Conditions d'utilisation IBM – Modalités relatives aux offres de Logiciel-service

IBM Watson Health Core

Les Conditions d'utilisation se composent du présent document intitulé «Conditions d'utilisation IBM – Modalités relatives aux offres de Logiciel-service» (les «Modalités des offres de Logiciel-service») et d'un document intitulé «Conditions d'utilisation IBM – Modalités générales» (les «Modalités générales»), qui est disponible à l'adresse http ://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Advenant une incompatibilité entre les Modalités générales et les présentes Modalités des offres de Logiciel-service, ces dernières prévaudront. Le Client accepte les présentes Conditions d'utilisation en commandant le Logiciel-service IBM, en y accédant ou en l'utilisant.

Ces Conditions d'utilisation sont régies par le Contrat Passport Advantage international IBM, le Contrat Passport Advantage Express international IBM ou le Contrat international régissant les offres désignées relatives aux Logiciels-services IBM (aussi appelés Logiciels sous forme de services), selon le cas (le «Contrat»), et celui-ci, de pair avec les Conditions d'utilisation, constitue l'entente intégrale.

1. Logiciel-service IBM

Les offres de Logiciel-service IBM suivantes sont régies par les présentes Modalités des offres de Logiciel-service :

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

2. Paramètres de calcul des frais

Le Logiciel-service IBM est vendu en fonction d'un des paramètres de calcul des frais suivants, comme spécifié dans le Document transactionnel :

a. Un **Accès** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Un Accès correspond à un droit d'utiliser le Logiciel-service IBM. Le Client doit obtenir une seule autorisation d'Accès pour utiliser le Logiciel-service IBM au cours de la période de mesure indiquée dans son Autorisation d'utilisation ou dans son Document transactionnel.

b. Une **Entité** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Une Entité correspond à une seule chose ou à un être humain. Il faut obtenir un nombre suffisant d'autorisations pour couvrir chaque Entité traitée ou gérée par le Logiciel-service IBM pendant la période de mesure indiquée dans l'Autorisation d'utilisation ou le Document transactionnel du Client.

   Aux fins du présent Logiciel-service IBM, une Entité peut correspondre à une personne, à un appareil ou à une application mobile dont les données sont gérées par le Logiciel-service IBM.

c. Une **Instance** est une unité de mesure servant de base pour obtenir le Logiciel-service IBM. Une Instance correspond à un accès à une configuration spécifique du Logiciel-service IBM. Il faut obtenir un nombre suffisant d'autorisations pour couvrir chaque Instance du Logiciel-service IBM mise en disponibilité aux fins d'accès et d'utilisation pendant la période de mesure indiquée dans l'Autorisation d'utilisation ou le Document transactionnel du Client.

3. Frais et facturation

Le montant exigible pour le Logiciel-service IBM est indiqué dans un Document transactionnel.

3.1 Frais mensuels partiels

Des frais mensuels partiels spécifiés dans le Document transactionnel et calculés au prorata peuvent être exigés.

3.2 Frais d'utilisation excédentaire

Si l'utilisation réelle que fait le Client du Logiciel-service IBM au cours de la période de mesure excède l'utilisation autorisée spécifiée dans l'Autorisation d'utilisation, le Client devra payer des frais d'utilisation excédentaire, au tarif indiqué dans le Document transactionnel.

4. Période d'abonnement et options de renouvellement

La période d'abonnement au Logiciel-service IBM commence à la date à laquelle IBM avise le Client qu'il a accès à l'environnement d'exploitation pilote du Logiciel-service IBM, comme indiqué dans le Document de commande. La période d'abonnement pour les Entités commence lorsque IBM avise le Client qu'il a accès à l'environnement d'exploitation en production. Le Document de commande spécifiera si l'abonnement au Logiciel-service IBM se renouvelle automatiquement, s'il se poursuit sur une base continue ou s'il se termine à la fin de la période d'abonnement.

Dans le cas d'un renouvellement automatique, l'abonnement au Logiciel-service IBM se renouvellera automatiquement pour la période indiquée dans l'Autorisation d'utilisation, à moins que le Client n'avise IBM par écrit, au moins quatre-vingt-dix (90) jours à l'avance, de son intention de ne pas renouveler son abonnement.

S'il s'agit d'une utilisation continue, le Logiciel-service IBM continuera d'être disponible chaque mois, jusqu'à ce que le Client transmette à IBM un préavis écrit de quatre-vingt-dix (90) jours pour l'informer qu'il désire mettre fin à son abonnement. Le Logiciel-service IBM demeurera disponible jusqu'à la fin du mois civil suivant cette période de quatre-vingt-dix (90) jours.

5. Assistance technique

IBM mettra en disponibilité le guide d'assistance pour les Logiciels-services IBM («IBM Software as a Service Support Handbook») qui indique les coordonnées pour obtenir de l'assistance technique, les périodes de maintenance, ainsi que d'autres renseignements et processus concernant l'assistance technique. Les coordonnées pour l'assistance technique et d'autres détails sur cette assistance sont fournis dans le guide d'assistance pour les Logiciels-services IBM, à l'adresse https ://support.ibmcloud.com.

L'assistance technique et le traitement des demandes de configuration simples pour le Logiciel-service IBM sont offerts par voie électronique. L'assistance technique est incluse avec le Logiciel-service IBM et n'est pas offerte dans le cadre d'une offre distincte.

Aucun Renseignement personnel, Renseignement confidentiel sur la santé ou Renseignement personnel sensible ne doit être inclus dans la documentation ou l'information transmise au moment de signaler un problème.

6. Définitions

Lois applicables – Lois, règlements ou législation, règles, directives, mandats, décrets ou autres exigences émis par une autorité gouvernementale, ou normes de l'industrie généralement reconnues qui s'appliquent aux présentes Conditions d'utilisation.

API – Interface de programmation d'applications composée d'un ensemble de sous-programmes, de protocoles et d'outils servant à créer des applications logicielles. L'API indique comment les composants logiciels doivent interagir, et s'utilise pour programmer des composants d'interface utilisateur graphique.

Administrateur autorisé – Employé ou entrepreneur autorisé du Client, personne ou groupe responsable de gérer la maintenance et la fiabilité du fonctionnement de la plateforme. Les responsabilités peuvent inclure la configuration, l'assistance et la gestion des utilisateurs et des comptes. L'administrateur peut aussi jouer le rôle d'un investigateur clinicien chargé de préparer une étude dans le système de santé Watson.

Entité autorisée – Personne, application mobile ou appareil qui a été authentifié(e) et qui a obtenu le droit de transmettre des données au Logiciel-service IBM Watson Health Core. Il peut s'agir du Client ou de participants à une étude, de clients ou de patients de Clients.

Lois sur la protection des données applicables au Client – Lois sur la protection des données qui s'appliquent à l'acquittement des obligations du Client aux termes du Contrat, de Documents associés, de Descriptions de services, de Documents de commande et des Descriptions du travail applicables conclus entre les Parties.

Données du Client – Données introduites dans le Logiciel-service IBM par le Client ou en son nom, qu'il s'agisse de données du Client ou de données introduites par un client du Client ou un tiers ou en leur nom, y compris les données issues d'un appareil d'un tiers pour le contrôle de la santé.

Lois sur la protection des données – Lois applicables qui régissent la protection des données, des renseignements personnels ou la sécurité des données.

Personne concernée – Personne identifiée ou pouvant être identifiée pour laquelle des Renseignements personnels sont diffusés.

Centre informatique désigné – Centre informatique désigné comme principal centre informatique et pour la reprise après sinistre dans le Document transactionnel où s'exécute l'instance du Logiciel-service IBM du Client, s'il y a lieu.

Données de santé – Données ou information, y compris des images, qui sont des Renseignements personnels liés à la santé.

Homologué pour les données de santé – Capacité du Logiciel-service IBM de respecter les normes, les lois et les règlements qui régissent la sécurité et la protection des Renseignements personnels dans les Territoires visés pour les Données de santé, notamment les spécifications de mise en œuvre établies dans les sous-sections A et C de la section 164 des règlements de mise en œuvre de la loi américaine HIPAA (telle que modifiée par la loi américaine HITECH) et d'autres Lois applicables qui régissent les Données de santé. Ce terme ne signifie toutefois pas qu'IBM agit en tant que collaborateur («Business Associate») ou vérificateur de données («Data Controller»).

HIPAA – Acronyme désignant la Loi américaine Health Insurance Portability and Accountability Act, de 1996, telle que modifiée par la loi Health Information Technology for Economic & Clinical Health Act qui a été promulguée sous la loi American Recovery and Reinvestment Act de 2009 («loi HITECH»), certains règlements promulgués en vertu de la loi HIPAA par le département de la Santé et des Services sociaux des États-Unis dans les sections 160 et 164 du Code of Federal Regulations 45, ainsi que certains règlements promulgués conformément à la loi HITECH.

Lois sur la protection des données applicables à IBM – Lois sur la protection des données qui s'appliquent à l'acquittement des obligations d'IBM aux termes du Contrat, des Documents associés, des Description de services, des Documents de commande et des Descriptions du travail applicables conclus entre les Parties.

Personnel IBM – (a) IBM, ses sociétés affiliées et sous-traitants et leurs employés respectifs; et (b) tout tiers fournisseur qui, dans tous les cas fournissent des services au nom d'IBM, conformément au Contrat et aux Documents associés applicables, ou à qui IBM permet autrement d'accéder aux Renseignements personnels du Client.

Pays visés – Les 28 États membres de l'Union européenne, la Suisse et les autres pays qu'IBM peut éventuellement ajouter à cette liste.

Renseignements personnels ou **Information personnelle** – Information sur un support ou dans un format quelconque, électronique ou imprimé, qui porte sur une personne identifiée ou identifiable, une «personne identifiable» étant une personne pouvant être identifiée, que ce soit directement ou indirectement, tout particulièrement par un numéro d'identification ou par un ou plusieurs facteurs spécifiques concernant son identité physique, physiologique, mentale, économique, culturelle ou sociale.

Processus et ses variantes, comme **traitement** (comportant une majuscule initiale ou non) – Opération ou ensemble d'opérations qui sont exécutées sur les données, de manière automatique ou non, comme la collecte, l'enregistrement, l'organisation, l'entreposage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la divulgation par transmission, la diffusion ou la mise en disponibilité autrement, l'alignement ou la combinaison, le blocage, l'effacement ou la destruction.

Données traitées – Données, information ou document confidentiels ou exclusifs, dont des Données de santé et des Renseignements personnels, qui sont traités par IBM conformément au Contrat, à un Document associé, à une Description de services, à un Document de commande ou à une Description du travail.

Incident de sécurité – Incident tel que défini dans l'Appendice C (Sécurité et continuité des opérations) du présent document.

7. Gestion des comptes

Le Logiciel-service est accessible seulement aux utilisateurs autorisés du Client («**Administrateurs autorisés**» ou «**Entités autorisées**»). Le Client gérera les comptes qui sont autorisés à accéder au Logiciel-service IBM, ce qui peut inclure des applications, du personnel du Client, des tiers fournisseurs de services et des entrepreneurs du Client qui sont autorisés. Le Client assume seul la responsabilité de : (i) contrôler tous les utilisateurs autorisés, notamment de vérifier leur identité; et (ii) s'assurer que seuls les utilisateurs autorisés ont accès au Logiciel-service IBM

Les Entités autorisées qui sont des clients, des patients ou des participants à une étude du Client peuvent obtenir un accès uniquement aux fins de téléversement de données dans le Logiciel-service IBM, auquel cas ces Entités autorisées n'auront pas accès au Logiciel-service à toute autre fin.

8. Protection des renseignements personnels

8.1 Exigences générales

Le Client est le seul vérificateur de tous ses Renseignements personnels, et désigne IBM comme responsable du traitement des données. Conformément aux Lois sur la protection des données, le Client a le droit de fournir des instructions à IBM en lien avec le traitement que fait IBM des Renseignements personnels du Client.

Lorsqu'elle traite les Renseignements personnels du Client, IBM :

a. doit respecter toutes les Lois sur la protection des données applicables à IBM; et

b. ne doit pas combiner les Renseignements personnels du Client avec d'autres sources de données, sauf :

- dans la mesure nécessaire pour fournir le Logiciel-service IBM et seulement à cette fin, à moins d'y être expressément enjoint par le Client; ou
- conformément aux modalités des présentes Conditions d'utilisation et de l'Appendice C (Sécurité et continuité des opérations) du présent document.

Lorsque IBM traite des Renseignements personnels du Client, ce denier doit :

a. respecter toutes les Lois sur la protection des données applicables au Client;

b. assumer la responsabilité de toutes les communications du Client avec ses Sociétés affiliées, les patients, les utilisateurs finals, les Personnes concernées et les autres tiers fournisseurs du Client;

c. conclure des ententes de traitement de données requises avec ses vérificateurs pour permettre à IBM, en tant que responsable du traitement des données et aux sous-traitants responsables du traitement des données de traiter les Renseignements personnels du Client; et

d. jouer le rôle d'agent de liaison auprès d'IBM, et assumer seul la coordination, la révision interne et la soumission d'instructions ou de demandes que formulent à IBM des Sociétés affiliées du Client qui agissent comme d'autres vérificateurs. IBM sera libérée de son obligation d'informer ou d'aviser une Société affiliée du Client qui agit à titre de vérificateur lorsqu'elle a informé ou avisé le Client. IBM est autorisée à refuser les instructions fournies directement par une Société affiliée du Client qui agit à titre de vérificateur.

Aucune des parties ne doit être obligée d'agir en violation des Lois sur la protection des données auxquelles elle est assujettie.

8.2 Droits relatifs aux Données du Client

Le Client déclare et garantit qu'il : (a) est propriétaire des données qu'il introduira dans le Logiciel-service IBM; ou (b) qu'il a obtenu et qu'il a la responsabilité d'obtenir l'ensemble des droits, des autorisations et des consentements qui sont nécessaires pour donner le droit à IBM d'accéder aux Données du Client, de les utiliser et de les divulguer conformément aux modalités des présentes Conditions d'utilisation, du Contrat ou comme il est nécessaire pour lui permettre de fournir le Logiciel-service IBM. Le Client déclare et garantit également que les Données du Client seront seulement : (a) liées à des personnes qui résident aux États-Unis et qu'elles seront alors uniquement introduites dans le Logiciel-service IBM dans le centre informatique qui se trouve aux États-Unis; ou (b) liées à des personnes qui résident dans un ou plusieurs des Pays visés, auquel cas elles seront alors introduites dans le Logiciel-service IBM à partir du ou des Centres informatiques désignés.

8.3 Services et responsabilités concernant les données

a. Le Client convient qu'il analysera ou demandera à IBM d'analyser les Données du Client uniquement en lien avec les activités de soins de santé («health care operations») ou de recherche («research») du Client, tels que ces termes sont définis dans la loi HIPAA ou des termes semblables en vertu d'autres Lois sur la protection des données applicables, et qu'il utilisera les Données du Client ou demandera à IBM d'utiliser ces mêmes données en respectant toutes les exigences pertinentes (p. ex., l'aval d'un comité d'éthique indépendant ou une renonciation, si nécessaire) en vertu de ces lois ou d'autres Lois sur la protection des données applicables au Client.

b. Le Client assume seul la responsabilité d'obtenir les inscriptions, les consentements et les autorisations qu'exigent les Lois sur la protection des données applicables au Client dans chaque Pays visé, notamment la loi HIPAA et les autres lois et règlements sur la protection des renseignements personnels et la sécurité des données applicables, afin de permettre l'introduction des Données du Client dans le Logiciel-service IBM et leur utilisation et leur divulgation conformément aux modalités des présentes Conditions d'utilisation et du Contrat par le Client, IBM et les sous-traitants autorisés d'IBM. IBM n'a pas la responsabilité de vérifier à quel moment ces inscriptions, consentements ou autorisations sont reçus ou nécessaires.

c. Il incombe au Client de s'assurer que toutes les Données du Client qui sont introduites dans le Logiciel-service IBM concernent uniquement des personnes qui résident aux États-Unis ou dans un Pays visé.

d. IBM doit disposer, dans ses centres d'assistance, de membres du personnel qui ont été formés au sujet de la loi HIPAA et des autres Lois sur la protection des données applicables à IBM en ce qui concerne les données issues des Pays visés.

8.4 Incidents et mesures de sécurité

a. IBM doit mettre en œuvre, maintenir et respecter les mesures techniques et organisationnelles, dont les processus et procédures organisationnels, ainsi que les obligations spécifiques en matière de sécurité établies dans les présentes Conditions d'utilisation et dans l'Appendice C (Sécurité et continuité des opérations) du présent document ou qui y sont évoquées pour protéger les Renseignements personnels du Client contre un usage ou un accès non autorisé, une perte accidentelle, des dommages, la modification, la destruction, le vol ou la divulgation non autorisée.

b. Si IBM apprend qu'un Incident de sécurité (tel que défini dans l'Appendice C du présent document) touchant les Données traitées du Client est survenu, elle doit en informer le Client, conformément aux modalités dudit Appendice C et des Lois sur la protection des données applicables à IBM. L'avis fourni au Client devra inclure de l'information concernant tout impact connu de cet incident de sécurité sur le Client ou les Personnes concernées (s'il y a lieu), ainsi que les mesures correctives qui ont été prises ou qu'IBM propose de prendre.

8.5 Réception des demandes d'information et des plaintes

IBM doit aviser par écrit promptement le Client et, dans la mesure permise par les Lois sur la protection des données applicables à IBM, au plus tard cinq (5) jours ouvrables après que le responsable de la protection des Renseignements personnels du groupe Santé Watson IBM ait reçu une demande d'information, une communication ou une plainte reçue par IBM concernant les Renseignements personnels du Client :

a. d'une Personne concernée au sujet de ses Renseignements personnels traités par IBM. Le Client doit répondre à une telle demande des Personnes concernées, et IBM suivra les instructions raisonnables du Client pour aider ce dernier à répondre à de telles demandes. Si les Lois sur la protection des données applicables à IBM l'exigent, IBM pourra répondre directement à de telles demandes, dans la mesure où IBM avise le Client à l'avance d'une telle réponse et se coordonne raisonnablement avec le Client pour définir la forme et le contenu de cette réponse, lorsque les Lois sur la protection des données applicables à IBM le permettent ou que cette coordination est autrement possible;

b. d'une autorité juridique ou réglementaire concernant le Traitement par IBM des Renseignements personnels du Client, pourvu qu'IBM puisse répondre à de telles demandes reçues d'un organisme gouvernemental accompagnées d'une assignation à témoigner ou d'un document juridique semblable forçant la divulgation par IBM, ou requis autrement par les Lois sur la protection des données, dans la mesure où IBM avise le Client à l'avance d'une telle divulgation et se coordonne raisonnablement avec le Client pour définir la forme et le contenu d'une telle réponse, lorsque la loi le permet ou que cela est autrement possible.

8.6 Traitement des Renseignements personnels du Client

IBM doit limiter le droit de divulgation des Renseignements personnels du Client seulement au Personnel IBM qui doit l'aider à fournir les Services.

IBM acquiescera à toute demande raisonnable du Client visant à modifier, à corriger, à supprimer des Renseignements personnels du Client ou à en bloquer l'accès, conformément aux Lois applicables.

À la demande de l'une ou l'autre des Parties, IBM, le Client ou leurs Sociétés affiliées concluront les contrats standards requis par la loi pour la protection des Renseignements personnels du Client. Les Parties conviennent – et veilleront à ce que leurs Sociétés affiliées respectives acceptent – que de tels contrats supplémentaires seront assujettis à la limitation et aux exclusions de responsabilité définies dans le présent Contrat en ce qui concerne les réclamations faites entre les Parties. Les Parties coopéreront pour établir et respecter mutuellement les modalités ou les ententes que peuvent exiger les Lois sur la protection des données applicables ou veilleront à ce que leurs Sociétés affiliées respectives fassent de même.

8.7 Remise des Renseignements personnels du Client

Dès l'expiration ou la résiliation du Contrat, IBM doit cesser d'utiliser ou de traiter l'Information exclusive du Client et les Renseignements personnels du Client, veiller à ce que le Personnel IBM fasse de même et, à la demande éventuelle du Client :

a. retourner promptement, dans un format et sur un support de stockage que le Client peut raisonnablement demandé, toute l'Information exclusive et les Renseignements personnels du Client qu'IBM a entreposés par voie électronique et, après avoir reçu un avis de confirmation du Client, supprimer, détruire ou rendre autrement illisibles ou indéchiffrables de manière permanente l'Information exclusive et les Renseignements personnels du Client, y compris les copies et les sauvegardes. IBM peut facturer des frais pour couvrir le coût du support de stockage et de certaines activités exécutées à la demande du Client (comme la livraison de l'Information exclusive ou des Renseignements personnels du Client dans un format spécifique ou la destruction de ces mêmes éléments d'une façon particulière); et

b. supprimer ou détruire directement ou rendre autrement illisibles ou indéchiffrables l'Information exclusive et les Renseignements personnels du Client, y compris les copies et les sauvegardes.

8.8 Contrat de collaborateur

Dans la mesure appropriée et requise par la loi HIPAA, IBM et le Client concluront un Contrat de collaborateur («Business Associate Agreement»), qui régira les obligations d'IBM en tant que collaborateur du Client pour fournir le Logiciel-service IBM. Sans limiter les obligations expresses d'IBM aux termes du Contrat et du Contrat de collaborateur (s'il y a lieu), le Client reconnaît et convient qu'il a la responsabilité de déterminer l'applicabilité de l'ensemble des Lois applicables et des exigences de licence qui s'appliquent à l'utilisation et aux autres activités que le Client et ses Utilisateurs autorisés font du Logiciel-service IBM, et d'assurer le respect de ces lois et exigences.

8.9 Addenda relatif au traitement des données dans l'Union européenne

Si le Client demande à IBM de traiter des Renseignements personnels provenant de l'Union européenne, IBM et le Client concluront un Addenda relatif au traitement des données qui inclura, s'il y a lieu, des clauses modèles de l'Union européenne, mais qui exclura les clauses facultatives.

9. Modalités supplémentaires relatives aux offres de Logiciel-service IBM

9.1 Sécurité

Ce Logiciel-service IBM respecte les principes relatifs à la sécurité des données et à la protection des renseignements personnels pour les Logiciels-services IBM, qui sont énoncés à l'adresse http ://www.ibm.com/cloud/data-security, ainsi que les modalités supplémentaires stipulées ci-dessous et dans l'Appendice C (Sécurité et continuité des opérations) du présent document. Tout changement apporté aux principes d'IBM en matière de sécurité des données et de protection des renseignements personnels n'aura pas pour effet de dégrader la sécurité du Logiciel-service IBM.

Le Logiciel-service IBM Watson Health Core met en œuvre les politiques, les normes et les processus de sécurité qui sont basés sur le cadre de travail ISO 27001, tel que défini plus en détail dans la description de la sécurité. Parmi ses capacités en matière de sécurité, la solution met en œuvre ce qui suit :

a. Zones d'exploitation sécurisées

   Le Logiciel-service IBM Watson Health Core met en place une stratégie de défense en profondeur en utilisant de multiples zones de sécurité pour gérer les points d'intégration infonuagiques, comme l'introduction des données et le développement d'applications personnalisées.

b. Chiffrement

Toutes les Données du Client sont chiffrées au repos et en mouvement. Toutes les données en transit vers le Logiciel-service ou qui sont transmises par ce dernier sont chiffrées. Un service partagé gère les clés. Le Client est responsable de toute la connectivité et de la qualité du réseau entre le service de santé IBM Watson et le serveur mandataire du Client.

c. Surveillance des événements de sécurité

IBM tire parti de sa plateforme d'information sur la sécurité pour gérer l'information et les événements sur la sécurité, les journaux, la criminalistique pour les incidents, la détection des menaces et la gestion des vulnérabilités.

d. Gestion de l'identité

- Le Logiciel-service Watson Health Core est compatible avec les solutions des fournisseurs d'identité selon les normes ouvertes pour identifier les patients et les populations d'utilisateurs à large échelle, puisqu'il utilise OpenID Connect.
- Dans le cas des populations d'utilisateurs pour lesquelles IBM est le fournisseur d'identités, le Logiciel-service IBM Watson Health Core se sert des services d'annuaire et des fonctions de gestion d'identités appropriés pour gérer l'authentification.

e. Authentification forte et accès basé sur les rôles

- Le Logiciel-service Watson Health Core permet l'authentification par langage SAML comme mécanisme pour permettre aux Clients d'intégrer leurs services d'authentification unique ou leurs services d'annuaire.
- Ce Logiciel-service se sert d'une solution de gestion de l'accès et de composants associés pour gérer les politiques de sécurité au besoin.
- Le Logiciel-service IBM Watson Health Core permet d'utiliser l'authentification logicielle à deux facteurs.
- Ce Logiciel-service offre un contrôle d'accès de base en fonction des rôles, au besoin. Il donne la possibilité de se servir d'interfaces de programmation d'applications (API) qui permettent de contrôler l'accès en fonction des rôles par la définition d'une étude, de profils d'utilisateurs, de rôles et de groupes d'utilisateurs.

9.2 Témoins

Le Client sait et convient qu'IBM peut, dans le cadre de ses activités normales d'exploitation et de soutien du Logiciel-service, recueillir des renseignements personnels du Client (de ses employés et entrepreneurs) en lien avec l'utilisation du Logiciel-service IBM, en utilisant des technologies de surveillance ou d'autres technologies. IBM recueille de telles données afin d'obtenir des statistiques d'utilisation et de l'information sur l'efficacité de son Logiciel-service, en vue d'améliorer l'expérience des utilisateurs ou de personnaliser les interactions avec le Client. Ce dernier confirme qu'il obtiendra ou qu'il a obtenu le consentement pour permettre à IBM de traiter les renseignements personnels recueillis, aux fins énoncées plus haut, au sein d'IBM, dans d'autres entreprises d'IBM et dans l'entreprise de leurs sous-traitants, partout où ils font affaire, et conformément à ce que permettent les lois applicables. IBM acquiescera aux demandes des employés et des entrepreneurs du Client concernant leur accès aux renseignements personnels qui ont été recueillis sur eux, ainsi qu'à leurs demandes de mise à jour, de correction ou de suppression de ces mêmes renseignements.

9.3 Emplacements bénéficiaires

Les taxes applicables, s'il y a lieu, sont basées sur le ou les emplacements que le Client identifie comme étant ceux qui bénéficient du Logiciel-service IBM. Ainsi, IBM appliquera les taxes en se basant sur l'adresse professionnelle que le Client désigne comme l'emplacement qui est le principal bénéficiaire au moment de commander le Logiciel-service IBM, à moins que le Client ne fournisse à IBM de l'information supplémentaire à ce sujet. Le Client a la responsabilité de maintenir cette information à jour et d'informer IBM de tout changement.

9.4 Livraison en mode continu

Le Client a le droit de bénéficier des nouvelles capacités et des améliorations qui sont apportées à la solution et déployées par IBM selon un modèle de livraison infonuagique en continu.

9.5 Sauvegarde et restauration

Le Logiciel-service IBM Watson Health Core sauvegarde les Données du Client dans l'environnement de production (y compris les référentiels sous forme de Lac de données et de Réservoir de données) dans leur meilleur état le plus récent pour le service de restauration en cas d'une défaillance du système.

9.6 Haute disponibilité

Des composants du Logiciel-service IBM Watson Health Core dans l'environnement de production sont mis en œuvre dans des configurations à haute disponibilité, en utilisant des serveurs de bases de données en grappe pour obtenir une redondance, répartir la charge de travail et éliminer les points de défaillance uniques.

9.7 Reprise après sinistre

L'approche d'IBM en matière de reprise après sinistre consiste à utiliser de multiples centres informatiques dispersés dans différentes régions géographiques, afin d'atteindre ses objectifs de continuité des opérations indiqués ci-dessous pour son environnement de Production :

- Objectif de temps de reprise : Dans les 36 heures qui suivent la déclaration d'un sinistre
- Objectif de point de reprise – Perte de contenu du Client pendant un maximum de 24 heures

9.8 Outils de mesure

Le Logiciel-service IBM utilise une solution de surveillance synthétique pour surveiller, mesurer et signaler la disponibilité ou les pannes en regard de niveaux de service promis. Cette solution simule et fait le suivi des réponses et de l'expérience des utilisateurs à l'échelle mondiale, à la fois pour la disponibilité statique et les transactions.

Le Logiciel-service IBM se sert aussi d'un système de surveillance interne pour les mesures, les événements et les alertes dans toute la solution.

9.9 Publicité

Le Client convient qu'IBM peut rendre public le fait que le Client est abonné au Logiciel-service IBM, dans une publicité ou une communication pour la mise en marché.

Appendice A

1. IBM Watson Health Core

Le Logiciel-service Watson Health Core est une plateforme-service homologuée pour les données de santé, une plateforme de développement et un sous-système opérationnel servant à enregistrer, à organiser et à traiter des Renseignements confidentiels sur la santé, tel que défini dans la loi HIPAA, ainsi que d'autres Données de santé, conformément aux Lois sur la protection des données applicables à IBM. Cette plateforme se trouve dans un centre informatique qui appartient à IBM ou qui est géré par IBM. Le Client doit obtenir les autorisations d'utilisation appropriées pour IBM Watson Health Core et l'offre IBM Watson Health Core Access afin d'activer les fonctions et les capacités qui sont décrites ci-dessous.

1.1 Environnements d'exploitation de Watson Health Core

L'autorisation d'utilisation du Logiciel-service IBM Watson Health Core couvre trois environnements d'exploitation infonuagiques homologués pour les données de santé, en vue de permettre au Client de traiter des Données de santé :

- Environnement pilote

  Il s'agit d'un environnement bac à sable dans lequel le Client peut créer et tester des applications en se servant du Logiciel-service IBM. L'environnement pilote met en œuvre tous les contrôles de sécurité spécifiés par la loi HIPAA, sauf pour la reprise après sinistre, la haute disponibilité et la sauvegarde des systèmes d'enregistrement.

- Environnement de production

  Il s'agit de l'environnement exhaustif dans lequel le Client peut déployer des charges de travail comportant des Données de santé. L'environnement de Production est un environnement à haute disponibilité dans lequel les charges de travail sont équilibrées et qui a la capacité de basculer vers un emplacement de reprise après sinistre.

- Reprise après sinistre

  Cet environnement offre une réplique miroir de l'environnement de Production, et se situe dans un centre informatique distinct.

1.2 Développement d'applications

Le Logiciel-service IBM Watson Health Core permet de développer des applications et de recueillir des données de manière sécurisée à partir d'appareils du Client ou de ses Utilisateurs autorisés. Des API fournissent des interfaces de programmes et de la documentation dont les Utilisateurs autorisés et les tiers fournisseurs du Client peuvent se servir pour créer des applications et échanger des données avec le Logiciel-service IBM. L'utilisation des API par le Client ou ses développeurs doit toutefois respecter les exigences des développeurs des API.

- API REST

  Le Logiciel-service Watson Health Core fournit une série d'interfaces API REST et de services pour sa plateforme. Ces API comprennent entre autres des mécanismes pour accéder aux référentiels, au service d'organisation des données, des fonctions de gestion des utilisateurs et des journaux d'audit.

- Outils HealthKit etResearchKit d'Apple

  Le Logiciel-service Watson Health Core permet l'intégration à l'API ResearchKit d'Apple pour les études de recherche basées sur la plateforme iOS et à l'outil HealthKit d'Apple pour enregistrer des données sur le contrôle de la santé.

1.3 Gouvernance pour les données

- Gestion des consentements

  Le Logiciel-service Watson Health Core fournit le cadre de travail pour enregistrer les consentements fournis par les patients ou les participants à une étude. Il peut aussi entreposer un enregistrement de ces consentements de manière sécurisée à part des données utiles lorsque la personne pertinente s'inscrit à l'aide d'une application du Client qui traite les consentements.

- Masquage des données

  Le Logiciel-service Watson Health Core donne la possibilité de séparer les données utiles structurées des identificateurs de nom. Le Logiciel-service reçoit les données dans un nuage par l'intermédiaire d'interfaces de programmation d'applications. Ces interfaces permettent de séparer les identificateurs de nom des patients ou des personnes du reste des données utiles et de les entreposer dans un magasin de données distinct qui est chiffré. Les données utiles sont associées à un jeton anonymisé qui peut ensuite servir à faire le suivi de leur provenance.

1.4 Services de données de santé

Watson Health Core offre des fonctions de collecte, d'entreposage et de synchronisation de données, y compris des Données de santé et d'autres Renseignements personnels exogènes, à la fois structurés et non structurés.

- Ingestion de données

  Le Logiciel-service IBM Watson Health Core offre la possibilité d'ingérer des données issues d'applications pour les patients ou d'appareils des patients par l'intermédiaire d'API. Le Logiciel-service permet à chaque Entité autorisée du Client d'y téléverser jusqu'à vingt-cinq mégaoctets (25 Mo) de données pour chaque année de la période contractuelle. Le service peut traiter jusqu'à dix (10) téléversements par Entité quotidiennement.

- Lac de données opérationnelles

  Les données brutes du Client ou des patients sont entreposées dans le Logiciel-service IBM Watson Health Core en format natif, jusqu'à ce que ces données soient nécessaires aux fins analytiques et de modélisation.

- Technologie ETL (Extract Transform Load)

  Les données sont transformées dans un format normalisé à l'intérieur du sous-système opérationnel. Un bus de service d'entreprise standard dans l'industrie pour les soins de santé permet et facilite l'intégration entre différentes applications et divers protocoles du Client.

- Réservoir de données

  Une fois les données organisées. elles sont déplacées dans le Réservoir de données. Le Logiciel-service IBM Watson Health Core utilise certains aspects du modèle de données unifiées d'IBM pour les soins de santé afin de normaliser les données de gestion et techniques sur la santé à des fins analytiques.

- Index principal des personnes

  La solution de santé Watson fournit des outils de gestion des données de base pour regrouper les données issues de multiples sources afin de créer un dossier personnel longitudinal.

2. Options

2.1 Offre IBM Watson Health Core Terminology Service

Ce service complémentaire facilite l'intégration des données et l'interopérabilité entre des systèmes de santé disparates, en fournissant une terminologie clinique cohérente dans toutes les applications du Nuage Santé Watson IBM. Ce service offre la plateforme fonctionnelle permettant d'exécuter toutes les tâches qui comportent de la terminologie, des systèmes de codage et du contenu structuré, telles que :

- la création de nouveaux systèmes de codage;
- la traduction de systèmes de codage internationaux; et
- l'établissement d'une correspondance entre des listes de codes locaux et des normes internationales.

Appendice B

L'Entente de niveau de service sur la disponibilité qui suit s'applique au Logiciel-service IBM comme spécifié dans le Document transactionnel du Client. Cette entente ne constitue pas une garantie. Elle est offerte uniquement au Client et s'applique seulement aux environnements de production.

1. Crédits pour la disponibilité

Les remises pour la disponibilité s'appliquent uniquement aux frais d'abonnement pour les Entités.

Le Client doit ouvrir un dossier d'assistance de Gravité 1 au centre d'assistance technique IBM. Ce dossier doit être ouvert dans les vingt-quatre (24) heures après qu'il a pris connaissance pour la première fois qu'un événement a eu une incidence sur la disponibilité du Logiciel-service IBM. Le Client doit fournir une assistance raisonnable à IBM pour diagnostiquer tout problème et trouver une solution.

Le Client doit soumettre sa Réclamation pour le non-respect de l'Entente de niveau de service dans les trois (3) jours ouvrables qui suivent la fin du Mois de la période contractuelle pertinent. La compensation offerte pour une réclamation valide aux termes de cette Entente de niveau de service se fera sous la forme d'un crédit qui s'appliquera à une facture ultérieure pour le Logiciel-service IBM. Ce crédit sera établi en fonction de la durée pendant laquelle le traitement du système de production pour le Logiciel-service IBM n'a pas été disponible («Temps d'arrêt»). Le Temps d'arrêt se mesure à partir du moment où le Client signale l'événement, jusqu'à ce que le Logiciel-service IBM soit restauré. Cette période n'inclut pas le temps d'interruption associé à une maintenance périodique ou annoncée, à des causes sur lesquelles IBM n'a aucun pouvoir, à des problèmes avec le contenu, la technologie, les conceptions ou les instructions du Client ou d'un tiers, aux configurations de système et aux plateformes qui ne sont pas prises en charge ou aux autres erreurs du Client, à un incident de sécurité causé par le Client ou à des tests de sécurité effectués par le Client. IBM accordera la compensation la plus élevée qui s'applique en se fondant sur la disponibilité cumulée du Logiciel-service IBM au cours de chaque Mois de la période contractuelle, comme indiqué dans le tableau ci-après. La compensation totale au cours d'un mois quelconque de la période contractuelle ne peut excéder vingt pour cent (20 %) du un douzième (1/12^{e}) des frais annuels pour le Logiciel-service IBM.

2. Niveaux de service

Disponibilité du Logiciel-service IBM au cours d'un Mois de la période contractuelle

Disponibilité au cours d'un Mois de la période contractuelle	**Compensation (Pourcentage des frais d'abonnement mensuels* d'une Entité pour un Mois de la période contractuelle visé par une Réclamation)**
< 99,95 %	10 %
< 99 %	20 %

* Si le Client an acheté le Logiciel-service IBM auprès d'un partenaire commercial IBM, les frais d'abonnement mensuels seront alors calculés d'après le prix courant pour le Logiciel-service IBM en vigueur au cours du Mois de la période contractuelle faisant l'objet d'une Réclamation, auquel s'appliquera un escompte de cinquante pour cent (50 %). IBM accordera directement la remise au Client.

Le taux de disponibilité est calculé comme suit : (a) le nombre total de minutes dans un Mois de la période contractuelle, moins (b) le nombre total de minutes de Temps d'arrêt dans ce même mois, divisé par (c) le nombre total de minutes dans ce même mois. La fraction obtenue est ensuite exprimée sous la forme d'un pourcentage.

Exemple : Temps d'arrêt total de cent huit (108) minutes au cours d'un Mois de la période contractuelle

43 200 (nombre total de minutes dans un Mois de la période contractuelle comptant 30 jours) - 108 minutes de Temps d'arrêt = 43 092 minutes _____ 43 200 minutes au total	= Crédit pour la disponibilité de 10 % pour un taux de disponibilité de 99,75 % au cours du Mois de la période contractuelle

3. Exclusions

Cette même Entente de niveau de service ne s'applique pas dans les cas suivants :

- À part la surveillance des serveurs, l'Entente de niveau de service ne s'applique pas aux machines virtuelles hébergées servant à prendre en charge des applications personnalisées ou du Client.
- L'entente de niveau de service ne s'applique pas si le Client n'a pas respecté des obligations essentielles aux termes du présent Contrat.

Appendice C

Cet Appendice sur la sécurité et la continuité des opérations définit certaines exigences et obligations d'IBM concernant l'accès au Logiciel-service qu'IBM accorde au Client. Les exigences et les obligations définies dans ce document s'ajoutent à celles qui sont spécifiées dans la description des principes de sécurité et de protection des données pour les Logiciels-services IBM qui est disponible à l'adresse http ://www.ibm.com/cloud/data-security. Les termes comportant une majuscule initiale qui ne sont pas définis dans le présent document ont la signification qui leur a été attribuée dans le Contrat ou dans les Conditions d'utilisation.

1. Programme de sécurité de l'information

IBM a des politiques, des normes et des processus de sécurité internes qui sont basés sur le cadre de travail ISO 27001, de même que des zones de contrôle. En plus de la gouvernance du service de sécurité interne d'IBM Corporation, ces politiques, ces normes et ces processus font régulièrement l'objet d'audits internes.

IBM maintient un programme de sécurité de l'information comportant des mesures de protection organisationnelles, opérationnelles, administratives, physiques et techniques qui régissent le traitement, l'entreposage et la transmission du contenu du Client et qui répondent au moins aux exigences du présent Appendice C.

À la demande du Client, IBM doit partager avec le Client de l'information sur le programme de sécurité de l'information en santé IBM Watson, afin de pouvoir raisonnablement déterminer sa pertinence, son adéquation et son efficacité au fil du temps. Le programme de sécurité de l'information en santé IBM Watson doit être mis à jour de temps à autres, afin de demeurer à jour par rapport aux pratiques généralement reconnues dans l'industrie et de demeure conforme aux Lois de protection des données applicables à IBM.

2. Contrôles d'accès

IBM doit divulguer le contenu du Client uniquement à ses employés, à ses sous-traitants ou aux tiers qui ont un besoin professionnel légitime d'accéder à un tel contenu afin d'aider IBM à s'acquitter de ses obligations envers le Client, ou à d'autres personnes nécessaires pour fournir le Logiciel-service IBM, conformément aux Lois applicables, au Contrat ou un Document associé (selon le cas). Si IBM joue le rôle d'un collaborateur du Client, IBM et le Client doivent divulguer les Renseignements médicaux personnels seulement conformément aux modalités d'un contrat de collaboration conclu entre les Parties.

IBM utilise un processus interne officiel de gestion d'accès selon lequel l'accès d'un utilisateur est officiellement demandé, approuvé après vérification de l'identité et accordé en fonction du besoin de savoir, selon le principe de droit d’accès minimal. L'accès au contenu du Client doit être limité uniquement aux utilisateurs et aux comptes d'utilisateurs qui sont actifs. IBM utilise un processus officiel pour revalider périodiquement à l'interne l'accès des comptes d'utilisateurs actifs.

IBM utilise des protocoles d'authentification des utilisateurs sécurisés et attribue des identifications uniques et des mots de passe fiables pour les comptes d'utilisateurs dans les systèmes qui servent à fournir des services au Client, conformément aux normes et aux politiques de sécurité d'IBM :

a. Les mots de passe ne peuvent pas être des mots de passe par défaut fournis par des fournisseurs et doivent être conservés dans un endroit ou un format qui ne compromet pas la sécurité des données qu'ils protègent.

b. L'affichage et l'impression des mots de passe doivent être masqués, supprimés ou obscurcis de manière à ce que les personnes non autorisées ne soient pas capables de les observer ou de les récupérer par la suite. Les mots de passe ne doivent pas être consignés ou enregistrés lorsqu'ils sont saisis. Les mots de passe des utilisateurs ne doivent pas être entreposés sous la forme d'un texte en clair.

c. Les mots de passe pour chaque technologie incluse dans le Logiciel-service IBM sont choisis pour atténuer les risques associés aux vulnérabilités liées à la longueur connue des mots de passe et doivent être documentés.

d. Lorsqu'il faut utiliser des codes d'identification (ID) fonctionnels internes, privilégiés et partagés pour des raisons opérationnelles, IBM gère les ID partagés, fonctionnels ou de système en exigeant la vérification des mots de passe pour assurer la responsabilité individuelle.

Des Délais d'inactivité sont établis pour tous les systèmes et toutes les applications qui contiennent du contenu du Client.

Au besoin, un accès à distance au réseau, aux systèmes et aux applications d'IBM qui entreposent du contenu du Client sera établi à la demande du Client et après une approbation officielle d'IBM, et toutes les connections à distance devront être sécurisées à l'aide de protocoles d'authentification forte et de chiffrement fort. Les accès à distance doivent être consignés et surveillés.

Si la livraison du Logiciel-service exige qu'IBM accède à distance à un système qui se trouve dans les réseaux internes du Client, un tel accès à distance se fera uniquement en utilisant les systèmes et les protocoles d'accès à distance du Client, ainsi que les justificatifs d'identité que le Client fournit à IBM. L'accès à distance au réseau du Client doit se faire seulement à la demande d'IBM, après l'approbation du Client, et conformément aux politiques du Client alors en vigueur que le Client transmettra à IBM à l'avance. L'utilisation par IBM des réseaux internes du Client se fera conformément aux politiques d'utilisation et de sécurité du service TI du Client, qui seront transmises à IBM à l'avance.

IBM applique la séparation des tâches pour l'administration de la sécurité, l'examen des accès et les enquêtes sur les bris de sécurité.

L'entreposage, l'hébergement et le traitement du contenu du Client sont logiquement séparés des mêmes services rendus pour d'autres clients d'IBM. Dans les cas où le Client autorise un partage de l'espace de travail servant à l'entreposage, à l'hébergement ou au traitement, IBM doit mettre en place des procédures et des mesures de protection compatibles avec les exigences du présent Appendice C qui sont conçues pour prévenir la divulgation non autorisée du contenu du Client.

IBM applique des politiques de rangement des documents et d'écran vide pour assurer que le contenu du Client n'est en aucun temps laissé sans surveillance dans un endroit public.

3. Transfert et chiffrement

IBM doit prendre des précautions appropriées pour transmettre du contenu du Client (par télécopieur, par courriel, par courrier, etc.) afin de s'assurer d'utiliser les bonnes coordonnées pour le destinataire, et conclure des arrangements préalables avec le destinataire visé afin de sécuriser la réception de cette information.

IBM utilisera en tout temps et veillera à ce que son personnel utilise les formes de chiffrement appropriées ou d'autres technologies sécurisées pour le traitement du contenu du Client, notamment pour le transfert et la communication de ce contenu et son accès ou son entreposage à distance (y compris l'entreposage des copies de sauvegarde). Par exemple, IBM doit chiffrer à l'aide d'un chiffrement approprié selon les normes de l'industrie tous les enregistrements et les fichiers contenant du contenu du Client :

a. qui sont entreposés dans un ordinateur portable, dans des appareils mobiles ou sur des supports électroniques portables, dont des bandes de sauvegarde qui sont en transit vers un emplacement d'entreposage hors site;

b. entreposés ou transportés par IBM hors de bureaux ou d'installations physiquement sécurisés du Client ou d'IBM, exclusion faite des documents imprimés;

c. qu'IBM fait transiter sur des réseaux publics;

d. qui sont transférés au Client à partir des systèmes d'IBM;

e. qu'IBM transmet en mode sans fil; et

f. qu'IBM entrepose dans des serveurs et des bases de données.

4. Sécurité des réseaux

IBM utilise des versions raisonnablement à jour de logiciels de sécurité pour les systèmes, comme des pare-feu, des serveurs mandataires, des pare-feu et des interfaces d'applications Web. Ces logiciels doivent inclure une protection contre les logiciels malveillants, ainsi que des correctifs et des définitions de virus raisonnablement à jour. Conformément aux normes de l'entreprise, les logiciels antivirus doivent être installés dans les postes de travail, les serveurs et les points d'extrémité associés, lorsque cela est techniquement faisable, et les logiciels sont gérés selon les politiques de l'entreprise à l'aide de solutions de gestion internes.

IBM surveille le Logiciel-service IBM en vue de détecter et d'identifier des incidents de sécurité aussitôt que possible. IBM doit tout au moins maintenir en place des outils de détection d'intrusions ainsi que des processus de prévention, de surveillance et d'intervention conformes aux normes de l'industrie de

manière à identifier à la fois les vulnérabilités et les risques internes et externes pouvant causer une divulgation non autorisée, une utilisation inappropriée, l'altération ou la destruction du contenu du Client ou des systèmes d'information qui sont utilisés pour fournir des services au Client.

IBM souscrit aux services d'information sur les vulnérabilités ou aux services-conseils sur la sécurité de l'information et à d'autres sources pertinentes fournissant de l'information à jour sur les vulnérabilités des systèmes. IBM effectue régulièrement des vérifications et des corrections des vulnérabilités dans son réseau.

IBM surveille le Logiciel-service IBM pour détecter, identifier, contenir et résoudre les Incidents de sécurité.

IBM valide la disponibilité, l'intégrité et l'efficacité de l'infrastructure de sécurité du réseau sur laquelle le Logiciel-service IBM est mis en disponibilité, en suivant les processus de gestion des versions d'IBM.

5. Gestion et signalement des incidents

Les équipes chargées des solutions de santé IBM Watson travaillent de pair avec l'équipe IBM d'intervention pour incidents de cybersécurité, qui gère à l'échelle mondiale la réception, l'investigation et la coordination internes des incidents de sécurité liés aux offres IBM, afin de mettre en œuvre les mesures préventives nécessaires pour réduire les problèmes de sécurité liés aux logiciels. Un «Incident de sécurité» correspond à une tentative réussie d'accès, d'utilisation, de modification ou d'interférence non autorisés concernant des opérations d'un système ou des données dans un système d'information dont IBM se sert pour fournir le Logiciel-service IBM. Si une Incident de sécurité est découvert (à l'aide d'une analyse régulière, d'alertes, d'événements de seuil, etc.), IBM doit informer et aviser le Client :

a. de tout Incident de sécurité touchant le contenu du Client, dès que possible et jamais plus de deux (2) jours ouvrables après l'investigation et la confirmation d'un tel Incident de sécurité;

b. promptement après avoir reçu une demande d'accéder au contenu du Client ou un demande d'information concernant ce contenu de la part d'un administrateur gouvernemental (y compris un organisme chargé de la protection des données ou de l'application de la loi), à moins que la loi ou une ordonnance pertinente ne l'interdise; et

c. à l'avance de toute divulgation ou de tout transfert du contenu du Client à un tiers ou par un tiers ou de l'accès à ce contenu par un tiers, sauf comme autorisé dans la section intitulée Contrôles d'accès du présent Appendice C.

6. Journalisation

Conformément à ses politiques et aux pratiques de l'industrie généralement reconnues, IBM effectue une surveillance raisonnable des systèmes pour contrer l'utilisation non autorisée des Données traitées du Client ou l'accès non autorisé à ces mêmes données. Les ouvertures de session et les accès non autorisés réels ou les tentatives d'ouverture de session ou d'accès non autorisés seront consignées dans des journaux.

IBM maintient des registres de toutes les demandes d'accès et des journaux des accès pour tous les systèmes qui entreposent, traitent et transmettent des Données de santé du Client ou y accèdent, dans la mesure requise par la loi HIPAA et les autres Lois de protection des données applicables à IBM.

Les journaux et les rapports doivent inclure au minimum : (i) toutes les tentatives d'ouverture de session, réussies ou non, ainsi que des renseignements d'identification raisonnables; (ii) tous les changements apportés aux systèmes et aux réseaux, y compris l'installation d'applications, les changements concernant la gestion des utilisateurs et les modifications des droits d'accès aux fichiers; (iii) les tentatives d'accès aux ressources, réussies ou non, y compris les tentatives d'accès à un fichier, à un journal à une autre ressource ou de partager un réseau; et (iv) les téléchargements de données, dont le type de données visées et le protocole d'accès utilisé pour effectuer le téléchargement.

7. Développement d'applications logicielles et gestion des changements

IBM applique des pratiques de développement d'applications et de programmation sécurisées qui protègent l'intégrité des applications de production et le code source associé contre des modifications non autorisées et non testées.

IBM suit un processus de gestion des changements qui inclut : (a) la consignation et l'approbation officielle des changements et des procédures de retour à l'état initial; et (b) le test approprié des changements, y compris un test d'acceptation par l'utilisateur, s'il y a lieu, ainsi qu'un test de sécurité.

IBM suit un processus de gestion des correctifs qui comprend le test des correctifs avant de les installer dans tous les systèmes utilisés pour entreposer et transmettre du contenu du Client ou y accéder ou qui servent à fournir des services au Client, y compris le Logiciel-service IBM.

IBM exige que les administrateurs de systèmes conservent de l'information complète, exacte et à jour concernant la configuration de tous les systèmes d'information qui servent à entreposer et à transmettre le contenu du Client ou à accéder à ce contenu.

8. Sécurité physique et environnementale

La plateforme IBM Watson Health Core est déployée sur l'infrastructure de données SoftLayer IBM. Cette infrastructure est assortie de mesures de sécurité physique et environnementale, de contrôles d'accès et d'autres contrôles et processus visant à protéger les données du Client contre une brèche ou une incidence humaine, environnementale ou technique.

L'accès général aux installations dans lesquelles le Logiciel-service IBM est hébergé est contrôlé à l'aide d'un système d'accès par carte. Des caméras de télévision en circuit fermé sont installées dans l'ensemble des sites et sont surveillées par du personnel de sécurité. Certaines portes comportent un système d'alarme et le personnel de sécurité surveille ces alarmes.

L'accès aux zones contrôlées est géré par l'utilisation d'une carte d'accès ou des mécanismes de vérification biométriques supplémentaires. Toutes les personnes qui n'ont pas d'autorisation d'accès aux zones contrôlées doivent signer un registre et sont escortées par une personne qui est autorisée à accéder à ces zones. Toutes les sorties d'urgence dans les zones contrôlées sont pourvues d'une alarme sonore qui est surveillée par du personnel de sécurité. Le fonctionnement de ces alarmes est vérifié périodiquement, et cette vérification est documentée et conservée. Les droits d'accès pour les zones contrôlées sont tous revalidés chaque trimestre. L'accès aux zones contrôlées est révoqué dès la cessation d'emploi.

Les installations sont protégées contre les facteurs environnementaux, comme le feu, l'eau et la chaleur par l'intermédiaire d'alarmes d'incendie, d'extincteurs d'incendie, de détecteurs de fumée et de systèmes d'extinction d'incendie. Les installations sont protégées contre les interruptions ou les pannes de courant par l'entremise de systèmes d'alimentation sans coupure et de génératrices de secours, qui font l'objet d'une maintenance et de tests réguliers.

De l'information et des rapports sur la conformité de SoftLayer IBM sont disponibles à l'adresse http ://www.softlayer.com/compliance.

9. Continuité des opérations de l'entreprise

IBM dispose de plans pour la continuité des opérations et de plans antisinistres qui sont conçus pour maintenir un niveau de service adéquat en regard de ces obligations aux termes du Contrat. Ces plans sont mis à jour et testés périodiquement (au moins une fois par année). IBM doit apporter tous les changements raisonnables à ses plans de continuité des opérations et ses plans antisinistres qui sont nécessaires pour se conformer aux pratiques généralement reconnues dans l'industrie, en veillant dans tous les cas à ne pas interférer de manière déraisonnable avec le Logiciel-service IBM ou l'environnement de production qu'utilise le Client.

Si un sinistre a pour effet de rendre le Logiciel-service IBM non disponible pour le Client, IBM doit en aviser promptement le Client et exécuter son plan pour la continuité des opérations ou son plan antisinistre. Lors de la déclaration d'un sinistre, l'objectif du plan pour la continuité des opérations concernant le Logiciel-service IBM consiste à restaurer l'accès du Client au Logiciel-service comme suit : en cas de panne, l'Objectif de temps de reprise est de restaurer l'environnement de production du système de Santé Watson IBM dans les trente-six (36) heures qui suivent la déclaration du sinistre. L'Objectif de point de reprise correspond à une perte de contenu du Client pendant un maximum de vingt-quatre (24) heures dans l'environnement de production. Les objectifs de continuité des opérations peuvent varier selon les solutions de santé Watson.

L'approche d'IBM en matière de reprise après sinistre consiste à utiliser de multiples centres informatiques dispersés dans différentes régions géographiques.

Tous les centres informatiques SoftLayer IBM disposent de multiples sources d'alimentation électrique, de liaisons par fibres optiques, de génératrices dédiées et de batteries de secours. Ils comportent du matériel et de l'équipement d'avant-garde dans l'industrie et assurent les plus hauts niveaux de performances, de fiabilité et d'interopérabilité. Par exemple, tous les composants des centres

informatiques qui doivent inclure des unités d'alimentation électrique et de refroidissement redondantes (n+1) font l'objet d'une inspection afin de maintenir la stabilité dans les centres informatiques.

10. Conformité

Les pratiques de sécurité d'IBM sont basées sur la norme ISO 27001-27002. Ces pratiques fournissent des structures de contrôle, notamment pour l'analyse des risques, la sécurité physique, la planification des mesures d'urgence, les investigations, la protection de l'information, la formation, la protection des données et les opérations.

IBM vérifie la conformité des activités de sécurité et de protection des renseignements personnels par rapport à ses pratiques de sécurité.

IBM se conforme à toutes les Lois sur la protection des données qui s'appliquent à IBM dans les Territoires visés.

Les Règles de conduite dans les affaires d'IBM exigent aussi de traiter comme il se doit l'information confidentielle des Clients. Tous les employés d'IBM doivent passer en revue ces règles chaque année et certifier qu'ils les ont revues.

11. Divers

IBM doit s'assurer que tous ses contrats conclus avec des sous-traitants ou des tiers qui participent à la livraison du Logiciel-service IBM comportent des modalités qui protègent tout autant le contenu du Client que celles du présent Appendice C et tout Document associé applicable, dans la mesure où ces modalités s'appliquent aux services que doivent rendre ces sous-traitants et ces tiers.