IAED | International Academies of Emergency Dispatch

ACADEMY DATA CENTER DATA PROTECTION POLICY

The International Academies of Emergency Dispatch ("IAED") is committed to the responsible handling and protection of your Data. The Academy Data Center Protection Policy is intended to provide you with necessary information regarding the procedures followed with respect to the collection and transmission of your ProQA and AQUA Data.

WHAT DATA IS BEING COLLECTED?

The only Data we will be collecting is the ProQA and AQUA databases. These are the databases created during the use of the ProQA and AQUA software. These databases contain everything you have entered in the software.

HOW IS THE DATA COLLECTED?

IAED Data Center software is an application that provides a simple method to warehouse Data to the IAED Data Center. It saves time and resources when extracting and exporting ProQA and AQUA data files. ProQA and AQUA cases are transmitted in near real-time and seamlessly to the Academy data warehouse.

Installing the application does not affect your regular dispatch operation in any way, it simply provides an easier means to copy existing data files from one server to another.

The application is installed via an internet connection to the XLerator server (where ProQA files are stored) at your agency.

HOW IS THE DATA GOING TO BE USED?

The Data is used to benefit emergency agencies and allow for greater Data availability for research, as it relates to public safety.

To elaborate, the Data is used for the IAED's longitudinal research studies, which support protocol validation and evolution, building outcomes-predictive models, quality assessment, and generating content for training sessions.

Further, the Data Center makes possible the generation of free analytics for agencies to use to inform their own quality assurance and quality improvement programs, enhancing call-taking and response processes and demonstrating Return on Investment.

The legal basis for the processing of the data is a legitimate business interest (Research & Development), and the serving of the public interest by furthering public safety.

WHO HAS ACCESS TO THE DATA?

Access to data in the Data Center will be restricted to assigned IAED Data Analysts/ Statisticians and, in some instances, with external research partners. However, you have access to your agency-specific analytics dashboard based on the data you share with IAED as well as an overall analytics dashboard based on de-identified aggregated data from all agencies submitting data to the IAED Data Center.

Any personal information transferred between the United States and the European Union is transferred only upon your consent, and according to stipulated Data Processing Agreements between the parties in accordance to General Data Protection Regulation (GDPR).

Data received by the Data Center may be shared with external research partners for studies that require specialized collaboration. All data transfers are subject to GDPR-compliant Data Processing Agreements.

IS THE DATA SECURED?

We have implemented administrative, physical and technical security measures specifically designed to protect the Data from loss, theft, misuse, unauthorized access, disclosure, alterations, and destruction.

• The Data is stored to a secured server, which utilizes a modern, secure operating system.

• Access to the Data is locked down and strictly restricted to select staff of the IAED and access is password protected.

• The server has an active directory for authentication that utilizes secure passwords and security.

• A windows firewall is used on the server and a perimeter device is applied as the internal gateway. Firewall definitions are updated every 15-minutes for pattern recognition.

• Anti-virus software is installed with real time threat analysis and full scans run weekly.

• The Windows firewall is also locked down to allow only those with specific IP addresses to have access.

• Data Center backups occur every night

• Data is encrypted as uploaded and downloaded. Currently, it uses a SHA-256 SSL Certificate, which is a cryptographing hashing algorithm developed by the National Institute of Standards and Technology. Such certificate may change from time-to-time as technology and standards change.

• In the unlikely event that the Data contains identifiable personal health information, use of the Data shall be in compliance with applicable government regulations and restrictions, including HIPAA.

WHAT CONTROLS DO EMERGENCY AGENCIES HAVE OVER THE DATA?

You have access to the Data you share. You can request that the Data be returned and/or destroyed. To do so, agencies must contact our Data Protection Officer at DPO@emergencydispatch.org

WHO TO CONTACT

Any questions, concerns or complaints regarding the use or disclosure of Data should be directed to our Data Protection Officer via email at DPO@emergencydispatch.org

Mailing Address:

IAED
Attn: Data Protection Officer
110 South Regent Street, Suite 800
Salt Lake City, UT 84111

Email Address:

DPO@emergencydispatch.org