IBM Watson Health Core

The Terms of Use ("ToU") is composed of this IBM Terms of Use - SaaS Specific Offering Terms ("SaaS Specific Offering Terms") and a document entitled IBM Terms of Use - General Terms ("General Terms") available at the following URL: **www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/**.

In the event of a conflict, the SaaS Specific Offering Terms prevail over the General Terms. By ordering, accessing or using the IBM SaaS, Client agrees to the ToU.

The ToU is governed by the IBM International Passport Advantage Agreement, the IBM International Passport Advantage Express Agreement, or the IBM International Agreement for Selected IBM SaaS Offerings, as applicable ("Agreement") and together with the ToU make the complete agreement.

1. IBM SaaS

The following IBM SaaS offerings are covered by these SaaS Specific Offering Terms:

- IBM Watson Health Core
- IBM Watson Health Core Access
- IBM Watson Health Core Terminology Service

2. Charge Metrics

The IBM SaaS is sold under one of the following charge metric(s) as specified in the Transaction Document:

a. Access is a unit of measure by which the IBM SaaS can be obtained. An Access is the rights to use the IBM SaaS. Client must obtain a single Access entitlement in order to use the IBM SaaS during the measurement period specified in Client's Proof of Entitlement (PoE) or Transaction Document.

b. Individual is a unit of measure by which the IBM SaaS can be obtained. An Individual is a single thing or human being. Sufficient entitlements must be obtained to cover each Individual processed by or managed by the IBM SaaS during the measurement period specified in Client's PoE or Transaction Document.

For purposes of this IBM SaaS, an Individual includes a person, device or mobile application whose data is managed by the IBM SaaS.

c. Instance is a unit of measure by which the IBM SaaS can be obtained. An Instance is access to a specific configuration of the IBM SaaS. Sufficient entitlements must be obtained for each Instance of the IBM SaaS made available to access and use during the measurement period specified in Client's PoE or Transaction Document.

3. Charges and Billing

The amount payable for the IBM SaaS is specified in a Transaction Document.

3.1 Partial Month Charges

A partial month charge as specified in the Transaction Document may be assessed on a pro-rated basis.

3.2 Overage Charges

If Client's actual usage of the IBM SaaS during the measurement period exceeds the entitlement stated on the PoE, then Client will be invoiced for the overage, as set forth in the Transaction Document.

4. Term and Renewal Options

The term of the IBM SaaS begins on the date IBM notifies Client of their access to the Pilot operating environment of the IBM SaaS, as documented in the Order Document. The subscription period for Individual entitlements begins when IBM notifies Client of their access to the Production operating environment. The Order Document will specify whether the IBM SaaS renews automatically, proceeds on a continuous use basis, or terminates at the end of the term

For automatic renewal, unless Client provides written notice not to renew at least 90 days prior to the term expiration date, the IBM SaaS will automatically renew for the term specified in the PoE.

For continuous use, the IBM SaaS will continue to be available on a month to month basis until Client provides 90 days written notice of termination. The IBM SaaS will remain available to the end of the calendar month after such 90 day period.

5. Technical Support

IBM will make available the IBM Software as a Service Support Handbook which provides technical support contact information, maintenance times, and other information and processes. Technical support contact information and other details regarding support operations can be found at: IBM SaaS Support Handbook: https://support.ibmcloud.com

Technical support and simple configuration requests for the IBM SaaS are provided through electronic submission. Technical support is offered with the IBM SaaS and is not available as a separate offering.

No Personal Information (PI) including Protected Health Information (PHI) and sensitive personal information (SPI) should be included in any documentation or information when reporting a problem incident.

6. Definitions

"**Applicable Laws**" means any laws, statutes or legislative enactments, rules, regulations, directives, mandates, decrees or other requirements issued by a governmental authority or any generally recognized industry standards that are applicable to the performance of this Terms of Use

"**API**" shall mean application program interface, which is a set of routines, protocols, and tools for building software applications. The API specifies how software components should interact and APIs are used when programming graphical user interface (GUI) components.

"**Authorized Administrator**" is any Client employee, approved Client contractor, individual, or group responsible for managing the upkeep and reliable operation of the platform. Responsibilities may include configuration, support, and user and account management. The administrator may also be a clinical investigator responsible for setting up a study in the Watson Health system.

"**Authorized Individual**" is any authenticated person, mobile application or device that has been given access to access rights to send data to the Watson Health Core. This may include the Client; or study participants, customers, or patients of Clients.

"**Client Applicable Data Laws**" means the Data Laws applicable to the performance of Client's obligations under the Agreement, Associated Documents, and applicable Services Descriptions, Order Documents and Statements of Work between the Parties.

"**Client Data**" means any data input in the IBM SaaS by or for Client, whether Client's own data or data entered by or on behalf of Client's customer or any third party, and including any data from a third-party wellness health device.

"**Data Laws**" means any Applicable Laws that relate to data protection, privacy, or security.

"**Data Subject**" means an identified or identifiable individual to whom Personal Data relates.

"**Designated Data Center**" means the data center(s) specified for primary and disaster recovery data centers in the Transaction Document that runs Client's instance of the IBM SaaS, if applicable.

"**Health Data**" means any data or information, including images, that are health related Personal Information.

"**Health Data Enabled**" means, as to the IBM SaaS, the ability of the IBM SaaS to meet applicable security and privacy standards, laws, and regulations in In-Scope Jurisdictions 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 or a Data Controller.

"**HIPAA**" means the Health Insurance Portability and Accountability Act of 1996, as amended, including by the Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), certain regulations promulgated under HIPAA by the United States Department of Health and Human Services at 45 C.F.R. Parts 160 and 164 and certain regulations promulgated pursuant to the HITECH Act.

"**IBM Applicable Data Laws**" means the Data Laws applicable to the performance of IBM's obligations under the Agreement, Associated Documents, and applicable Services Descriptions, Order Documents and Statements of Work between the Parties.

"**IBM Personnel**" means (a) IBM, its Affiliates, and its subcontractors, and with respect to each of the foregoing, their employees; and (b) any third party suppliers; in each case that performs services on IBM's behalf pursuant to the Agreement and applicable Associated Documents or to whom IBM otherwise authorizes access to Client Personal Data.

"**In-scope Countries**" means the 28 European Union Member States and Switzerland, and those countries that IBM may add to this list from time to time.

"**Personal Data or Personal Information**" means information in any media or format, including electronic and paper records, that relates to an identified or identifiable individual, an "identifiable individual" being someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity.

"**Process**" and variants of it, such as "**processing**" (whether capitalized or not) means any operation or set of operations which is performed upon data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Processed Data**" means any data, confidential or proprietary information or materials, including Health Data and Personal Data, that is processed by IBM pursuant to the Agreement, an Associated Document, and/or a Services Description, Order Document and/or Statement of Work.

"**Security Incident**" has the meaning set forth in the SBCA.

7. Account Management

The IBM SaaS is accessible to Client's authorized users ("**Authorized Administrators**" or "**Authorized Individuals**") only. The Client will control the accounts authorized to access the IBM SaaS, which may include authorized applications, Client personnel, Client's third party service providers and contractors, and is solely responsible for (i) controlling all authorized users, including without limitation, verification of the identity of any authorized user; and (ii) ensuring that only authorized users access the IBM SaaS.

Authorized Individuals that are customers, patients or study participants of the Client may be given access solely for the purpose of uploading data to the IBM SaaS, in which case such Authorized Individuals will have no other access to the IBM SaaS.

8. Privacy

8.1 General Requirements

As between the Parties, Client is the sole controller of all Client Personal Data, and Client appoints IBM as a data processor. In accordance with the Applicable Data Laws, Client has the right to instruct IBM in connection with IBM's processing of Client Personal Data.

To the extent IBM processes Client Personal Data, IBM shall:

a. comply with all IBM Applicable Data Laws;

b. not comingle Client Personal Data with data from other sources except:

- as necessary to provide IBM SaaS and then not for any other purpose, unless specifically instructed by Client to do so; or
- in accordance with the terms of this Terms of Use and the SBCA Appendix.

To the extent IBM processes Client Personal Data, Client shall:

a. comply with all Client Applicable Data Laws;

b. be responsible for all communications by Client with Client' Affiliates, patients, end users, Data Subjects and/or other Client third parties;

c. enter into data processing agreements with its controllers that are required to allow IBM as a data processor and its sub-processors to process any Client Personal Data;

d. serve as a single point of contact for IBM and is solely responsible for the internal coordination, review and submission of instructions or requests of Client Affiliates that are other controllers to IBM. IBM shall be discharged of its obligation to inform or notify any Client Affiliate that constitutes a controller when it has provided such information or notice to Client. IBM is entitled to refuse any instructions provided directly by any Client Affiliate that constitutes a controller that is not Client.

Neither party shall be required to act in violation of such party's Applicable Data Laws.

8.2 Client Data Rights

Client represents and warrants that it (a) owns the data that it will input into the IBM SaaS, or (b) has obtained, and is responsible for maintaining, all necessary rights, permissions, consents and authorizations to grant IBM the rights to access, use, and disclose the Client Data in accordance with the terms set forth in this Terms of Use or the Agreement or as otherwise necessary for IBM to provide the IBM SaaS. Client further represents and warrants that the Client Data will only be either (a) related to individuals residing in the United States and will then only be inputted into the IBM SaaS at the United States data center or (b) related to individuals residing in one or more In-Scope countries and will then only be inputted into the IBM SaaS at the Designated Data Center(s).

8.3 Data Services and Responsibilities

a. Client agrees that it will only perform analytics or request that IBM perform analytics on the Client Data in connection with activities that constitute either the Client's "health care operations" or "research" as each is defined under HIPAA and/or similar terms under other Applicable Data Laws and that Client will use the Client Data or direct IBM to use the Client Data only in accordance with all relevant requirements (e.g. Institutional Review Board determination or waiver where required) under these and any other Client Applicable Data Laws.

b. Client is solely responsible for obtaining any and all registrations, consents, authorizations, and permissions as required by Client Applicable Laws in each applicable In-Scope Country, including, without limitation, HIPAA and any other applicable data privacy and security laws, rules, and regulations, in order for the Client Data to be inputted into the IBM SaaS and used and disclosed as contemplated under this Terms of Use and the Agreement by Client and by IBM and IBM's permitted subcontractors. IBM shall have no responsibility for monitoring when such registrations, consents, authorizations and permissions are received or required.

c. Client is solely responsible for ensuring that all Client's Data inputted in the IBM SaaS is limited to data relating to individuals residing in the United States or in an applicable In-Scope country.

d. IBM shall have support centers with personnel trained on HIPAA and other IBM Applicable Data Laws regarding data from In-Scope countries.

8.4 Security Measures and Security Incidents

a. IBM shall implement, maintain and comply with the technical and organizational measures (including organizational processes and procedures, and including any specific security obligations set out or referred to in this Terms of Use and the SBCA to protect the Client Personal Data from unauthorized use or access, accidental loss, damage, modification, destruction, theft or unauthorized disclosure.

b. In the event that IBM becomes aware of a Security Incident (as defined by the SBCA) involving Client Processed Data, IBM shall inform Client in accordance with the terms of the SBCA and IBM Applicable Data Laws and such notice will include information regarding any known impact on Client or any Data Subjects (if any) affected by such Security Incident and the corrective action taken or proposed to be taken by IBM.

8.5 Receipt of Inquiries and Complaints

IBM shall notify Client in writing promptly and, to the extent allowed by IBM Applicable Data Laws, not later than five (5) business days following IBM Watson Health Data Privacy Officer's receipt of any inquiry, communication or complaint received by IBM in relation to Client Personal Data from:

a. Any Data Subject, relating to Personal Data about such Data Subject Processed by IBM. Client shall respond to any such requests from Data Subjects and IBM will comply with reasonable instructions of Client in assisting Client to respond to such requests. If required by IBM Applicable Laws, IBM may respond directly to such requests, provided that IBM notifies Client in advance of any such response and reasonably coordinates with Client with respect to the form and content of such response, when permitted by IBM Applicable Laws or otherwise possible.

b. any legal or regulatory authority, relating to the Processing by IBM of any Client Personal Data, provided that IBM may respond to such requests received from a governmental agency with a subpoena or similar legal document compelling disclosure by IBM or as otherwise required by Applicable Data Law, provided that IBM notifies Client in advance of any such disclosure and

reasonably coordinates with Client with respect to the form and content of such response, where permitted by law or otherwise possible.

8.6 Processing of Client Personal Data

IBM shall restrict the disclosure of Client Personal Data to those IBM Personnel who may be required to assist it in providing the Services.

IBM shall comply with any reasonable request from Client requiring IBM to amend, correct, delete or block Client Personal Data in accordance with Applicable Law.

Upon request by either Party, IBM, Client or their Affiliates will enter into standard agreements required by law for the protection of Client Personal Data. The Parties agree (and will procure that their respective Affiliates agree) such agreements will be subject to the limitation and exclusions of liability in this Agreement for purposes of claims between the Parties. The Parties shall cooperate in entering into (or procuring that such Party's Affiliates enters into) and complying with further mutually agreed terms or agreements as may be required by Applicable Data Laws.

8.7 Return of Client Personal Data

On expiry or termination of the Agreement, IBM shall, and shall cause all IBM Personnel to, cease to use or process any Client Proprietary Information and any Client Personal Data and shall, at Client' option and request:

a. promptly return in a format and on storage media that Client may reasonably request all Client Proprietary Information and Client Personal Data that IBM is electronically storing and upon Client' confirmation of receipt, delete, destroy, or otherwise make permanently unreadable or indecipherable the Client Proprietary Information and the Client Personal Data, including copies and back-ups. IBM may charge for the cost of storage media and certain activities performed at Client' request (such as delivering Client Proprietary Information and Client Personal Data in a specific format or destroying the Client Proprietary Information and Client Personal Data in a particular manner).

b. directly delete destroy, or otherwise make permanently unreadable or indecipherable the Client Proprietary Information and Client Personal Data, including copies and back-ups.

8.8 Business Associate Agreement

To the extent appropriate and required by HIPAA, IBM and Client will enter into a Business Associate Agreement ("BAA"), which shall govern IBM's obligations as a Business Associate of Client in the provision of the IBM SaaS. Without limiting IBM's express obligations under the Agreement and the BAA if applicable, Client acknowledges and agrees that it is responsible for determining the applicability of, and complying with, all Applicable Laws and licensing requirements that apply to Client's use or other activities with respect to (including use or other activities by Authorized Users) the IBM SaaS

8.9 European Union Data Processing Addendum

If Client directs IBM to process European Union Personal Data, IBM and Client will enter into a Data Processing Addendum including, as appropriate, E.U. Model Clauses, with optional clauses removed.

9. IBM SaaS Offering Additional Terms

9.1 Security

This IBM SaaS follows IBM's data security and privacy principles for IBM SaaS which are available at www.ibm.com/cloud/data-security and the additional terms set forth below and in the Security and Business Continuity Appendix to this Terms of Use. Any change to IBM's data security and privacy principals will not degrade the security of the IBM SaaS.

IBM Watson Health Core implements security policies, standards, and processes based on the ISO 27001 framework as further described in the Security Description. Among its security capabilities, the solution implements the following:

a. **Secure Operating Zones.** IBM Watson Health Core implements a defense in depth strategy, utilizing multiple security zones to manage cloud integration points such as data onboarding and custom application development.

b. **Encryption.** All Client Data is encrypted at rest and in flight. All data in transit to and from IBM Watson Health Core are encrypted. A shared service provides encryption key management. Client

is responsible for all network connectivity and quality between IBM Watson Health Service and Client's proxy server.

c. **Security Event Monitoring.** IBM leverages its security intelligence platform for security information and event management, log management, incident forensics, threat detection and vulnerability management.

d. **Identity Management**

- Watson Health Core supports open standards identity providers for large scale patient and user populations using OpenID Connect;
- For user populations where IBM is the identity provider, Watson Health Core leverages appropriate directory services and identity management capabilities to handle authentication.

e. Strong Authentication and Role Based Access

- Watson Health Core supports authentication through SAML as the mechanism for Clients to integrate their Single Sign On (SSO) or directory services.
- Watson Health Core leverages an access management solution and related components to manage security policies, where required.
- Watson Health Core supports software-based two-factor authentication.
- Watson Health Core provides basic role-based access control, as required; Watson Health Core supports the configuration of study, user profiles, roles, and user groups through program application programming interfaces ("API" or "APIs") that enable role based access.

9.2 Cookies

Client is aware and agrees that IBM may, as part of the normal operation and support of the IBM SaaS, collect personal information from Client (your employees and contractors) related to the use of the IBM SaaS, through tracking and other technologies. IBM does so to gather usage statistics and information about effectiveness of our IBM SaaS for the purpose of improving user experience and/or tailoring interactions with Client. Client confirms that it will obtain or have obtained consent to allow IBM to process the collected personal information for the above purpose within IBM, other IBM companies and their subcontractors, wherever we and our subcontractors do business, in compliance with applicable law. IBM will comply with requests from Client's employees and contractors to access, update, correct or delete their collected personal information.

9.3 Derived Benefit Locations

Where applicable, taxes are based upon the location(s) Client identifies as receiving benefit of the IBM SaaS. IBM will apply taxes based upon the business address listed when ordering an IBM SaaS as the primary benefit location unless Client provides additional information to IBM. Client is responsible for keeping such information current and providing any changes to IBM.

9.4 Continuous Delivery

Client is entitled to capabilities and enhancements made to the solution and deployed by IBM in a continuous cloud delivery model.

9.5 Backup and Restore

IBM Watson Health Core provides backup of Client Data in the production environment (including the Data Lake and Data Reservoir repositories) to the last known good state for the purpose of recovering service in the event of system failure.

9.6 High Availability

IBM Watson Health Core components in the production environment are implemented in high availability configurations, with database servers clustered for redundancy to provide workload distribution and eliminate single point of failures.

9.7 Disaster Recovery

IBM's approach for disaster recovery consists of multiple data centers in dispersed geographical areas to achieve its business continuity objectives as follows for its Production environment:

- RTO – within 36 hours of disaster declaration
- RPO – no more than 24 hours of loss of Client's content

9.8 Measurement Tools

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

9.9 Publicity

Client agrees IBM may publicly refer to Client as a subscriber to the IBM SaaS in a publicity or marketing communication.

Appendix A

1. IBM Watson Health Core

IBM Watson Health Core is a Health Data Enabled platform as a service (PaaS), development platform, and operational subsystem for storing, curating, and processing Protected Health Information (PHI), as defined by HIPAA, and other Health Data in accordance with IBM Applicable Data Laws located in an IBM owned or controlled data center. Client must acquire appropriate entitlements to IBM Watson Health Core and IBM Watson Health Core Access to enable the features and capabilities described below.

1.1 Watson Health Core Operating Environments

The Watson Health Core entitlement encompasses three Health Data Enabled cloud operating environments, designed to allow Client to process Health Data.

- **Pilot** provides a sandbox environment where Clients can develop and test applications built using the IBM SaaS. The pilot environment implements all of the HIPAA security controls except for Disaster Recovery, high availability and backup of systems of record.
- **Production** environment provides the full scale environment where Clients can deploy Health Data workloads. 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 environment; and is located in a separate data center location.

1.2 Application Development

IBM Watson Health Core 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 IBM SaaS. Use of the APIs by Client or its developers is subject to compliance with the API Developer Requirements.

- **REST APIs.** Watson Health Core provides a series of REST APIs and services for the Watson Health Core platform. API capabilities include, but not limited to, mechanisms to access the data repositories, the data curation service, user management, and audit logs.
- **Apple HealthKit and Apple ResearchKit.** Watson Health Core supports integration with the Apple ResearchKit API framework for iOS based research studies, and with Apple HealthKit to capture wellness data.

1.3 Data Governance

- **Consent Management.** Watson Health Core 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.
- **Data Masking.** Watson Health Core provides the ability to separate name identifiers from structured data payloads. Watson Health Core 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.

1.4 Health Data Services

Watson Health Core provides collection, storage, synchronization of data, including exogenous Health Data and other Personal Information, both structured and unstructured.

- Data Ingestion. Watson Health Core provides the ability to ingest data from patient applications or devices through program APIs. Watson Health Core entitles each of the Client's Authorized Individuals to upload up to 25 MB of data to the Health Core each year of the contract term. The service accommodates up to 10 uploads per Individual per day.

- **Operational Data Lake.** Raw Client or patient data is stored in Watson Health Core in its native form until needed for analytics and modeling.
- **Extract Transform Load (ETL)**. Data is transformed into a normalized format within the operational sub system. An industry standards based Enterprise Service Bus for healthcare facilitates allows for integration across different Client applications and protocols.
- **Data Reservoir.** Once curated, data is moved to the Data Reservoir. Watson Health Core utilizes aspects of the IBM Unified Data Model for Healthcare to normalize business and technical health data for use in analytics.
- **Master Person Index.** Watson Health provides Master Data Management tools in order to consolidate data from multiple sources to create a Longitudinal Person Record (LPR).

2. Optional Features

2.1 IBM Watson Health Core Terminology Service

This add-on service facilitates data integration and interoperability between disparate health systems, providing consistent clinical terminology usage across all Watson Health Cloud applications. This service provides the functional platform for all tasks involving terminologies, code systems, and structured content, such as:

- creation of new code systems
- translation of international code systems
- mappings between local code lists and international standards

Appendix B

IBM provides the following availability service level agreement ("SLA") for the IBM SaaS as specified in a PoE. The SLA is not a warranty. The SLA is available only to Client and applies only to use in production environments.

1. Availability Credits

Availability rebates are only applicable to subscription fees for Individual entitlements.

Client must log a Severity 1 support ticket with the IBM technical support help desk within 24 hours of first becoming aware of an event that has impacted the IBM SaaS availability. Client must reasonably assist IBM with any problem diagnosis and resolution.

A support ticket claim for failure to meet an SLA must be submitted within three business days after the end of the contracted month. Compensation for a valid SLA claim will be a credit against a future invoice for the IBM SaaS based on the duration of time during which production system processing for the IBM SaaS is not available ("Downtime"). Downtime is measured from the time Client reports the event until the time the IBM SaaS is restored and does not include time related to a scheduled or announced maintenance outage; causes beyond IBM's control; problems with Client or third party content or technology, designs or instructions; unsupported system configurations and platforms or other Client errors; or Client-caused security incident or Client security testing. IBM will apply the highest applicable compensation based on the cumulative availability of the IBM SaaS during each contracted month, as shown in the table below. The total compensation with respect to any contracted month cannot exceed 20 percent of one twelfth (1/12th) of the annual charge for the IBM SaaS.

2. Service Levels

Availability of the IBM SaaS during a contracted month

Availability during a contracted month	Compensation (% of monthly Individual subscription fee* for contracted month that is the subject of a claim)
< 99.95%	10%
< 99.0%	20%

* If the IBM SaaS was acquired from an IBM Business Partner, the monthly subscription fee will be calculated on the then-current list price for the IBM SaaS in effect for the contracted month which is the subject of a claim, discounted at a rate of 50%. IBM will make a rebate directly available to Client.

Availability, expressed as a percentage, is calculated as: the total number of minutes in a contracted month minus the total number of minutes of Downtime in a contracted month divided by the total number of minutes in the contracted month.

Example: 108 minutes total Downtime during contracted month

$$\frac{\text{43,200 total minutes in a 30 day contracted month} - \text{108 minutes Downtime} = \text{43,092 minutes}}{\text{43,200 total minutes}} = \text{10\% Availabilty credit for 99.75\% availability during the contracted month}$$

3. Exclusions

This SLA does not apply to the following:

- Aside from server monitoring, the SLA does not apply to hosted virtual machines to support custom or Client applications.
- If Client has breached any material obligations under the current agreement obligations.

Appendix C

This Security and Business Continuity Appendix (this "SBCA") sets forth certain requirements and obligations of IBM in its provision of the IBM SaaS to Client. The requirements and obligations set forth herein are in addition to those set forth in the description of principles for data security for IBM SaaS which are available at www.ibm.com/cloud/data-security. Capitalized terms that are not defined herein shall have the meanings set forth in the Agreement or Terms of Use.

1. Information Security Program

IBM has internal security policies, standards and processes based on the ISO 27001 framework and control areas. In addition to IBM Corporate Security Organization governance, these policies, standards, and processes are regularly the subject of internal audits.

IBM maintains an information security program of organizational, operational, administrative, physical, and technical safeguards governing the processing, storage and transmission of Client content that at minimum are consistent with the requirements of this SBCA.

IBM shall share with Client, at Client's request, information about the IBM Watson Health information security program so that Client can reasonably determine its continuing suitability, adequacy and effectiveness. The IBM Watson Health information security program shall be updated from time to time, to stay current with generally accepted industry practices and IBM Applicable Laws.

2. Access Controls

IBM shall disclose Client content only to its employees, subcontractors or third parties who have a legitimate business need to access such Client content in order to assist IBM to carry out its obligations to Client or other persons as required to provide the IBM SaaS in accordance with Applicable Laws, the Agreement or an Associated Document, as applicable. In the event IBM is a Business Associate of Client, IBM and Client shall disclose Personal Health Information only in accordance with the terms of an applicable Business Associate Agreement between the Parties.

IBM has a formal, internal user access management process whereby user access is formally requested, approved upon identity verification, and is granted based on the need to know, utilizing the concept of least privilege. Access to Client content shall be restricted only to active users and active user accounts. IBM has a formal process for periodic internal access revalidation of active user accounts.

IBM uses secure user authentication protocols, including assigning unique identifications and strong passwords for active user accounts on systems used to provide services to Client in accordance with IBM corporate security standards and policies:

a. Passwords shall not be vendor supplied default passwords and shall be kept in a location and/or format that do not compromise the security of the data they protect.

b. The display and printing of passwords must be masked, suppressed, or otherwise obscured such that unauthorized parties are not able to observe or subsequently recover them. Passwords must not be logged or captured as they are being entered. User passwords must not be stored in clear text.

c. Passwords for each technology comprising the IBM SaaS are chosen to mitigate the risks associated with known password length vulnerabilities and must be documented.

d. When use of internal, privileged, shared functional IDs are required for operational reasons, IBM manages shared, functional, and/or System IDs requiring check out of passwords to maintain individual accountability.

Inactivity timeouts are established for all systems and applications that store Client content.

If required, remote access to IBM's network, systems and applications that store Client content shall be established upon Client request and IBM's formal approval, and all such remote connections shall be secured using strong authentication and encryption protocols. Remote access activity shall be logged and monitored.

To the extent that delivery of the IBM SaaS requires IBM to remotely access any system within Client's internal networks, all such remote access will be performed solely using Client's secure remote access

systems and protocols and using access credentials provided to IBM by the Client. Remote access to Client's network shall be established only upon request by IBM and approval by the Client, and in accordance with Client's then-current policies, which will be provided to IBM in advance. IBM's use of the Client's internal networks will be subject to Client's IT usage and security policies, which will be provided to IBM in advance.

IBM implements separation of duties for security administration, access review, and security violation investigations.

Storage, hosting and processing of Client content specific to Client are logically separate from that of other clients serviced by IBM. In instances where a shared storage, hosting or processing work area is authorized by Client, IBM shall have procedures and safeguards in place consistent with the requirements set forth in this SBCA that are designed to prevent the unauthorized disclosure of such Client content.

IBM implements clean desk/clear screen policies to make sure that Client content is not left unattended in any public place at any time.

3. Transfer and Encryption

IBM shall take appropriate precautions transmitting Client content (by fax, email, courier, etc.) to make sure that the correct contact information is used for the recipient and making prior arrangements with the intended recipient to secure the receipt of such information.

IBM uses, and will cause IBM Personnel to use, appropriate forms of encryption or other secure technologies at all times in connection with the processing of Client content, including in connection with any transfer, communication, remote access or storage (including back-up storage) of Client content. For example, IBM shall encrypt, using an appropriate industry-standard encryption, all records and files containing Client content:

a. stored on IBM laptops, portable devices or portable electronic media including backup tapes when in transit to an offsite storage facility

b. stored or transported by IBM outside of Client's or IBM's physically secured offices and facilities, excluding hard copy paper documents

c. while traveling across public networks by IBM

d. while being transferred from IBM's systems to Client

e. while being transmitted wirelessly by IBM

f. stored by IBM on servers and databases

4. Network Security

IBM uses reasonably up-to-date versions of system security software such as firewalls, proxies, web application firewalls and interfaces. Such software must include malware protection and reasonably up-to-date patches and virus definitions. In accordance with corporate standards, antivirus software shall be installed on workstations, servers and related endpoints where technically feasible and the software is managed to corporate policy with internal management solutions.

IBM monitors the IBM SaaS to detect and identify security incidents as early as possible. IBM shall maintain, at minimum, industry standard intrusion detection tools and prevention, monitoring and response processes in a manner designed to identify both internal and external vulnerabilities and risks that could result in unauthorized disclosure, misuse, alteration, or destruction of Client content or information systems that are used to deliver services to Client.

IBM subscribes to vulnerability intelligence services or to information security advisories and other relevant sources providing current information about system vulnerabilities. IBM performs regular vulnerability assessments and remediation of its network.

IBM monitors the IBM SaaS to detect, identify, contain, and resolve Security Incidents.

IBM validates the availability, integrity and effectiveness of the network security infrastructure on which the IBM SaaS is made available, through the IBM release management processes.

5. Incident Management and Notifications

IBM Watson Health teams work in conjunction with the IBM Cybersecurity Incident Response Team, a global team that manages the receipt, investigation and internal coordination of security incidents related to IBM offerings, and to implement preventive steps necessary to reduce software related security issues.

A “Security Incident” is the successful unauthorized access, use, disclosure, modification, or interference with system operations or data in an information system used by IBM to provide the IBM SaaS. If a Security Incident is discovered (via routine scanning, alerts, threshold events etc.), IBM shall inform and notify Client:

a. Of any confirmed Security Incident involving Client content as soon as practicable and in no event later than 2 business days after investigation and confirmation of such Security Incident;

b. Promptly following any request for access to, or information about, any Client content from any government official (including any data protection agency or law enforcement agency) unless prohibited from doing so by law or relevant order;

c. Except as permitted in section titled Access Controls of this SBCA, in advance of any disclosure or transfer of, or access to, Client content to or by a third party;

6. Logging

IBM maintains, in accordance with IBM’s policies and practices and generally accepted industry practices, reasonable monitoring of systems for unauthorized use of or access to Client Processed Data. Actual or attempted logon violations and access violations shall be logged.

IBM maintains records of all access requests and logs of access activities for all systems that store, access, process and transmit Client and Health Data for as long as required by HIPAA and other IBM Applicable Data Laws.

The logs and reports include, at minimum: (i) all login attempts, whether or not successful, including reasonable identifying information; (ii) all system and network configuration changes, including application installations, user management changes, and modifications to file access permissions; (iii) resource access attempts, whether successful or not, including attempts to access any file, network share, log, or other resource; and (iv) data downloads, including the content type of the data and access protocol used to achieve the download.

7. Software Application Development and Change Management

IBM follows secure application development and coding practices that protect the integrity of production applications and associated source code from unauthorized and untested modifications.

IBM follows a change management process which includes (a) recording and formal approval of changes, and back out procedures; and (b) appropriate testing of such changes, including user acceptance testing where appropriate, as well as security testing.

IBM follows a patch management process that includes testing patches before installation on all systems used to store, access and transmit Client content or are used to deliver services, including IBM SaaS, to Client.

IBM requires that system administrators maintain complete, accurate, and up-to-date information regarding the configuration of all information systems used to store, access and transmit Client content.

8. Physical and Environmental Security

IBM Watson Health Core platform is deployed upon IBM SoftLayer data infrastructure. IBM SoftLayer maintains physical and environmental security, access control, controls and processes to protect Client data from human, environmental, and technical breach or impact.

General access to the facilities in which the IBM SaaS is hosted is controlled by the use of a card access system. Closed circuit television (CCTV) cameras are installed throughout the sites and monitored by security personnel. Selected access doors are alarmed and security personnel monitor these alarms.

Access to controlled areas is restricted through the use of card access and/or additional biometric verification. All individuals without authorized access to the controlled areas must sign in and be escorted by an individual with approved controlled area access. All controlled area emergency exits have audible alarms and security personnel monitor these alarms. Periodic verification that the alarms are functioning is performed, documented, and retained. Access rights to controlled areas are fully revalidated on a quarterly basis. Access to controlled areas is revoked upon termination of employment.

Facilities are protected against environmental factors such as fire, water, and heat through fire alarms, fire extinguishers, smoke alarms, and fire suppression and extinguishing systems. Facilities are protected against power disruptions or failures through Uninterruptible Power Supply (UPS) systems and backup generators, which are maintained and tested on a regular basis.

IBM SoftLayer compliance information and reports can be found at: http://www.softlayer.com/compliance

9. Continuity of Business Operations

IBM has business continuity and disaster recovery plans which are designed to maintain a level of service consistent with its obligations under the Agreement. Such business continuity and disaster recovery plans shall be periodically updated and tested (at least once per year). IBM shall implement all reasonable changes to business continuity and disaster recovery plans necessary to remain in compliance with generally accepted industry practices, in each case without unreasonably interfering with the IBM SaaS or production environment in use by Client.

In the event that a disaster arises that makes the IBM SaaS unavailable to Client, IBM shall promptly notify Client and activate the business continuity and/or disaster recovery plan. When a disaster is declared, the IBM SaaS business continuity objective is to restore Client's access to the IBM SaaS 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 24 hours of loss of the Client's content within the production environment. Specific Watson Health solutions business continuity objectives may vary.

IBM's approach for disaster recovery consists of multiple datacenters in dispersed geographical areas.

All IBM SoftLayer data centers maintain multiple power feeds, fiber links, dedicated generators, and battery backup. They are built from industry-leading hardware and equipment, providing the highest level of performance, reliability, and interoperability. All of data center components to include, redundant n+1 power and cooling resources for example, are inspected to maintain stability in within the data centers.

10. Compliance

IBM's security practices are based on ISO 27001-27002. These practices provide control structures for, but not limited to, Risk Analysis, Physical Security, Emergency Planning, Investigations, Information Protection, Education, Data protection, and Operations.

IBM reviews security and privacy related activities for compliance with IBM's security practices.

IBM complies with IBM Applicable Data Laws in In-Scope Jurisdictions.

Proper handling of Clients' confidential information is also required under IBM's Business Conduct Guidelines, which all employees must review (and certify their review of) on an annual basis.

11. Miscellaneous

IBM shall ensure that its agreements with all subcontractors and/or third parties engaged in the delivery of the IBM SaaS have terms that are at least as protective of Client content as those in this SBCA, and any applicable Associated Document, each to the extent such terms are applicable to the services to be performed by such subcontractors and/or third parties.