IQVIA Third Party Access (TPA) Program

Policy on IT-support Vendor Access to IQVIA Data

Introduction. IQVIA licenses IQVIA data to clients for internal use. IQVIA will authorize a client to release IQVIA data to an unaffiliated individual or organization performing work for that client ("vendor") when the vendor has the appropriate license(s) through the IQVIA TPA program. A TPA license agreement between IQVIA and a vendor operates as IQVIA's authorization to the client to release data to that vendor. IQVIA also uses a written TPA policy as IQVIA's authorization to the client to release data to a vendor. This document is a TPA policy describing those circumstances in which a client is authorized to provide IQVIA data to certain types of IT-support vendors retained by the client to perform IT Support Services on behalf of the client. If this TPA policy does not apply, then client needs another form of IQVIA written authorization to provide vendor access to IQVIA data (e.g., TPA license agreement or another TPA policy) before sharing IQVIA data with that vendor.

This IQVIA TPA policy authorizes a client to provide IQVIA data to IT support vendors to provide IT Support Services when all of the following conditions apply:

Vendor Engagement

1. **Vendor Classification:** The vendor is primarily an IT service provider.
2. **Services are Data Agnostic:** The IT Support Services are not tailored to or dependent on specific data types, including but not limited to Target Data. The IT Support Services are applicable across various data types without requiring specialized knowledge or customization for Target Data.
3. **Services are Industry Agnostic:** The vendor provides its IT Support Services to clients in the Target Industries and other industries without being tailored to or dependent on any specific industry.
4. **Engagement Scope:** IQVIA data will only be used in connection with the performance of IT Support Services.

Access and Use Conditions

1. **Access is Necessary:** Access to IQVIA data is necessary for the vendor to perform the IT Support Services.
2. **Access is Incidental:** The vendor's need to access IQVIA data is incidental to the delivery of IT Support Services.
3. **Minimum Access:** The vendor is granted the minimum access to IQVIA data necessary to perform the IT Support Services, and further data access and use are not authorized under this TPA policy.
4. **Exclusive Use:** Uses of IQVIA data is limited to use for IT Support Services and for no other purpose.
5. **Non-Disclosure:** The vendor does not disclose IQVIA data to any third party. IQVIA data is disclosed to those vendor employees with an actual need to access the data to perform IT Support Services for the client.

Exclusions

1. **Services Exclusion Clause:** IT Support Services that involve the use of IQVIA data for purposes beyond the scope of generalized IT support are explicitly excluded from this TPA policy. Such excluded services include, but are not limited to, data analysis, data processing, data mining, data visualization, data integration, data reporting, or any activity that directly manipulates, utilizes, or derives insights from the data.
2. **Vendor Exclusion Criteria:** Vendors that offer products or services specifically designed for the Target Industries are excluded from this TPA policy. This includes vendors with one or more business(es) involved in

providing technology, data, software, services, or solutions that are tailored to meet the needs of the Target Industries. Any vendor with offerings intended to serve or enhance the operations within the Target Industries is not eligible under this TPA policy.

Client Contract with Vendor: The client must have a written contract with the vendor that strictly limits the vendor's access, use, and disclosure of all data to meet the requirements of this TPA policy and the applicable agreement between the client and IQVIA.

Vendor Oversight: Client will use commercially reasonable efforts to confirm the vendor has reasonable and appropriate safeguards and controls to comply with the terms and conditions of this TPA policy during the period the vendor provides IT Support Services for the client.

Notification of Non-Compliance: Client will promptly notify IQVIA in writing if client becomes aware of any use of IQVIA data by the vendor in a manner that is inconsistent with the terms of this TPA policy.

Use of Artificial Intelligence (AI) with IQVIA Data: Vendor may not use IQVIA data with any machine learning application, large language models (LLMs), artificial intelligence (AI) algorithms (e.g., generative AI algorithms), AI software or any other artificial intelligence capabilities to train or validate an AI model, develop prompts, produce output or create, enhance, test or validate any AI-related intellectual property using IQVIA data (collectively “AI Tools”) unless such use is solely for the benefit of the client providing the IQVIA data to the vendor. Client will not authorize a vendor to retain any IQVIA data, or any information, algorithm, model, or AI Tool derived from the use of IQVIA data, whether used with IQVIA data alone or in combination with other data, for the vendor’s own purposes or for the benefit of any person or organization other than client. If there is any data use restriction relating to AI in a contract between IQVIA and the client, then that data use restriction takes precedence over the other terms of this paragraph.

Application: It is the client's responsibility to apply this TPA policy and to apply it correctly. If in doubt, please speak with a representative on the IQVIA TPA Program team to determine whether this TPA policy applies or a different form of written authorization from IQVIA is required before sharing access to IQVIA data.

IQVIA Right to Modify: IQVIA reserves the right to modify this document at any time, effective upon the later of (i) public release of the updated document, or (ii) the effective date specified at the time of the release with the updated document.

////////////////////////////////

IQVIA Third Party Access (TPA) Program

Policy on IT-support Vendor Access to IQVIA Data

Attachment 1: Definitions:

- **Target Data** refers to data relating to medicines, medical devices, healthcare, healthcare professionals, healthcare organizations, clinical laboratories or related activities.
- **Target Industries** refers to the life sciences, medical, medical device, or healthcare industries.
- **IT Support Services** refer to a range of information technology services aimed at maintaining and supporting an organization's information technology infrastructure. These services include, but are not limited to:

  a. Hardware Maintenance and Repair: Fixing or replacing faulty hardware components like storage devices, processors, network hardware, memory, motherboards, and power supplies.

  b. Software Installation and Updates: Installing new software or updates to existing software to ensure systems are running current versions.

  c. Network Configuration and Troubleshooting: Setting up and maintaining network hardware like routers and switches, and resolving connectivity issues.

  d. User Account Management: Creating, modifying, and deleting user accounts, and managing permissions and access rights.

  e. Technical Support and Helpdesk Services: Providing assistance to users experiencing technical issues with their computer hardware, personal devices or software.

  f. System Monitoring and Performance Tuning: Monitoring and managing system performance to maintain connectivity, operations, and security.

  g. Security Management: Implementing and managing security measures like firewalls, antivirus software, and intrusion detection systems.

  h. Backup and Recovery: Setting up and managing backup systems to ensure data can be recovered in case of hardware failure or other issues.

  i. Infrastructure Management: Managing the physical and virtual infrastructure, including servers, storage systems, and network devices.

  j. IT Asset Management: Tracking and managing IT assets, including hardware and software inventory, lifecycle management, and related compliance activities.

  k. Managing a Data Center: Overseeing the operations and security of a data center.

  l. Managing Virtual Resources: Managing and allocating virtual resources such as virtual machines and storage for operations.

  m. Hardware Configurations: Configuring hardware to meet specific organizational needs.

  n. Network Systems Management: Managing network systems for connectivity, operations, and security.

  o. Server Systems Management: Managing server systems for operations and security.