



Service Description

IBM Watson Platform for Health GxP

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

The Cloud Service is a Health Data-enabled platform as a service (PaaS), development platform, and operational subsystem for storing, curating, and processing Health Data. The Cloud Service is designed for clients who want to use cloud data services as part of a regulated solution. Client must acquire appropriate entitlements to enable the instances and capabilities listed below.

See Section 2 below for information pertaining to content and data protection within and outside the United States.

The Cloud Service is designed to support compliance with Part 11 of Title 21 of the U.S. Code of Federal Regulations and EU GMP Annex 11.

Health Data Enabled – means, as to the Cloud Service, the ability of the Cloud Service to meet applicable security and privacy standards, laws, and regulations for Health Data including the implementation specifications set forth in Part 164, Subparts A and C, of the regulations implementing HIPAA (as modified by the HITECH Act) and other applicable laws pertaining to Health Data, but does not mean that IBM is acting in the capacity of a Business Associate.

Health Data – means any Personal or Sensitive data or information, including images, that are health related. Protected Health Information (PHI) and other Health Data are managed in accordance with laws and regulations applicable to IBM when located in an IBM owned or controlled data center. Client must acquire appropriate entitlements to the Cloud Service to enable the features and capabilities described below.

GxP – means Good Laboratory Practices, Good Clinical Practices and Good Manufacturing Practices defined by global regulatory authorities, such as the United States Food and Drug Administration (FDA), and international quality management system standards for medical devices, ISO 13485.

Health Data Services

- **Health Data Integration**
 - Fast Health Interoperability Resources

Supports the Fast Health Interoperability Resources specification (FHIR) interface, enabling easier integration of health data into a standardized format ready for analytics. Supports near real-time and batch ingestion of files, documents, images or data.
- **Data Governance**
 - Patient Consent Management

The Cloud Service provides the framework to capture consent provided by patients or study participants and can securely store a record of consents apart from the data payload when the individual enrolls via a consent-enabled Client application. The Cloud Service also provides the ability to use a flexible Role-Based Access Control (RBAC) mechanism to access to an individual's data access and usage based on consent.
 - De-Identification Services

The Cloud Service provides the ability to separate any personal identifiers from structured data payloads. The Cloud Service receives data in the cloud through program APIs. The APIs enable separation of patient or individual name identifiers from the rest of the data payload, to be stored in a separate encrypted data store. The data payload is assigned an anonymized token that can be used in future provenance tracking.
- **Health Data Services**
 - Data Lake

Offers a repository for storing large volumes of raw health data or files.

- Data Reservoir
Houses client de-identified data, stored in a standardized format and ready for analytics.
- Patient Data Export
Provides a way to securely collect, store, export and share personal and sensitive information with approved external stakeholders across the value chain (including data scientists, developers, and chief medical officers), effectively allowing them to find insights using analytics models.
- Drug Dictionary Hosting
For customers who have licensed the World Health Organization's Drug Dictionary (WHO DD, available from WHO Uppsala Monitoring Center) as a global drug dictionary, the Cloud Service provides the ability to host the dictionary as part of a customer solution.
- **Audit Services Designed to Support Client's Compliance Activities**
The Cloud Service supports clients who seek 21 CFR Part 11 compliance and was built under an ISO13485 certified Watson Health quality management system (WH-QMS) that meets FDA 21 CFR Part 820 guidelines, critical for organizations seeking a cloud service with data and product quality controls, including audit services, required for conducting clinical trials and developing medical devices. The Cloud Service is also Health Insurance Portability and Accountability Act (HIPAA) and European Union's General Data Protection Regulation (GDPR)-enabled to address global health industry security and privacy requirements.

Developer Services

Select APIs and services are available to data scientists or to IBM services teams for building applications on behalf of the client. The Cloud Service enables application development and secure data collection from Client devices or devices of Client's authorized users. APIs provide program interfaces and documentation that Client's authorized users, including Client's third-party service providers, can use to develop applications and exchange data with the Cloud Service. Use of the APIs by Client or its developers is subject to compliance with the API Developer Requirements.

Health-Grade Foundational Services

- **Health and security standards**
Designed and managed to critical health and security standards, including HIPAA, GxP, 21 CFR Part 11 and ISO 13485, ISO 27001.
- **Multi-Tiered Security, including:**
 - Encryption
End to end encryption of PHI is performed for data at rest and in transit for applicable services.
 - Granular access management and authorization
Fine-grained access control of data based on users and defined roles.
 - Two Factor Authentication, Single Sign On
 - Supports authentication through SAML as the mechanism for Clients to integrate their Single Sign On (SSO) or directory services.
 - Leverages an access management solution and related components to manage security policies, where required.
 - Supports software-based two-factor authentication.
Provides basic role-based access control, as required; Supports the configuration of study, user profiles, roles, and user groups through program application programming interfaces ("API" or "APIs") that enable role-based access.
 - Intrusion Detection
Ongoing vulnerability and intrusion scanning is performed.

- Identity Management

Supports open-standards for external identity providers using open standards:

 - Supports open standards identity providers for large scale patient and user populations using OpenID Connect.
 - Leverages appropriate directory services and identity management capabilities to handle authentication for user populations where IBM is the identity provider.
- **Business Continuity and Resiliency**
 - Backup and Restore for Production Instances

Retention of system logs, access logs, and audit trail. Backups are performed daily for Production Instances. IBM will retain a backup copy of Client's data for a maximum period of defined by applicable regulations/laws.

Client is responsible for configuring the Cloud Service security to prohibit individual users from deleting data, and once the data is deleted Client acknowledges and agrees IBM is not obligated to recover the deleted data and, if available, may charge for such effort.
 - High availability

HA configurations of all services that are accessible via API.
 - Disaster recovery for Production Instances

If Client has purchased a Production instance, which includes disaster recovery, in the event of a major system disruption caused by a natural disaster (e.g. fire, earthquake, flood, etc.), disaster recovery will be accomplished by using commercially reasonable efforts to restore Client's production data with a recovery objective of 36 hours. This is not a warranty and no service level agreement is available.

In the event of a disaster that makes the Cloud Service unavailable, IBM shall promptly notify Client and activate the business continuity and/or disaster recovery plan. When a disaster is declared, the Cloud Service business continuity objective is to restore Client's access to the Cloud Services as follows: In the event of an outage, Recovery Time Objective (RTO) to restore IBM Watson Health production environment is within 36 hours of disaster declaration. Recovery Point Objective (RPO) is no more than 12 hours of loss of the Client's content within the production environment.
 - Availability Monitoring

The Cloud Service uses a synthetic monitoring solution to monitor, measure and report on availability or outages against committed service levels. This solution simulates and tracks user response and user experience at a global level – both for static availability and transactions.

The Cloud Service also uses an internal monitoring system for metrics, events, and alerts across the entire solution.

Watson Platform for Health GxP Environments

Each Watson Platform for Health GxP Instance is composed of either one or two separately deployed environments, depending on instance type, that operate as a single logical entity. In both types, the Instance can be ordered in one size (the Large Instance) that has the Health Data and Foundational Services deployed in a configuration using 32 compute nodes and 288TB of storage primarily dedicated to Client data storage.

Note: The storage available for Client Content is less than the absolute storage capacity stated above due to system overhead.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 Production Instance

A Production instance includes two GxP-enabled cloud environments paired in a DR configuration, designed to allow Client to process Health Data.

- **Potential Uses**

Provides the environment where Clients can deploy Health Data workloads into production. The production environment is a highly-available, load balanced environment and is able to fail over to a disaster recovery location.

- **Disaster Recovery**

Provides a mirror replica of the Production Instance; and is in a separate data center location.

- **High Availability**

Provides service architecture and design to continue processing and interacting without significant downtime after a component failure.

- **Multi-site Redundancy**

Provides a mirror replica of the Production Instance in a physically separated data center location.

- **Data Backup and Retention**

Maintains a backup of the client data and operational state to enable it to be restored in a properly configured Production Instance. The backup is retained per the retention policy of the specific Production Instance.

- **HIPAA- and GxP-enabled**

The Production Instances are GxP-enabled for electronic records under the WH-QMS.

- **Service Level Agreement**

A Production Instance includes availability credits as detailed in the following paragraphs.

- **Network Access**

External network (internet) access for client use is available.

1.1.2 Development / Test Instances

A Development / Test Instance includes a single GxP-enabled cloud environment, designed to allow Client to process Health Data, but does not include a paired DR environment.

- **Potential uses**

Provides an environment suitable for development, cognitive training, validation.

- **Single site**

A Development / Test Instance is deployed in a single data center location.

- **High Availability**

Provides service architecture and design to continue processing and interacting without significant downtime after a component failure.

- **HIPAA- and GxP-enabled**

The Development / Test Instances are GxP-enabled for electronic records under the WH-QMS.

- **Network Access**

External network (internet) access for client use is available.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below provide additional data protection information for the Cloud Services and its options regarding the types of Content that may be processed, the processing activities involved, the data protection features, and specifics on retention and

return of Content. The DPA applies if and to the extent the European General Data Protection Regulation (EU/2016/679) (GDPR) applies to personal data contained in Content.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=68779140ADAE11E6BE74C84817AAB206>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at https://www.ibm.com/software/support/saas_support_overview.html.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Instance is each access to specific configuration of the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

5.1 Client Acknowledgements

IBM is acting as an information technology provider only. IBM does not purport to be engaged in the practice of medicine or any other professional clinical or licensed activity, and the Cloud Service, all components thereof and future updates thereto, and all deliverables of related IBM professional services are not designed or intended to constitute protocols for delivering medical care, a substitute for professional medical advice, diagnosis or treatment or judgment, a drug, drug-adjunct technology, or drug development tool subject to quality system requirements or medical device as defined under the laws of any jurisdiction. As between IBM and Client, Client is solely responsible for complying with all such laws and regulations relative to Client's use of the Cloud Service and IBM's professional services.

Client may suggest that IBM enhance the Cloud Service or IBM's other offerings or services ("Feedback"). Client is under no obligation to provide Feedback and IBM is free to use all Feedback that Client provides.

Client agrees not to use any name, trade name, trademark, or other designation of IBM, including any contraction, abbreviation, or simulation of any of the foregoing in advertising, promotion, publication, publicity, or any marketing activity without IBM's prior written consent.

5.2 Client Compliance Support

IBM Watson Health's Quality and Regulatory team (WH Q&R) supports the quality management processes for this Cloud Service. The WH Q&R has oversight responsibility for the processes and procedures in accordance with the WH-QMS to support Client's audit readiness for life sciences regulatory compliance. IBM will support the Client during applicable life sciences regulatory agency audits and scheduled supplier audits. This support will include gathering and providing records of system validation, documentation of standard operating procedures, and records of relevant individual training, etc. to comply with FDA and global regulations. All IBM supplied records, including Client-specific and system-wide records may contain IBM Confidential information and shall be governed under the confidentiality agreement between the parties.

Client will be responsible for all regulatory compliance including:

- determining if the Cloud Services meets applicable regulatory compliance requirements; and
- regulatory compliance of all system components installed and integrating with the Cloud Service.

IBM Watson Health will maintain all client compliance-relevant records including but not limited to Design History File, Audit logs, Consent for storage and use of Personal Data, Employee training records in accordance with applicable life sciences regulatory agencies.

5.3 Multi-tenancy

Watson Health utilizes multi-tenancy for services. It is intended that the use of multitenancy will increase in future versions. If client chooses to have specific services dedicated to their use, additional charges will be incurred.

5.4 Upgrading to new versions

Over time, new versions of the Cloud Service will be made available to Client. IBM Watson Health will communicate the timing of new versions promptly and will work with Client to assess the impact to Client's software, compliance posture, and plan and collaborate on the upgrade to new versions. Client agrees to move to using the new version within 6 months of the version's availability. Watson Health reserves the right to renegotiate terms and charges if the transition period is not completed within 6 months of version availability.