Conditions d'Utilisation IBM – Conditions spécifiques de l'Offre SaaS

IBM Watson Health Core

Les Conditions d'Utilisation regroupent les présentes Conditions d'Utilisation IBM – Conditions Spécifiques de l'Offre SaaS (« Conditions Spécifiques de l'Offre SaaS ») et un document intitulé Conditions d'Utilisation IBM – Conditions Générales (« Conditions Générales ») disponibles à l'adresse URL suivante : http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

En cas de conflit, les Conditions Spécifiques de l'Offre SaaS prévalent sur les Conditions Générales. En accédant à l'Offre IBM SaaS, en la commandant ou en l'utilisant, le Client de l'Offre IBM SaaS accepte les présentes Conditions d'Utilisation.

Les Conditions d'Utilisation sont régies par le Contrat International IBM Passport Advantage, le Contrat International IBM Passport Advantage Express ou le Contrat International IBM relatif à une Sélection d'Offres IBM SaaS, selon le cas (ci-après le « Contrat ») qui, avec les Conditions d'Utilisation, représentent l'intégralité de l'accord entre les parties.

1. Offres IBM SaaS

Les Conditions Spécifiques de l'Offre SaaS s'appliquent aux Offres IBM SaaS suivantes :

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

2. Unités de mesure des redevances

L'Offre IBM SaaS est vendue en fonction d'une des unités de mesure de redevance suivantes précisée dans le Document de Transaction :

a. **Accès** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un Accès est le droit d'utilisation de l'Offre IBM SaaS. Le Client doit se procurer une autorisation d'Accès unique pour utiliser l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (ci-après « Autorisation d'Utilisation » ou « PoE ») ou le Document de Transaction du Client.

b. **Individu** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Un Individu est un objet ou un être humain unique. Des droits d'utilisation suffisants sont nécessaires pour couvrir chaque Individu traité ou géré par l'Offre IBM SaaS pendant la période de mesure indiquée dans l'Autorisation d'Utilisation (« PoE ») ou le Document de Transaction du Client.

   Dans le cadre de cette Offre IBM SaaS, un Individu inclut une personne, un appareil ou une application mobile dont les données sont gérées par l'Offre IBM SaaS.

c. **Instance** : unité de mesure par laquelle l'Offre IBM SaaS peut être acquise. Une Instance est l'accès à une configuration spécifique de l'Offre IBM SaaS. Des droits suffisants sont nécessaires pour chaque Instance de l'Offre IBM SaaS mise à disposition à des fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'Utilisation ou le Document de Transaction du Client.

3. Redevances et facturation

Le montant à régler pour l'Offre IBM SaaS est indiqué dans un Document de Transaction.

3.1 Redevances Mensuelles Partielles

Une Redevance Mensuelle Partielle, comme indiqué dans le Document de Transaction, peut être estimée au prorata.

3.2 Redevances de dépassement

Si l'utilisation réelle de l'Offre IBM SaaS par le Client pendant la période de mesure dépasse les droits indiqués dans l'Autorisation d'Utilisation (ou « PoE »), le Client sera facturé pour l'excédent, comme stipulé dans le Document de Transaction.

4. Durée et Options de Renouvellement

La durée de l'Offre IBM SaaS commence à la date à laquelle IBM notifie au Client que ce dernier a accès à l'environnement d'exploitation Pilote de l'Offre IBM SaaS, comme décrit dans le Bon de Commande. La période d'abonnement pour les droits d'utilisation Individu commence lorsqu'IBM notifie au Client que ce dernier a accès à l'environnement d'exploitation de Production. Le Bon de Commande indiquera si l'Offre IBM SaaS est renouvelée automatiquement, si elle se poursuit en continu ou si elle prend fin à l'issue de la durée.

Pour un Renouvellement Automatique, l'Offre IBM SaaS est automatiquement renouvelée pour la durée indiquée dans l'Autorisation d'Utilisation, sauf si le Client notifie par écrit, avant la date d'expiration de la durée, son intention de ne pas renouveler.

Pour une utilisation en continu, l'Offre IBM SaaS continuera d'être disponible mois par mois jusqu'à ce que le Client notifie la résiliation moyennant un préavis écrit de 90 jours. L'Offre IBM SaaS demeure disponible jusqu'à la fin du mois suivant ladite période de 90 jours.

5. Support Technique

IBM mettra à disposition le manuel IBM Software as a Service Support Handbook qui contient les coordonnées des personnes à contacter, les délais de maintenance ainsi que des informations et processus relatifs au support technique. Les coordonnées des personnes à contacter ainsi que les détails relatifs au support technique sont disponibles à l'adresse https://support.ibmcloud.com.

Le support technique et les demandes de configuration simple destinés aux Offres IBM SaaS sont fournis par voie de transmission électronique. Le support technique est proposé avec les Offres IBM SaaS et n'est pas disponible en tant qu'offre distincte.

Aucune Information Personnelle (« PI »), notamment aucune Information Personnelle sur la Santé (« PHI ») et aucune Information Personnelle Sensible (« SPI »), ne doit être incluse dans les documentations ou communications lorsqu'un incident est signalé.

6. Définitions

Lois Applicables : tous règlements, lois, statuts, textes de loi, directives, dispositions, décrets ou autres exigences établis par une instance gouvernementale ou toutes normes en vigueur dans le secteur d'activité qui sont applicables à l'exécution des présentes Conditions d'Utilisation.

API (interface de programmation d'application) : ensemble de routines, de protocoles et d'outils permettant de générer des applications logicielles. Les API définissent comment les composants logiciels doivent interagir et comment les API sont utilisées lors de la programmation de composants d'interface utilisateur graphique.

Administrateur Autorisé : tout employé du Client, sous-traitant agréé du Client, individu ou groupe responsable de la gestion de l'entretien et du fonctionnement fiable de la plateforme. Il peut être notamment responsable de la configuration, du support et de la gestion des utilisateurs et des comptes. L'administrateur peut également être un investigateur clinique responsable de la configuration d'une étude dans le système Watson Health.

Individu Autorisé : toute personne, application mobile ou unité authentifiée ayant reçu des droits d'accès permettant d'envoyer des données à Watson Health Core. Il peut s'agir du Client ou des participants à l'étude, de la clientèle ou des patients des Clients.

Lois relatives aux Données Applicables au Client : Lois relatives aux Données applicables à l'exécution des obligations du Client au titre du Contrat, des Documents Associés et des Descriptifs de Services, Bons de Commande et Descriptifs de Prestations applicables entre les Parties.

Données Client : toute entrée de données dans l'Offre IBM SaaS par ou pour le Client, qu'il s'agisse de données propres au Client ou de données entrées par ou pour le compte de tout tiers ou de la clientèle du Client, y compris toute donnée issue d'un dispositif médical de bien-être tiers.

Lois relatives aux Données : toute Loi Applicable relative à la protection, la confidentialité ou la sécurité des données.

Personne Concernée : individu identifié ou identifiable concerné par les Données à caractère personnel.

Centre de Données Désigné : le ou les centres de données désignés pour les centres de données principaux et les centres de données de reprise après incident dans le Document de Transaction, qui exécutent l'instance de l'Offre IBM SaaS du Client, le cas échéant.

Données sur la Santé : toute donnée ou information, y compris des images, correspondant aux Informations Personnelles sur la santé.

Données sur la Santé Prises en Charge : signifie, en ce qui concerne l'Offre IBM SaaS, la capacité de l'Offre IBM SaaS à se conformer aux normes, lois et réglementations applicables en matière de sécurité et de confidentialité dans les Pays Couverts pour les Données sur la Santé, y compris les spécifications de mise en œuvre stipulées dans les sous-parties A et C de la partie 164 des règlements d'application de la loi HIPAA (dans sa version modifiée par la loi HITECH Act) et d'autres Lois Applicables relatives aux Données sur la Santé, mais ne signifie pas qu'IBM intervient en qualité de Partenaire Commercial ou Sous-traitant du Traitement des Données.

HIPAA : loi Health Insurance Portability and Accountability Act de 1996, telle qu'elle est modifiée, notamment par la loi Health Information Technology for Economic & Clinical Health Act de l'American Recovery and Reinvestment Act de 2009 (« HITECH ACT »), certaines réglementations promulguées en vertu de la loi HIPAA par le Department of Health and Human Services (DHHS, ministère américain de la santé et des services sociaux) au titre du 45 C.F.R., Parties 160 et 164, et certaines réglementations promulguées conformément à la loi HITECH Act.

Lois relatives aux Données Applicables à IBM : Lois relatives aux Données applicables à l'exécution des obligations d'IBM au titre du Contrat, des Documents Associés et des Descriptifs de Services, Bons de Commande et Descriptifs de Prestations applicables entre les Parties.

Personnel IBM : (a) IBM, ses Sociétés Affiliées et ses sous-traitants, ainsi que leurs employés, et (b) tout fournisseur tiers, chacun effectuant des services pour le compte d'IBM au titre du Contrat et des Documents Associés applicables ou autorisé par IBM à accéder aux Données à caractère personnel du Client.

Pays Couverts : les 28 Etats membres de l'Union Européenne et la Suisse, ainsi que les pays qu'IBM pourra ajouter périodiquement à cette liste.

Données à caractère personnel ou **Informations Personnelles** : informations de tout support ou format, y compris les enregistrements électroniques et papier, concernant un individu identifié ou identifiable ; est réputée « identifiable » une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale.

Traitement et ses variantes, telles que **traiter** (commençant ou non par une lettre majuscule) : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Données Traitées : toutes données, informations ou éléments confidentiels ou propriétaires, y compris les Données sur la Santé ou les Données à caractère personnel, qui sont traitées par IBM conformément au Contrat, à un Document Associé et/ou à un Descriptif de Services, un Bon de Commande ou un Descriptif de Prestations.

Incident de Sécurité : a la signification qui lui est attribuée dans l'Annexe SBCA.

7. Gestion du Compte

L'Offre IBM SaaS n'est accessible qu'aux utilisateurs autorisés du Client (« **Administrateurs Autorisés** » ou « **Individus Autorisés**»). Le Client contrôlera les comptes autorisés à accéder à l'Offre IBM SaaS, notamment les applications autorisées, le personnel du Client, les sous-traitants et fournisseurs de services tiers du Client, et est seul responsable (i) du contrôle de tous les utilisateurs autorisés, y compris, sans s'y limiter, de la vérification de l'identité de tout utilisateur autorisé ; et (ii) de veiller à ce que seuls les utilisateurs autorisés accèdent à l'Offre IBM SaaS.

L'accès est accordé aux Individus Autorisés qui sont des clients, patients ou participants à l'étude du Client uniquement en vue de télécharger des données vers l'Offre IBM SaaS, auquel cas lesdits Individus Autorisés n'auront aucun autre accès à l'Offre IBM SaaS.

8. Confidentialité

8.1 Exigences Générales

Entre les Parties, le Client est le seul responsable du traitement des Données à caractère personnel du Client et désignera IBM comme sous-traitant du traitement des données. Conformément aux Lois relatives aux Données Applicables, le Client a le droit de donner des instructions à IBM en rapport avec le traitement des Données à caractère personnel du Client par IBM.

Dans la mesure où IBM traite les Données à caractère personnel du Client, IBM s'engage :

a. à se conformer à toutes les Lois relatives aux Données Applicables à IBM ; et

b. à ne pas combiner les Données à caractère personnel du Client avec des données d'autres sources, sauf :

- en cas de besoin pour fournir l'Offre IBM SaaS et à aucune autre fin, sauf si le Client demande spécifiquement à IBM de le faire ; ou
- conformément aux dispositions des présentes Conditions d'Utilisation et de l'Annexe SBCA.

Dans la mesure où IBM traite les Données à caractère personnel du Client, le Client accepte :

a. de se conformer à toutes les Lois relatives aux Données Applicables au Client ;

b. d'assumer la responsabilité de toutes les communications par le Client avec les Sociétés Affiliées, les patients, les utilisateurs finaux, les Personnes Concernées du Client et/ou tout autre tiers du Client ;

c. de conclure avec ses responsables du traitement des données des contrats de traitement de données nécessaires pour permettre à IBM, en tant que sous-traitant des données et ses sous-traitants ultérieurs du traitement des données, de traiter les Données à caractère personnel du Client ; et

d. de servir de point de contact unique pour IBM et d'être seul responsable de la coordination, de l'examen et de la soumission en interne des instructions ou demandes des Sociétés Affiliées du Client qui sont d'autres responsables du traitement de données pour IBM. IBM sera libérée de son obligation d'informer ou de notifier toute Société Affiliée du Client qui constitue un responsable du traitement des données lorsqu'elle a fourni ladite information ou notification au Client. IBM a le droit de refuser toutes instructions fournies directement par une Société Affiliée du Client qui constitue un responsable du traitement des données autre que le Client.

Aucune partie ne sera tenue d'agir en violation des Lois relatives aux Données Applicables à ladite partie.

8.2 Droits afférents aux Données Client

Le Client déclare et garantit (a) qu'il est le propriétaire des données qu'il entrera dans l'Offre IBM SaaS, ou (b) qu'il a obtenu et est responsable de maintenir tous les droits, autorisations, consentements et accords nécessaires pour octroyer à IBM les droits d'accès, d'utilisation et de communication des Données Client conformément aux dispositions des présentes Conditions d'Utilisation ou du Contrat ou pour permettre à IBM de fournir l'Offre IBM SaaS. En outre, le Client déclare et garantit que les Données Client (a) ne concerneront que les individus résidant aux Etats-Unis et ne seront entrées dans l'Offre IBM SaaS que dans le centre de données aux Etats-Unis, ou (b) ne concerneront que les individus résidant dans un ou plusieurs Pays Couverts et ne seront entrées dans l'Offre IBM SaaS que dans le ou les Centres de Données Désignés.

8.3 Services de Données et Responsabilités

a. Le Client accepte d'analyser ou de demander à IBM d'analyser les Données Client uniquement en rapport avec les activités constituant des opérations de prestation de soins de santé ou des recherches, chacun de ces termes étant défini conformément à la loi HIPAA et/ou à des dispositions similaires au titre d'autres Lois relatives aux Données Applicables, et d'utiliser les Données Client ou demander à IBM d'utiliser les Données Client uniquement en conformité avec toutes les exigences pertinentes (par exemple, détermination ou dérogation du Comité d'Evaluation Institutionnel, le cas échéant) en vertu de ces Lois relatives aux Données et de toute autre Loi relative aux Données Applicable au Client.

b. Le Client est seul responsable de l'obtention de tous les enregistrements, autorisations et accords requis par les Lois Applicables au Client dans chaque Pays Couvert applicable, y compris, sans s'y limiter, la loi HIPAA et toute autre loi, règle et réglementation applicable à la confidentialité et la sécurité des données, de sorte que les Données Client soient entrées dans l'Offre IBM SaaS et utilisées et communiquées comme prévu au titre des présentes Conditions d'Utilisation et du Contrat par le Client et par IBM et les sous-traitants autorisés d'IBM. IBM ne sera en aucun cas tenue pour responsable en matière de surveillance lorsque ces enregistrements, autorisations et accords sont reçus ou requis.

c. Le Client est seul responsable de veiller à ce que toutes les Données du Client entrées dans l'Offre IBM SaaS soient limitées aux données liées aux individus résidant aux Etats-Unis ou dans un Pays Couvert applicable.

d. IBM disposera de centres de support avec du personnel formé sur la loi HIPAA et toute autre Loi relative aux Données Applicable à IBM et aux données issues des Pays Couverts.

8.4 Mesures de Sécurité et Incidents de Sécurité

a. IBM mettra en œuvre, maintiendra et respectera les mesures techniques et organisationnelles (y compris les processus et procédures organisationnels ainsi que toutes obligations de sécurité particulières stipulées ou mentionnées dans les présentes Conditions d'Utilisation et l'Annexe SBCA) permettant de protéger les données Personnelles du Client contre tout accès ou utilisation non autorisé, perte accidentelle, dommage, modification, destruction, vol ou communication non autorisée.

b. Au cas où IBM prendrait connaissance d'un Incident de Sécurité (tel que défini par l'Annexe SBCA) impliquant les Données traitées par le Client, IBM informera le Client conformément aux dispositions de l'Annexe SBCA et des Lois relatives aux Données Applicables à IBM, et cette notification contiendra des informations sur tout impact connu sur le Client ou toute Personne Concernée (le cas échéant) affectée par ledit Incident de Sécurité, ainsi que l'action corrective effectuée ou proposée par IBM.

8.5 Réception de Demandes et de Plaintes

IBM notifiera le Client par écrit dans les meilleurs délais et, dans les limites permises par les Lois relatives aux Données Applicables à IBM, au plus tard cinq (5) jours ouvrables suivant la réception par l'IBM Watson Health Data Privacy Officer de toute demande, communication ou plainte reçue par IBM en rapport avec les Données à caractère personnel du Client de la part :

a. de toute Personne Concernée, en rapport avec les Données à caractère personnel de ladite Personne Concernée traitées par IBM. Le Client répondra auxdites demandes des Personnes Concernées et IBM se conformera aux instructions raisonnables du Client en aidant ce dernier à répondre à ces demandes. Si les Lois Applicables à IBM l'exigent, IBM pourra répondre directement auxdites demandes, à condition qu'IBM notifie au Client à l'avance une telle réponse et qu'elle collabore raisonnablement avec le Client quant à la forme et au contenu de ladite réponse, dans les limites permises par les Lois Applicables à IBM ou dans la mesure du possible ;

b. de toute autorité juridique ou réglementaire, en rapport avec le Traitement par IBM de toute Donnée Personnelle du Client, sous réserve qu'IBM pourra répondre aux demandes reçues d'un organisme gouvernemental avec une assignation ou un document juridique similaire imposant la divulgation par IBM ou au titre d'autres exigences prévues par les Lois Applicables aux Données, à condition qu'IBM notifie au Client à l'avance une telle divulgation et qu'elle collabore raisonnablement avec le Client quant à la forme et au contenu de ladite réponse, dans les limites permises par la loi ou dans la mesure du possible.

8.6 Traitement des Données à caractère personnel du Client

IBM limitera la divulgation des Données à caractère personnel du Client au Personnel IBM qui pourra être amené à l'aider à fournir les Services.

IBM se conformera à toute demande raisonnable du Client exigeant qu'IBM modifie, corrige, supprime ou bloque les Données à caractère personnel du Client conformément à la Loi Applicable.

A la demande de l'une ou l'autre des Parties, IBM, le Client ou leurs sociétés affiliées concluront des accords standard requis par la loi pour la protection des Données à caractère personnel du Client. Les Parties acceptent (et s'assureront que leurs Sociétés Affiliées respectives acceptent) que lesdits accords seront régis par la limitation et les exclusions de responsabilité du présent Contrat dans le cadre des

réclamations entre les Parties. Les Parties coopéreront pour conclure (ou s'assurer que les Sociétés Affiliées de ladite Partie concluent) et respecter tout autre accord ou disposition convenu mutuellement en vertu des Lois Applicables aux Données.

8.7 Retour des Données à caractère personnel du Client

A l'expiration ou la résiliation du Contrat, IBM s'engage et fera en sorte que l'ensemble de son personnel s'engage à cesser d'utiliser ou de traiter toute Information Propriétaire du Client et toute Donnée Personnelle du Client et, au gré et à la demande du Client :

a. retournera dans les meilleurs délais dans un format et sur un support de stockage demandés raisonnablement par le Client toutes les Informations Propriétaires du Client et les Données à caractère personnel du Client stockées par IBM par voie électronique et, une fois que le Client en accuse réception, IBM supprimera, détruira ou autrement rendra définitivement illisibles ou indéchiffrables les Informations Propriétaires du Client et les Données à caractère personnel du Client, y compris les copies et les sauvegardes. IBM pourra facturer le coût des supports de stockage et certaines activités effectuées à la demande du Client (par exemple, livraison des Informations Propriétaires du Client et des Données à caractère personnel du Client dans un format spécifique, ou destruction des Informations Propriétaires du Client et des Données à caractère personnel du Client d'une manière particulière) ; et

b. supprimera et détruira directement ou autrement rendra définitivement illisibles ou indéchiffrables les Informations Propriétaires du Client et les Données à caractère personnel du Client, y compris les copies et les sauvegardes.

8.8 Accord de Partenariat

Dans les limites appropriées et prescrites par la loi HIPAA, IBM et le Client concluront un Accord de Partenariat (« BAA »), qui régira les obligations d'IBM en tant que Partenaire du Client dans le cadre de la fourniture de l'Offre IBM SaaS. Sans limiter les obligations expresses d'IBM au titre du Contrat et de l'Accord BAA le cas échéant, le Client reconnaît et accepte qu'il est tenu de déterminer l'applicabilité et le respect de toutes les Lois Applicables et les exigences en matière de licence qui s'appliquent à l'utilisation ou d'autres activités effectuées par le Client (y compris l'utilisation ou d'autres activités effectuées par les Utilisateurs Autorisés) liées à l'Offre IBM SaaS.

8.9 Avenant relatif au Traitement des Données originaires de l'Union Européenne

Si le Client demande à IBM de traiter des Données à caractère personnel originaires de l'Union Européenne, IBM et le Client concluront un Avenant relatif au Traitement de Données y compris, selon le cas, des Clauses Contractuelles Types correspondantes adoptées par l'Union Européenne, en supprimant les clauses facultatives.

9. Dispositions supplémentaires spécifiques à l'Offre IBM SaaS

9.1 Sécurité

Cette Offre IBM SaaS se conforme aux principes de confidentialité et de sécurité de données d'IBM pour l'Offre IBM SaaS, qui sont disponibles à l'adresse http://www.ibm.com/cloud/data-security, ainsi qu'aux dispositions additionnelles stipulées ci-dessous et dans l'Annexe relative à la Sécurité et à la Continuité des Opérations jointe aux présentes Conditions d'Utilisation. Les éventuelles modifications des principes de sécurité et confidentialité de données d'IBM ne dégraderont pas la sécurité de l'Offre IBM SaaS.

IBM Watson Health Core met en œuvre des politiques, normes et processus de sécurité basés sur la norme ISO 27001, comme décrit plus en détail dans la clause Description de la Sécurité. La solution met en œuvre les fonctionnalités de sécurité suivantes :

a. Zones d'exploitation sécurisées

   IBM Watson Health Core implémente une stratégie de protection avancée, utilisant plusieurs zones de sécurité pour gérer des points d'intégration de cloud tels que l'intégration de données et le développement d'applications personnalisées.

b. Chiffrement

   Toutes les Données du Client sont chiffrées lorsqu'elles sont stockées et en transit. Toutes les données en transit à destination et en provenance d'IBM Watson Health Core sont chiffrées. Un service partagé permet la gestion de clé de chiffrement. Le Client est responsable de la connectivité et la qualité du réseau entre IBM Watson Health Service et le serveur proxy du Client.

c. Surveillance d'événements de sécurité

IBM tire parti de sa plateforme de veille sécuritaire pour les informations en matière de sécurité et la gestion d'événement, la gestion de journal, l'expertise d'incident, la détection de menace et la gestion des vulnérabilités.

d. Gestion des identités

- Watson Health Core prend en charge les fournisseurs d'identité de normes ouvertes pour les populations de patients et d'utilisateurs à grande échelle à l'aide d'OpenID Connect.
- En ce qui concerne les populations d'utilisateurs pour lesquelles IBM est le fournisseur d'identité, Watson Health Core tire parti des services d'annuaire appropriés et des fonctionnalités de gestion des identités pour traiter l'authentification.

e. Authentification forte et Accès basé sur les rôles

- Watson Health Core prend en charge l'authentification via SAML comme mécanisme permettant aux Clients d'intégrer la connexion unique (« SSO » ou « Single Sign On ») ou les services d'annuaire.
- Watson Health Core utilise une solution de gestion des accès et les composants associés pour gérer les politiques de sécurité, en cas de besoin.
- Watson Health Core prend en charge l'authentification logicielle à deux facteurs.
- Watson Health Core permet, selon les besoins, le contrôle d'accès de base en fonction des rôles ; Watson Health Core prend en charge la configuration des études, des profils d'utilisateur, des rôles et des groupes d'utilisateurs par le biais d'interfaces de programmation d'application (« API ») qui permettent l'accès basé sur les rôles.

9.2 Cookies

Le Client reconnaît et accepte qu'IBM peut, dans le cadre du fonctionnement et du support normaux de l'Offre IBM SaaS, collecter des informations personnelles auprès du Client (employés et sous-traitants du Client) liées à l'utilisation de l'Offre IBM SaaS, par le biais de processus de suivi et d'autres technologies. Cela permet à IBM de rassembler des statistiques et informations d'utilisation relatives à l'efficacité de l'Offre IBM SaaS pour améliorer l'acquis utilisateur et/ou personnaliser les interactions avec le Client. Le Client confirme qu'il obtiendra ou a obtenu l'accord permettant à IBM de traiter les informations personnelles collectées pour le but susmentionné chez IBM, d'autres sociétés d'IBM et leurs sous-traitants, quel que soit l'endroit où IBM et ses sous-traitants exercent leurs activités, conformément à la loi applicable. IBM se conformera aux demandes des employés et sous-traitants du Client pour l'accès, la mise à jour, la correction ou la suppression de leurs informations personnelles collectées.

9.3 Sites Bénéficiaires Dérivés

Le cas échéant, les taxes sont fonction du(es) site(s) que le Client identifie comme bénéficiant de l'Offre IBM SaaS. IBM appliquera les taxes en fonction de l'adresse indiquée lors de la commande d'une Offre IBM SaaS comme étant le site bénéficiaire principal, sauf si le Client fournit des informations supplémentaires à IBM. Le Client est responsable de la mise à jour de ces informations et est tenu de fournir les éventuelles informations à IBM.

9.4 Prestation en continu

Le Client a droit aux fonctionnalités et améliorations apportées à la solution et déployées par IBM dans un modèle de prestation cloud en continu.

9.5 Sauvegarde et Restauration

IBM Watson Health Core permet la sauvegarde des Données Client dans l'environnement de production (y compris les référentiels Lac de Données et Réservoir de Données) au dernier état correct connu en vue de rétablir le service dans le cas d'un incident système.

9.6 Haute disponibilité

Les composants d'IBM Watson Health Core dans l'environnement de production sont implémentés dans des configurations à haute disponibilité, avec des serveurs de base de données mis en cluster pour la redondance afin d'assurer la distribution de la charge de travail et d'éliminer les points de défaillance uniques.

9.7 Reprise après Incident

L'approche d'IBM en matière de reprise après incident consiste en plusieurs centres de données dans des zones géographiques dispersées pour atteindre ses objectifs de continuité des opérations comme suit pour son environnement de Production :

- Objectif de temps de reprise (RTO) – sous un délai de 36 heures après la déclaration du sinistre
- Objectif de point de reprise (RPO) – sous un délai maximum de 24 heures suivant la perte du contenu du Client

9.8 Outils de mesure

L'Offre IBM SaaS utilise une solution de surveillance synthétique pour surveiller, mesurer et signaler la disponibilité ou les immobilisations par rapport aux engagements de niveau de service. Cette solution simule et suit la réponse et l'expérience des utilisateurs à un niveau global, les deux visant la disponibilité et les transactions statiques.

L'Offre IBM SaaS utilise également un système de surveillance interne pour les métriques, les événements et les alertes dans l'ensemble de la solution.

9.9 Publicité

Le Client accepte qu'IBM pourra désigner publiquement le Client en tant qu'abonné à l'Offre IBM SaaS dans les communications publicitaires ou marketing.

Annexe A

1. IBM Watson Health Core

IBM Watson Health Core est une plateforme sous forme de service (PaaS) prenant en charge les données sur la santé, une plateforme de développement et un sous-système opérationnel permettant le stockage, l'organisation et le traitement des Informations Personnelles sur la Santé Protégées (PHI), comme défini par la loi HIPAA, ainsi que d'autres Données sur la Santé conformément aux Lois relatives aux Données Applicables à IBM situées dans un centre de données détenu ou contrôlé par IBM. Le Client doit se procurer des droits d'utilisation appropriés pour IBM Watson Health Core et IBM Watson Health Core Access pour activer les modules et fonctionnalités décrits ci-dessous.

1.1 Environnements d'exploitation de Watson Health Core

Les droits d'utilisation de Watson Health Core comprennent trois environnements d'exploitation cloud prenant en charge les Données sur la Santé, conçus pour permettre au Client de traiter les Données sur la Santé :

- Pilote

  Fournit un environnement sandbox dans lequel les Clients peuvent développer et tester des applications générées à l'aide de l'Offre IBM SaaS. L'environnement pilote implémente tous les dispositifs de contrôle de sécurité HIPAA, à l'exception de la reprise après incident, la haute disponibilité et la sauvegarde des systèmes d'enregistrement.

- Environnement de production

  Fournit l'environnement complet dans lequel les Clients peuvent déployer des charges de travail de Données sur la Santé. L'environnement de production est un environnement équilibré hautement disponible et peut basculer sur un site de Reprise après Incident.

- Reprise après Incident

  Fournit une réplique miroir de l'environnement de Production et se trouve dans un site de centre de données distinct.

1.2 Développement d'applications

IBM Watson Health Core permet le développement d'application et la collecte sécurisée des données à partir des appareils du Client ou des utilisateurs autorisés du Client. Les API fournissent des interfaces de programmation et des documentations que les utilisateurs autorisés du Client, y compris les fournisseurs de services tiers du Client, peuvent utiliser pour développer des applications et échanger des données avec l'Offre IBM SaaS. L'utilisation des API par le Client ou ses développeurs est soumise au respect des Exigences en matière de Développement d'API.

- API REST

  Watson Health Core fournit une série d'API REST et de services pour la plateforme Watson Health Core. Les fonctionnalités des API incluent, sans s'y limiter, des mécanismes permettant d'accéder aux référentiels de données, au service d'organisation de données, à la gestion d'utilisateurs et aux journaux d'audit.

- Apple HealthKit et Apple ResearchKit

  Watson Health Core permet l'intégration au framework d'API Apple ResearchKit pour les travaux de recherche iOS et à Apple HealthKit pour la capture des données sur le bien-être.

1.3 Gouvernance des données

- Gestion des consentements

  Watson Health Core fournit le framework permettant de capturer le consentement des patients ou des participants aux études et peut stocker en toute sécurité un dossier de consentements indépendamment du contenu des données lorsque l'individu s'inscrit par le biais d'une application Client prenant en charge les consentements.

- Masquage de données

  Watson Health Core permet de séparer les identifiants de nom du contenu des données structurées. Watson Health Core reçoit les données dans le cloud par le biais d'API de programmation. Les API permettent de séparer les identifiants de nom des patients ou des individus du reste du contenu des données, afin de les stocker dans un magasin de données chiffré distinct. Le contenu des données reçoit un jeton anonyme qui peut être utilisé dans les futurs suivis de la provenance.

1.4 Services de Données sur la Santé

Watson Health Core permet la collecte, le stockage, la synchronisation des données, notamment des Données sur la Santé exogènes et d'autres Informations Personnelles, les deux étant structurées et non structurées.

- Acquisition de Données

  Watson Health Core permet d'acquérir des données des applications ou appareils des patients par le biais d'API de programmation. Watson Health Core autorise chacun des Individus Autorisés du Client à télécharger jusqu'à 25 Mo de données dans Health Core par an pendant la durée du contrat. Le service a une capacité de 10 téléchargements maximum par Individu et par jour.

- Lac de Données Opérationnel

  Les données brutes du Client ou des patients sont stockées dans Watson Health Core dans leur format natif jusqu'à ce qu'elles soient requises pour les analyses et la modélisation.

- Extraction, Transformation et Chargement (ETC)

  Les données sont converties vers un format normalisé au sein du sous-système opérationnel. Un Bus de Services d'Entreprise aux normes du secteur d'activité pour les soins de santé permet l'intégration à différents protocoles et applications du Client.

- Réservoir de Données

  Une fois organisées, les données sont transférées vers le Réservoir de Données. Watson Health Core utilise les aspects d'IBM Unified Data Model for Healthcare pour normaliser les données commerciales et techniques sur la santé à des fins d'utilisation dans les analyses.

- Index Patient Maître

  Watson Health fournit des outils de gestion des données de référence (Master Data Management) afin de consolider les données issues de plusieurs sources pour créer un dossier LPR (Longitudinal Person Record).

2. Dispositifs en Option (Optional Features)

2.1 IBM Watson Health Core Terminology Service

Ce service complémentaire facilite l'interopérabilité et l'intégration des données entre différents systèmes de santé, afin d'harmoniser l'usage de la terminologie clinique dans toutes les applications Cloud Watson Health. Ce service fournit la plateforme fonctionnelle pour toutes les tâches impliquant les terminologies, les systèmes de code et le contenu structuré, par exemple :

- la création de nouveaux systèmes de code ;
- la traduction des systèmes de code internationaux ; et
- les mappages entre les listes de codes locaux et les normes internationales.

Annexe B

IBM fournit l'Accord relatif aux Niveaux de Service (ci-après dénommé « Accord relatif aux Niveaux de Service » ou « SLA ») de disponibilité ci-dessous pour l'Offre IBM SaaS, comme indiqué dans une Autorisation d'Utilisation (« PoE »). Le SLA ne constitue pas une garantie. Il n'est disponible que pour le Client et ne peut être utilisé que dans les environnements de production.

1. Crédits de Disponibilité

Les remises de disponibilité ne sont applicables qu'aux redevances d'abonnement relatives aux droits d'utilisation Individu.

Le Client doit consigner un ticket de support de Gravité 1 auprès du centre d'assistance technique IBM dans les 24 heures suivant la première fois où le Client a eu connaissance qu'un événement a eu une incidence sur la disponibilité de l'Offre IBM SaaS. Le Client doit raisonnablement aider IBM dans le cadre du diagnostic et de la résolution des problèmes.

Une demande de ticket de support pour non-respect d'un SLA doit être soumise dans les trois jours ouvrables suivant la fin du mois contractuel. Le dédommagement relatif à une réclamation de SLA valide sera un avoir sur une future facture de l'Offre IBM SaaS en fonction de la période de temps pendant laquelle le traitement du système de production pour l'Offre IBM SaaS n'est pas disponible (« Durée d'Indisponibilité »). La Durée d'Indisponibilité est calculée depuis le moment où le Client signale l'événement jusqu'au moment où l'Offre IBM SaaS est restaurée ; elle ne comprend pas les périodes d'indisponibilité pour les raisons suivantes : indisponibilité de maintenance programmée ou annoncée, causes échappant au contrôle d'IBM, incidents liés au contenu, à la technologie, aux conceptions ou aux instructions du Client ou d'un tiers, plateformes et configurations de système non prises en charge ou autres erreurs du Client, incident de sécurité du fait du Client ou test de sécurité mené par le Client. IBM appliquera le dédommagement correspondant le plus élevé, en fonction de la disponibilité cumulée de l'Offre IBM SaaS pendant chaque mois contractuel, comme indiqué dans le tableau ci-dessous. Le dédommagement total relatif à tout mois contractuel ne pourra pas dépasser 20 % d'un douzième (1/12ème) de la redevance annuelle de l'Offre IBM SaaS.

2. Niveaux de Service

Disponibilité de l'Offre IBM SaaS pendant un mois contractuel

Disponibilité pendant un mois contractuel	**Indemnisation (% de redevance d'abonnement Individuel mensuelle* pour le mois contractuel objet d'une réclamation)**
< 99,95 %	10 %
< 99,0 %	20 %

* Si l'Offre IBM SaaS a été acquise auprès d'un Partenaire Commercial IBM, la redevance d'abonnement mensuelle sera calculée sur le prix en vigueur à ce moment-là pour l'Offre IBM SaaS concernée pendant le mois contractuel qui fait l'objet d'une réclamation, avec une réduction de cinquante pour cent (50 %). IBM accordera une remise directement au Client.

La disponibilité, exprimée en pourcentage, est calculée comme suit : le nombre total de minutes d'un mois contractuel moins le nombre total de minutes de la Durée d'Indisponibilité au cours d'un mois contractuel, divisé par le nombre total de minutes d'un mois contractuel.

Exemple : 108 minutes de Durée d'Indisponibilité totale pendant un mois contractuel

Au total 43 200 minutes dans un mois contractuel de 30 jours - 108 minutes de Durée d'Indisponibilité = 43 092 minutes _____ Au total 43 200 minutes	= 10 % de crédit de Disponibilité pour 99,75 % de disponibilité pendant le mois contractuel

3. Exclusions

Ce SLA ne s'applique pas :

- hormis la surveillance de serveur, aux machines virtuelles hébergées pour la prise en charge des applications Client ou personnalisées ;
- si le Client a manqué à l'une de ses obligations essentielles au titre des obligations contractuelles en cours.

Annexe C

La présente Annexe relative à la Sécurité et à la Continuité des Opérations (ci-après l'Annexe « SBCA ») stipule certaines exigences et obligations d'IBM dans le cadre de la fourniture de l'Offre IBM SaaS au Client. Les exigences et obligations ci-incluses s'ajoutent à celles figurant dans la description des principes de sécurité de données pour l'Offre IBM SaaS qui sont disponibles à l'adresse http://www.ibm.com/cloud/data-security. Les termes commençant par une majuscule non définis dans le présent document auront les significations qui leur sont attribuées dans le Contrat ou dans les Conditions d'Utilisation.

1. Programme de Sécurité des Informations

IBM dispose de politiques, normes et processus de sécurité internes basées sur la norme ISO 27001 et les zones de contrôle. Outre la gouvernance d'IBM Corporate Security Organization, ces politiques, normes et processus font régulièrement l'objet d'audits internes.

IBM gère un programme de sécurité des informations pour les mesures de protection organisationnelles, opérationnelles, administratives, physiques et techniques régissant le traitement, le stockage et la transmission du contenu du Client qui, au minimum, sont en conformité avec les exigences de la présente Annexe SBCA.

IBM partagera avec le Client, à la demande de ce dernier, des informations relatives au programme de sécurité des informations d'IBM Watson Health de sorte que le Client puisse raisonnablement déterminer leur pertinence, adéquation et efficacité en continu. Le programme de sécurité des informations d'IBM Watson Health sera mis à jour périodiquement de manière à rester en phase avec les pratiques généralement admises dans le secteur d'activité et avec les Lois Applicables à IBM.

2. Contrôles d'Accès

IBM ne communiquera le contenu du Client qu'à ses employés, sous-traitants ou tiers qui ont un besoin professionnel légitime d'accéder audit contenu du Client afin d'aider IBM à remplir ses obligations vis-à-vis du Client ou d'autres personnes dans la mesure nécessaire pour fournir l'Offre IBM SaaS conformément aux Lois Applicables, au Contrat ou à un Document Associé, selon le cas applicable. Dans le cas où IBM est un Partenaire Commercial du Client, IBM et le Client ne communiqueront les Informations Personnelles sur la Santé que conformément à un Accord de Partenariat applicable entre les Parties.

IBM dispose d'un processus formel et interne de gestion des accès utilisateur où l'accès utilisateur est formellement demandé, approuvé après vérification de l'identité et accordé en fonction du besoin d'en connaître, à l'aide du principe du moindre privilège. L'accès au contenu du Client sera limité uniquement aux utilisateurs actifs et aux comptes d'utilisateur actifs. IBM dispose d'un processus formel permettant la revalidation d'accès interne périodique des comptes d'utilisateur actifs.

IBM utilise des protocoles d'authentification d'utilisateur sécurisés, y compris l'attribution d'identifiants uniques et de mots de passe fiables pour les comptes d'utilisateur actifs sur les systèmes utilisés pour fournir des services au Client conformément aux normes et politiques de sécurité d'IBM :

a. Les mots de passe ne doivent pas être des mots de passe par défaut fournis par le constructeur et seront conservés dans un emplacement et/ou format ne compromettant pas la sécurité des données qu'ils protègent.

b. L'affichage et l'impression des mots de passe doivent être masqués, supprimés ou rendus illisibles de sorte que les parties non autorisées ne puissent pas les voir ou les récupérer ultérieurement. Les mots de passe ne doivent pas être journalisés ou capturés lors de leur saisie. Les mots de passe utilisateur ne doivent pas être stockés en texte clair.

c. Les mots de passe relatifs à chaque technologie constituant l'Offre IBM SaaS sont choisis pour atténuer les risques associés aux vulnérabilités connues en matière de longueur de mot de passe et doivent être documentés.

d. Lorsque l'utilisation d'identifiants fonctionnels internes, privilégiés et partagés est requise pour des raisons opérationnelles, IBM gère des identifiants partagés, fonctionnels et/ou Système nécessitant la vérification des mots de passe pour maintenir la responsabilisation individuelle.

Des délais d'inactivité sont établis pour tous les systèmes et applications stockant le contenu du Client.

Si nécessaire, l'accès à distance au réseau, aux systèmes et aux applications d'IBM stockant le contenu du Client sera établi à la demande du Client et sous réserve de l'accord formel d'IBM, et toutes ces connexions à distance seront sécurisées à l'aide de protocoles d'authentification et de chiffrement puissants. Les activités d'accès à distance seront journalisées et surveillées.

Dans la mesure où la livraison de l'Offre IBM SaaS nécessite l'accès à distance d'IBM à tout système situé dans les réseaux internes du Client, cet accès à distance sera réalisé uniquement à l'aide des systèmes et protocoles d'accès à distance sécurisés du Client et des droits d'accès fournis à IBM par le Client. L'accès à distance au réseau du Client sera établi uniquement à la demande d'IBM et sous réserve de l'approbation du Client, conformément aux politiques en vigueur du Client qui seront fournies à IBM à l'avance. L'utilisation des réseaux internes du Client par IBM sera soumise aux règles d'utilisation et de sécurité informatiques du Client qui seront fournies à IBM à l'avance.

IBM met en œuvre la répartition des tâches pour l'administration de la sécurité, la vérification des accès et les enquêtes sur les violations de sécurité.

Le stockage, l'hébergement et le traitement du contenu du Client spécifiques au Client sont logiquement distincts de ceux des autres clients pris en charge par IBM. Dans les cas où une zone de travail de stockage, d'hébergement ou de traitement partagée est autorisée par le Client, IBM mettra en place des procédures et des mesures de protection conformes aux exigences stipulées dans la présente Annexe SBCA afin d'empêcher la communication non autorisée dudit contenu du Client.

IBM applique des politiques de rangement de bureau/écran vide pour s'assurer que le contenu du Client n'est jamais laissé sans surveillance dans un lieu public.

3. Transfert et Chiffrement

IBM prendra les précautions appropriées lors de la transmission du contenu du Client (par télécopie, e-mail, coursier, etc.) pour s'assurer que les coordonnées utilisées pour le destinataire sont correctes et lors des contacts préalables avec le destinataire prévu pour sécuriser la réception desdites informations.

IBM utilise et fera en sorte que son Personnel utilise des formes de chiffrement appropriées ou toute autre technologie liée au traitement du contenu du Client, notamment en rapport avec tout transfert, communication, accès à distance ou stockage (y compris le stockage des sauvegardes) du contenu du Client. Par exemple, IBM chiffrera, à l'aide d'une méthode de chiffrement standard appropriée, tous les enregistrements et fichiers contenant le contenu du Client :

a. qui sont stockés sur des ordinateurs portables, périphériques portables ou supports électroniques portables d'IBM, y compris les bandes de sauvegarde lors du transfert vers une unité de stockage hors site ;

b. qui sont stockés ou transportés par IBM hors des bureaux et installations physiquement sécurisés du Client ou d'IBM, à l'exclusion des documents papier ;

c. lors de leur transfert sur des réseaux publics par IBM ;

d. lors de leur transfert des systèmes d'IBM vers le Client ;

e. lors de leur transmission sans fil par IBM ; et

f. qui sont stockés par IBM sur des serveurs et bases de données.

4. Sécurité réseau

IBM utilise des versions raisonnablement à jour des logiciels de sécurité système tels que les firewalls, les proxys, les interfaces et les firewalls d'application Web. Ces logiciels doivent inclure la protection contre les programmes malveillants ainsi que des correctifs et des définitions de virus raisonnablement à jour. Conformément aux normes de l'entreprise, les logiciels antivirus seront installés sur des postes de travail, des serveurs et des points d'extrémité associés lorsque cela est techniquement faisable et les logiciels sont gérés en fonction des politiques de l'entreprise à l'aide de solutions de gestion internes.

IBM surveille l'Offre IBM SaaS pour détecter et identifier les incidents de sécurité le plus tôt possible. IBM mettra en place au minimum des outils de détection d'intrusion standard et des processus de prévention, de surveillance et d'intervention permettant d'identifier les vulnérabilités et risques internes et externes pouvant donner lieu à la communication, l'utilisation incorrecte, la modification ou la destruction non autorisées du contenu du Client ou des systèmes d'information qui sont utilisés pour fournir des services au Client.

IBM souscrit des services d'informations sur les vulnérabilités ou des alertes de sécurité informatique et toute autre source pertinente fournissant des informations à jour sur les vulnérabilités des systèmes. IBM évalue et corrige régulièrement les vulnérabilités de son réseau.

IBM surveille l'Offre IBM SaaS pour détecter, identifier, contenir et résoudre les Incidents de Sécurité.

IBM valide la disponibilité, l'intégrité et l'efficacité de l'infrastructure de sécurité réseau sur laquelle l'Offre IBM SaaS est mise à disposition, par le biais de ses processus de gestion des éditions.

5. Gestion et Notifications d'Incident

Les équipes IBM Watson Health collaborent avec l'équipe d'intervention en matière d'incident de cybersécurité d'IBM, une équipe mondiale qui gère la réception, l'investigation et la coordination interne des incidents de sécurité liés aux offres IBM et qui prend des mesures préventives nécessaires pour réduire les problèmes de sécurité logiciels. Un « Incident de Sécurité » est l'accès aux, l'utilisation, la communication, la modification ou le brouillage non autorisés des opérations ou données système dans un système d'information utilisé par IBM pour fournir l'Offre IBM SaaS. Si un Incident de Sécurité est détecté (par le biais des scannages de routine, des alertes, des événements de seuil, etc.), IBM informera le Client :

a. de tout Incident de Sécurité confirmé impliquant le contenu du Client, dès que possible et, en tout état de cause, au plus tard dans les 2 jours ouvrables suivant l'investigation et la confirmation dudit Incident de Sécurité ;

b. immédiatement après toute demande d'accès ou d'information sur le contenu du Client de la part de tout représentant du gouvernement (y compris toute agence de protection de données ou autorité de réglementation), à moins d'une interdiction en vertu d'une législation ou d'une décision de justice pertinente ; et

c. sauf dans les cas permis dans la clause intitulée Contrôles d'Accès de la présente Annexe SBCA, avant toute communication ou tout transfert du contenu du Client à ou par un tiers ou avant tout accès au contenu du Client par un tiers.

6. Journalisation

IBM gère, conformément à ses politiques et pratiques et aux pratiques généralement admises dans le secteur d'activité, la surveillance raisonnable des systèmes pour toute utilisation non autorisée des Données Traitées par le Client ou tout accès non autorisé à celles-ci. Les violations de connexion et d'accès réelles ou visées seront journalisées.

IBM gère des dossiers de toutes les demandes d'accès et des journaux des activités d'accès pour tous les systèmes qui stockent, accèdent aux, traitent et transmettent du contenu Client et des Données sur la Santé aussi longtemps que cela s'avère nécessaire en vertu de la loi HIPAA et de toute autre Loi relative aux Données Applicable à IBM.

Les journaux et rapports incluent au minimum : (i) toutes les tentatives d'accès, qu'elles aboutissent ou non, y compris des informations d'identification raisonnables ; (ii) toutes les modifications de configuration système et réseau, y compris les installations d'application, les modifications de la gestion d'utilisateur et les modifications des droits d'accès aux fichiers ; (iii) les tentatives d'accès aux ressources, qu'elles aboutissent ou non, y compris les tentatives d'accès à tout fichier, partage de réseau, journal ou autre ressource ; et (iv) les téléchargements de données, y compris le type de contenu des données et le protocole d'accès utilisé pour réaliser le téléchargement.

7. Développement d'Applications Logicielles et Gestion des Modifications

IBM suit les pratiques de codification et de développement d'application sécurisées qui protègent l'intégrité des applications de production et du code source associé contre les modifications non autorisées et non testées.

IBM suit un processus de gestion des modifications qui comprend (a) l'enregistrement et l'approbation formelle des modifications, ainsi que des procédures d'annulation ; et (b) le test approprié desdites modifications, notamment les tests d'acceptation utilisateur, le cas échéant, ainsi que les tests de sécurité.

IBM suit un processus de gestion de correctif qui comprend le test des correctifs avant l'installation sur tous les systèmes utilisés pour stocker, accéder au et transmettre le contenu du Client ou utilisés pour fournir des services, y compris l'Offre IBM SaaS, au Client.

IBM demande aux administrateurs système de maintenir des informations complètes, exactes et à jour concernant la configuration de tous les systèmes d'information utilisés pour stocker, accéder au et transmettre le contenu du Client.

8. Sécurité Physique et Environnementale

La plateforme IBM Watson Health Core est déployée sur l'infrastructure de données IBM SoftLayer. IBM SoftLayer gère des contrôles et processus de sécurité physique et environnementale et de contrôle d'accès pour protéger les données du Client de toute violation ou tout impact humain, environnemental et technique.

L'accès général aux installations hébergeant l'Offre IBM SaaS est contrôlé via l'utilisation d'un système d'accès par carte. Des caméras de télévision en circuit fermé (CCTV) sont installées dans les sites et surveillées par le personnel de sécurité. Les portes d'accès sélectionnées sont équipées d'un système d'alarme qui est surveillé par le personnel de sécurité.

L'accès aux zones contrôlées est restreint via l'utilisation d'un système d'accès par carte et/ou d'une vérification biométrique supplémentaire. Toutes les personnes ne disposant pas d'accès autorisé aux zones contrôlées doivent s'identifier et être accompagnées d'une personne disposant d'un accès approuvé aux zones contrôlées. Les issues de secours de toutes les zones contrôlées possèdent des alarmes audibles qui sont surveillées par le personnel de sécurité. Une vérification période du fonctionnement des alarmes est effectuée, documentée et conservée. Les droits d'accès aux zones contrôlées sont entièrement revalidées trimestriellement. L'accès aux zones contrôlées est révoqué à la cessation d'emploi.

Les installations sont protégées contre des facteurs d'environnement tels que le feu, l'eau et la chaleur via des alarmes d'incendie, des extincteurs d'incendie, des détecteurs de fumée et des systèmes de suppression et d'extinction d'incendie. Les installations sont protégées contre les coupures et pannes de courant par le biais de systèmes d'alimentation de secours (UPS) et de groupes électrogènes qui sont entretenus et testés régulièrement.

Les informations et rapports de conformité IBM SoftLayer sont disponibles à l'adresse http://www.softlayer.com/compliance.

9. Continuité des Opérations Internes

IBM dispose de plans de continuité des opérations et de reprise après incident qui sont conçus pour maintenir un niveau de service conforme aux obligations nées du présent Contrat. Ces plans de continuité des opérations et de reprise après incident seront périodiquement mis à jour et testés (au moins une fois par an). IBM appliquera aux plans de continuité des opérations et de reprise après incident toutes les modifications raisonnables nécessaires pour rester en conformité avec les pratiques généralement admises dans le secteur d'activité, sans toutefois perturber de façon déraisonnable l'Offre IBM SaaS ou l'environnement de production utilisé par le Client.

Dans le cas d'un incident qui rend l'Offre IBM SaaS indisponible pour le Client, IBM en informera rapidement le Client et activera le plan de continuité des opérations et/ou de reprise après incident. Lorsqu'un incident est déclaré, l'objectif des opérations IBM SaaS consiste à restaurer l'accès du Client à l'Offre IBM SaaS comme suit : dans le cas d'une indisponibilité, l'Objectif de Temps de Reprise (RTO) pour la restauration de l'environnement de production IBM Watson Health est un délai de 36 heures suivant la déclaration de l'incident. L'Objectif de Point de Reprise (RPO) est un délai maximum de 24 heures suivant la perte du contenu du Client dans l'environnement de protection. Les objectifs de continuité des opérations des solutions Watson Health spécifiques peuvent varier.

L'approche d'IBM en matière de reprise après incident consiste en plusieurs centres de données dans des zones géographiques dispersées.

Tous les centres de données IBM SoftLayer gèrent plusieurs sources d'alimentation, liaisons par fibre optique, générateurs dédiés et batteries de secours. Ils s'appuient sur du matériel et des équipements de pointe, afin de fournir le maximum de performances, de fiabilité et d'interopérabilité. Tous les composants de centre de données, comprenant par exemple des ressources de refroidissement et d'alimentation n+1 redondantes, sont inspectés pour maintenir la stabilité dans les centres de données.

10. Conformité

Les pratiques d'IBM en matière de sécurité sont basées sur la norme ISO 27001-27002. Ces pratiques fournissent les structures de contrôle des éléments suivants (sans s'y limiter) : analyse des risques,

sécurité physique, planification d'urgence, investigations, protection des informations, formation, protection de données et opérations.

IBM examine les activités liées à la sécurité et la confidentialité quant à leur conformité aux pratiques d'IBM en matière de sécurité.

IBM respecte les Lois relatives aux Données Applicables à IBM dans les Pays Couverts.

Le traitement approprié des informations confidentielles des Clients est également requis au titre des Principes de conduite dans les affaires d'IBM que tous les employés doivent lire (et certifier avoir lu) tous les ans.

11. Divers

IBM veillera à ce que ses contrats avec tous les sous-traitants et/ou tiers engagés dans la livraison de l'Offre IBM SaaS comportent des dispositions au moins aussi protectrices du contenu du Client que celles de la présente Annexe SBCA et de tout Document Associé applicable, dans la mesure où ces dispositions sont applicables aux services à effectuer par lesdites sous-traitants et/ou tiers.