b) represents current Pearson Clinical Product offerings and practices, which are subject to change without notice. Pearson agreements control the responsibilities and liabilities of Pearson to its customers, and this document is not part of, nor does it modify, any agreement between Pearson and its customers. Furthermore, this document does not provide legal advice, and the information we present may not take into account future changes in laws and regulations. We urge customers to consult with their legal counsel to familiarize themselves with the requirements that govern their specific situation making their independent assessment of the information included in this whitepaper.

Introduction

Pearson takes data protection and privacy seriously, incorporating these components as fundamental principles within its product and service development framework. This whitepaper serves to demystify the privacy and security measures that Pearson has implemented for Q-global and Q-interactive (collectively referred to as ”Pearson Clinical Products”), its web-based platforms aimed at robust test administration, scoring, and reporting. Recognizing the paramount importance of safeguarding its customers' personal data (as defined under relevant data protection laws), this document, along with Pearson's **Terms of Use** and **Privacy Policy**, emphasizes its commitment to protecting customers' personal data. Pearson achieves this through stringent protocols pertaining to data collection, processing, storage, and security, in strict compliance with applicable data protection legislation and regulations.

Overview of Q-global and Q-interactive

Both Pearson's Clinical Products are utilized by mental health specialists, educators, and other professionals to conduct assessments, compute scores, and generate reports efficiently. These systems are accessible anytime from any computer and house over 60 industry-leading assessment tools. All features of Pearson Clinical Products operate within a secure, private web environment, assisting professionals to streamline their assessment workflows.

Data Collection and Processing

The table below presents a summary of the types of personal data Pearson Clinical Products collect and the purposes for each category:

Data Subject Categories	Categories of Personal Data Collected	Purpose of Collection
Patient/Examinee	Name (optional)	Examinee identification
	Date of Birth	Calculating examinee age at testing and ensuring correct administration and scoring
	ID (optional)	Examinee identification
	Demographic Data	For assessment administration and inclusion in score reports
	Assessment Responses	Examinee responses to assessment items for the purpose of scoring
	Assessment Scores	Calculated scores for the purpose of reporting/exporting
Provider, Administrator	Username	Providing access to the platform
	Name	Customer identification
	Email	To allow receipt of system emails
	Telephone Numbers	To allow contact for technical support issues

Data minimisation stands as a foundational principle in our approach to data privacy and protection. As providers of clinical products, we prioritize collecting only essential data for assessments, ensuring privacy and compliance. Additionally, we empower our customers by offering optional data fields, enabling them to exercise control over data processing and fostering a relationship of trust.

Legal basis and role of Pearson with respect to Pearson Clinical Products:

Pearson Clinical Products manage different types of customer personal data, and therefore, Pearson's role in processing personal data varies according to the source and purpose.

1. **Data from Educators, Qualified Customers, and Test Administrators:** In instances where Pearson Clinical Products handle personal data provided by these parties, Pearson acts as a data processor. It processes personal data based on the instructions given by the customer, acting as the data controller, ensuring compliance with their directives. The data controller is responsible for determining the legal basis and purpose of processing.

2. **Data related to products directly offered to end customers:** When processing personal data in connection with products sold directly to end customers, Pearson assumes the role of a data controller. In such cases, it relies on three key legal grounds for data processing: consent, the performance of a contract, and legitimate interest. This approach enables Pearson to abide by all applicable data protection regulations while maintaining the highest standards of privacy and security for its customers.

For the purpose of the above section, the following definitions shall apply:

"Provider and Test Administrator" shall mean a qualified customer or an individual designated and authorized by the qualified customer to coordinate and manage the assessment and scoring process and/or receive assessment test results and reports.

"Patient or Examinee" shall mean an individual who is assigned or administered a clinical assessment by a test administrator.

For more details about the categories of data processing, purpose and legal basis, please refer to Pearson's Clinical Privacy Statement.

Secure Storage Controls and Technologies

Pearson and its subcontractors are committed to safeguarding personal data collected via Pearson Clinical Products by employing appropriate operational, administrative, technical, and physical security measures to prevent loss, misuse, or alteration of the information under its control. Its approach includes encrypting all sensitive data transmissions and securing all data repositories. Using HTTPS encryption, personal data is protected from a customer's browser to Pearson servers.

Where payment information is processed, Pearson protects such information according to Payment Card Industry (PCI) standards. Where Pearson uses third parties to process personal data, it ensures they have appropriate technical and organisational control to protect the personal data they process. Furthermore, Pearson's servers utilize Secure Sockets Layer (SSL) encryption technology, which is compatible with most major browsers and designed to protect its customer's personal data and privacy.

To provide optimal security for customers' data, the Pearson Clinical Products database utilizes Advanced Encryption Standard (AES) 256-bit encryption, a widely recognized and trusted encryption method. This robust security measure effectively protects customers' data from unauthorized access and ensures the confidentiality and integrity of the data while stored within the system.

Pearson Clinical Products is certified to ISO 27001 for Information Security Management. Our certificate is available on request.

Amazon AWS is certified to SOC 2, demonstrating how AWS achieves key compliance controls and objectives. The SOC 2 report is available on request.

For more information regarding Pearson's security measures, please click here.

Data Transfers and Processor Compliance

When transferring personal data from the United Kingdom (UK), the European Union (EU) and European Economic Area (EEA), Pearson relies on the principles recognized under the General Data Protection Regulation (GDPR), particularly the adequacy decision by the European Commission (EC) and UK Secretary of State (SoS).

In the course of delivering the services, certain aspects may require engagement with a data processor. In such instances, Pearson ensures that these processors have adequate technical and organisational measures in place to protect its customers' data. The terms of engagement with these processors are also aligned with GDPR requirements and our contractual commitments to our customers.

Pearson has partnered with Amazon Data Services Canada, Inc. and MongoDB Limited to provide hosting services via Amazon Web Services (AWS). AWS is pivotal in hosting data for Pearson's Clinical Products whilst we leverage MongoDB Atlas to ensure robust data management that aligns with global operational efficiency and privacy compliance standards. All collected data is securely stored on AWS servers situated in Montreal, Canada.The EC and SoS have identified Canadian commercial organisations as a sector in Canada as having sufficient data protection standards, allowing for the transfer of data from the UK, EU and EEA to Canada and processed in accordance with the GDPR without any additional safeguards or authorizations. This is known as an adequacy decision. This principle guides the relationship with AWS and is reflected in the AWS Customer Agreement, which governs Pearson's use of AWS services and incorporates the AWS Data Processing Addendum via AWS Service Terms.

Pearson Clinical Products does not utilise any Amazon Services which require the transfer of data to Amazon's third-party service providers. As such, all hosted data remains on AWS serv-ers in Canada. Amazon's list of sub-processors is maintained here. Amazon is certified to the Data Privacy Framework, please click here to see the details.

Additionally, we have partnered with Twilio SendGrid, an email service, to streamline email communications for our clinical customers with their patients or examinees. SendGrid's primary role is ensuring your emails reach their intended recipients. The content of the email is stored only temporarily, just long enough for successful transmission. Email addresses are retained for a brief 30-day period to analyze click and open rates, after which they're promptly deleted. This approach minimizes the personal data retained by SendGrid. Importantly, this data is transferred to the United States for email routing and delivery purposes. SendGrid is certified under the Data Privacy Framework as approved by the European Commission. For more details on this certification, please click here.

The list of sub-processors utilized by Twilio is also publicly available and the list could be reviewed here.

We recognise that some of our customers are concerned that the United States FISA regulations may apply to Amazon's international subsidiaries. Pearson has assessed this in-depth with assistance from the EU and SoS adequacy decisions and AWS's comprehensive transfer impact assessment documentation. Pearson has determined that the FISA regulations do not apply to Canadian businesses and that the Canadian PIPEDA is applicable. Amazon has further asserted that no request has resulted in the disclosure to the U.S. government of enterprise or government content data located outside the United States. Amazon publishes half-yearly reports regarding information requests, which can be found here.

Throughout the data transfer process, it utilizes secure connections and encryption standards (AES256 and HTTPS) to protect data at rest and in transit. Data in transit is protected with AES-128 and TLS encryption, and data at rest is secured using AES-256 encryption and Federal Information Processing Standards (FIPS). Furthermore, Pearson Clinical Products platforms incorporate features such as two-factor authentication, strong password security, automatic logout following periods of inactivity, and non-collection of sensitive information such as actual names or social security numbers.

The customers can rest assured that data backups are maintained consistently, allowing continuous access to our platforms 24 x 7 x 365 unless they choose to delete data from Pearson Clinical Products. For more information regarding Pearson's security measures, please click here.

Furthermore, Pearson's internal support team, which is situated across various global locations, may occasionally need to access personal data for the purpose of providing technical support. Pearson has implemented a comprehensive intra-group data transfer agreement (IGA) to assure that every Pearson affiliate adheres to the relevant data privacy laws while handling personal data.

In addition, every employee within Pearson is obligated to undergo thorough training regarding the processing of personal data in compliance with the pertinent laws. They are also contractually committed to maintaining the utmost confidentiality, thereby ensuring that personal data always remains secure and confidential.

For a more in-depth understanding of the architecture of Pearson Clinical Products, you can examine our data flow diagram available at these links: Q-Global and Q-Interactive.

An up-to-date list of sub processors is maintained online here.

Data Subject Rights

When a Provider or a Test Administrator, acting in the capacity of a data controller, shares personal data with Pearson and uploads it on the Pearson Clinical Products web portal, any requests related to data privacy rights should be addressed directly to the relevant Provider or Test Administrator that shared the personal data, who will fulfil the request. Functionality has been provided to enable all data to be exportable.

If a user rights request involves Pearson Clinical Products' personal data within the scope, the Provider or a Test Administrator should forward the request to Pearson by emailing dataprivacy@pearson.com, and Pearson will fulfil its part of the request accordingly.

However, for Pearson products offered directly to end-customers, Pearson assumes the role of a data controller. The end-customer may exercise their data privacy rights, including the right of access, erasure, or any rights under GDPR and/or applicable privacy laws, by contacting Pearson as outlined in our Privacy Policy.

Data Deletion Compliance

Pearson acknowledges the paramount importance of its customers' personal data. When availing of the services of Pearson Clinical Products, customers retain absolute command over the data they upload on Pearson Clinical Products web portal.

As controllers, customers possess the prerogative to erase their data when deemed necessary. Functionality is provided, enabling customers to export and delete their data at their convenience and schedule. In Pearson's capacity as a data processor, it will ensure to implement any customer requests for deletion in a prompt and comprehensive manner. Additionally, we ensure to abide by the statutory timelines set forth by data privacy regulations to complete such requests.

In essence, customers' personal data is their domain. Pearson respects this principle and ensures that customers have the ultimate control over the destiny of their data when utilizing Pearson Clinical Products.

Use of De-Identified Data

In the realm of data privacy and protection, the use of de-identified data is a pivotal practice. It ensures the safeguarding of personal information while facilitating research, development, and improvement of products and services. This section outlines our approach to the use of de-identified data, aligning with the principles enshrined in our contracts and reflecting our commitment to privacy and compliance with applicable laws.

DEFINITION AND SCOPE

Per our agreements, we stipulate that during and subsequent to the term of the Main Agreement, we are permitted to employ and disclose customer personal data, from which directly identifying features have been eliminated and therefore rendered anonymous. This process transforms the data into an anonymised format, thus removing it from the ambit of ‘Customer Personal Data’. Such de-identified data enables us to engage in activities that validate the efficacy and quality of our services and assessments, enabling further development and enhancement of said services and assessments for the benefit of our clients.

METHODOLOGY

The process of de-identification is rigorous and is designed to ensure that individual identifiers are irreversibly removed. This involves:

- **Stripping Direct Identifiers:** To prevent the re-identification of individuals, all direct identifiers such as names, identification numbers, and specific geographic markers are removed.
- **Disassociation from Client Accounts:** Data is further disassociated from client accounts, eliminating any indirect paths to re-identification.
- **Aggregation:** Data is used in a fully aggregated form, which ensures that it cannot be linked back to any individual, enhancing privacy safeguards.

APPLICATION AND LIMITATIONS

Our use of de-identified data is strictly in a fully aggregated and de-identified manner, primarily to investigate product reliability post-publication. By analysing aggregated assessment data across items and scores, we can validate that test constructs are being measured reliably.

It’s noteworthy that privacy regulations, especially those governing health data in the United States, impose stringent restrictions on the use of identifiable data. These legal constraints significantly limit our ability to utilise the data for further developmental activities. As such, our engagement with de-identified data remains circumscribed to areas where it can be employed without contravening privacy laws.

COMMITMENT TO PRIVACY

Our approach to the use of de-identified data is underpinned by a steadfast commitment to privacy and compliance with relevant legislation. We continuously monitor and adapt our practices to align with evolving legal standards and ethical considerations. By prioritising the de-identification of data, we strive to harness the potential of information to advance educational research and innovation while ensuring the utmost respect for individual privacy.