IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding

IBM Watson Health Core

De Gebruiksvoorwaarden ("ToU") bestaan uit deze IBM Gebruiksvoorwaarden – SaaS Specifieke Voorwaarden voor Aanbieding ("SaaS Specifieke Voorwaarden voor Aanbieding") en een document met de titel IBM Gebruiksvoorwaarden – Algemene bepalingen ("Algemene Voorwaarden") dat beschikbaar is op de volgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

In geval van tegenstrijdigheid prevaleren de SaaS Specifieke Voorwaarden voor Aanbieding boven de Algemene Voorwaarden. Door de IBM SaaS te bestellen, te openen of te gebruiken, geeft Klant aan akkoord te gaan met de Gebruiksvoorwaarden.

De Gebruiksvoorwaarden worden beheerst door de IBM International Passport Advantage Overeenkomst, de IBM International Passport Advantage Express Overeenkomst of de IBM International Agreement for Selected IBM SaaS Offerings, zoals van toepassing ("Overeenkomst") en vormen samen met de Gebruiksvoorwaarden de volledige overeenkomst.

1. IBM SaaS

De volgende IBM SaaS-aanbiedingen worden gedekt door deze SaaS Specifieke Voorwaarden voor Aanbieding:

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

2. Maateenheden voor verschuldigde bedragen

De IBM SaaS wordt verkocht onder een van de volgende maateenheden voor verschuldigde bedragen, zoals aangegeven in het Transactiedocument:

a. **Toegang** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Toegang is het recht om gebruik te maken van de IBM SaaS. Klant dient een enkel gebruiksrecht voor Toegang te verkrijgen om tijdens de in het Bewijs van Gebruiksrecht of Transactiedocument van Klant aangegeven meetperiode gebruik te mogen maken van de IBM SaaS.

b. **Individu** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Een Individu is één mens of één ding. Er dienen voldoende gebruiksrechten te worden verworven ter dekking van elk Individu dat tijdens de in het Bewijs van Gebruiksrecht of Transactiedocument van Klant aangegeven meetperiode door de IBM SaaS wordt verwerkt of beheerd.

   Voor het doel van deze IBM SaaS is een Individu: een persoon, apparaat of mobiele applicatie waarvan de data door de IBM SaaS worden beheerd.

c. **Instance** – is een maateenheid onder welke de IBM SaaS kan worden verkregen. Een Instance is de toegang tot een specifieke configuratie van de IBM SaaS. Er dienen voldoende gebruiksrechten te worden verworven voor elke Instance van de IBM SaaS die tijdens de in het Transactiedocument van Klant aangegeven meetperiode beschikbaar wordt gesteld voor toegang en gebruik.

3. Verschuldigde bedragen en facturering

Het verschuldigde bedrag voor de IBM SaaS wordt aangegeven in een Transactiedocument.

3.1 Verschuldigd bedrag voor een deel van een maand

Voor een deel van een maand kunnen er pro rato verschuldigde bedragen in rekening worden gebracht, zoals aangegeven in het Transactiedocument.

3.2 Verschuldigde bedragen bij overschrijding

Indien het feitelijke gebruik van de IBM SaaS door Klant tijdens de meetperiode het in het Bewijs van Gebruiksrecht aangegeven gebruiksrecht overschrijdt, wordt Klant voor de overschrijding gefactureerd zoals uiteengezet in het Transactiedocument.

4. Looptijd en verlengingsopties

De looptijd van de IBM SaaS begint op de datum waarop IBM Klant informeert omtrent diens toegang tot de operationele Pilot-omgeving van de IBM SaaS, zoals gedocumenteerd in het Besteldocument. De abonnementsperiode voor gebruiksrechten van Individuen begint op het moment dat IBM Klant informeert omtrent de toegang van die Individuen tot de operationele Productie-omgeving. In het Besteldocument wordt aangegeven of de IBM SaaS automatisch wordt verlengd, wordt voortgezet op basis van doorlopend gebruik, of eindigt aan het einde van de looptijd.

Bij automatische verlenging geldt dat de IBM SaaS automatisch met de in het Bewijs van Gebruiksrecht aangegeven looptijd wordt verlengd, tenzij Klant minimaal 90 dagen vóór het einde van looptijd schriftelijk opzegt.

Bij doorlopend gebruik blijft de IBM SaaS op maandelijkse basis beschikbaar, totdat Klant op een termijn van 90 dagen schriftelijk opzegt. Na die periode van 90 dagen blijft de IBM SaaS tot het einde van de kalendermaand beschikbaar.

5. Technische ondersteuning

IBM zal het IBM Software as a Service Support Handbook ter beschikking stellen, met daarin contactgegevens en onderhoudstijden voor technische ondersteuning en andere informatie en processen. Contactgegevens voor technische ondersteuning en andere informatie met betrekking tot ondersteuningsactiviteiten is te vinden in het IBM SaaS Support Handbook: https://support.ibmcloud.com.

Technische ondersteuning en eenvoudige configuratieverzoeken voor de IBM SaaS worden via elektronische verzending behandeld. Technische ondersteuning wordt verleend in combinatie met de IBM SaaS en is niet verkrijgbaar als afzonderlijke aanbieding.

Bij het melden van een incident mogen er geen Persoonsgegevens of Persoonlijke Gezondheidsgegevens worden opgenomen in de documentatie of informatie.

6. Definities

Van Toepassing Zijnde Wetgeving – betekent alle wetten, beschikkingen, wettelijke besluiten, regels, verordeningen, instructies, bevelen, uitspraken of andere vereisten van een overheidsinstantie en alle algemeen erkende branchestandaarden die van toepassing zijn op de uitvoering van deze Gebruiksvoorwaarden.

API – betekent een application program interface. Dit is set routines, protocollen en tools voor het bouwen van softwareapplicaties. De API geeft aan op welke manier de softwarecomponenten met elkaar moeten interacteren. API's worden gebruikt bij het programmeren van componenten voor grafische gebruikersinterfaces.

Geautoriseerde Beheerder – is een werknemer van Klant, een goedgekeurde contractant van Klant, een individu of een groep die verantwoordelijk is voor het onderhoud en de betrouwbare werking van het platform. Tot de verantwoordelijkheden kunnen onder meer behoren: configuratie, ondersteuning en gebruikers- en accountbeheer. De beheerder kan ook een klinisch onderzoeker zijn die verantwoordelijk is voor het opzetten van een onderzoek in het Watson Health-systeem.

Geautoriseerd Individu – is een geauthenticeerde persoon, geauthenticeerde mobiele applicatie of geauthenticeerd apparaat waaraan toegangsrechten zijn verleend voor het verzenden van data naar de Watson Health Core. Het kan hierbij gaan om Klant of om onderzoeksdeelnemers, klanten of patiënten van Klant.

Op Klant Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens – betekent de Wetgeving Inzake Persoonsgegevens die van toepassing is op de uitvoering van de verplichtingen van Klant krachtens de Overeenkomst, Bijbehorende Documenten en de desbetreffende Beschrijvingen van de Services, Besteldocumenten en Statements of Work tussen de Partijen.

Klantgegevens – betekent alle gegevens die door of voor Klant in de IBM SaaS worden ingevoerd, zijnde hetzij eigen gegevens van Klant, hetzij gegevens die door of namens een klant van Klant of enige derde worden ingevoerd, en met inbegrip van gegevens van een medisch welzijnsapparaat van een derde.

Wetgeving Inzake Persoonsgegevens – betekent de Van Toepassing Zijnde Wetgeving met betrekking tot privacy, bescherming en beveiliging van persoonsgegevens.

Betrokkene – betekent een geïdentificeerd of identificeerbaar individu op wie Persoonsgegevens betrekking hebben.

Aangewezen Datacenter – betekent het datacenter dat (of de datacenters die) in het Transactiedocument is (zijn) opgegeven voor de primaire en disaster recovery datacenters waarin de instance van de IBM SaaS van Klant draait, indien van toepassing.

Gezondheidsgegevens – betekent alle gegevens of informatie, met inbegrip van afbeeldingen, die worden aangemerkt als gezondheidsgerelateerde Persoonsgegevens.

Geschikt Voor Gezondheidsgegevens – betekent, wat betreft de IBM SaaS, het vermogen van de IBM SaaS om te voldoen aan de toepasselijke normen, wetten en regelingen inzake beveiliging en bescherming binnen In-Scope Landen voor Gezondheidsgegevens, met inbegrip van de in Artikel 164, Lid A en C van de verordeningen voor de tenuitvoerlegging van HIPAA (zoals gewijzigd door de HITECH Act) uiteengezette implementatiespecificaties en andere Van Toepassing Zijnde Wetgeving met betrekking tot Gezondheidsgegevens, maar betekent niet dat IBM optreedt in de hoedanigheid van Zakenpartner of Voor Gegevensverwerking Verantwoordelijke Partij.

HIPAA – betekent de Amerikaanse Health Insurance Portability and Accountability Act uit 1996, zoals geamendeerd, met inbegrip van de Health Information Technology for Economic & Clinical Health Act van de American Recovery and Reinvestment Act uit 2009 ("HITECH Act"), bepaalde door het United States Department of Health and Human Services in 45 C.F.R. Artikel 160 en 164 uitgevaardigde verordeningen onder HIPAA en bepaalde ingevolge de HITECH Act uitgevaardigde Verordeningen.

Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens – betekent de Wetgeving Inzake Persoonsgegevens die van toepassing is op de uitvoering van de verplichtingen van IBM krachtens de Overeenkomst, Bijbehorende Documenten en de desbetreffende Beschrijvingen van de Services, Besteldocumenten en Statements of Work tussen de Partijen.

IBM Personeel – betekent (a) IBM, zijn Gelieerde Ondernemingen en zijn subcontractanten, en met betrekking tot elk van de voorgaande: hun werknemers; en (b) alle derde-partij leveranciers, in elk geval, die namens IBM services uitvoeren ingevolge de Overeenkomst en de toepasselijke Bijbehorende Documenten of aan wie IBM anderszins toegang verleent tot Persoonsgegevens van Klant.

In-scope Landen – betekent de 28 Lidstaten van de Europese Unie en Zwitserland, en die landen die IBM van tijd tot tijd aan deze lijst kan toevoegen.

Persoonsgegevens of **Persoonlijke Informatie** – betekent informatie op enig medium of in enige indeling, met inbegrip van elektronisch en op papier, die betrekking heeft op een geïdentificeerd of identificeerbaar individu, waarbij een "identificeerbaar individu" een persoon is die, rechtstreeks of indirect, kan worden geïdentificeerd, met name onder verwijzing naar een identificatienummer of naar een of meer factoren die kenmerkend zijn voor zijn/haar fysieke, fysiologische, mentale, economische, culturele of sociale identiteit.

Verwerken en de varianten ervan, zoals **verwerking** (al dan niet met hoofdletters) – betekent enige bewerking of groep bewerkingen die op gegevens wordt uitgevoerd, al dan niet op automatische wijze, zoals het verzamelen, opnemen, ordenen, opslaan, aanpassen of wijzigen, ophalen, raadplegen, gebruiken, middels transmissie, verspreiding of anderszins openbaar maken, afstemmen of combineren, blokkeren, wissen of vernietigen van gegevens.

Verwerkte Gegevens – alle gegevens, vertrouwelijke of eigen informatie of materialen, met inbegrip van Gezondheidsgegevens en Persoonsgegevens, die door IBM worden verwerkt ingevolge de Overeenkomst, een Bijbehorend Document en/of een Beschrijving van de Services, Besteldocument en/of Statement of Work.

Beveiligingsincident – heeft de in de SBCA uiteengezette betekenis.

7. Account Management

De IBM SaaS is uitsluitend toegankelijk voor geautoriseerde gebruikers van Klant ("**Geautoriseerde Beheerders**" of "**Geautoriseerde Individuen**"). Klant controleert de voor toegang tot de IBM SaaS gemachtigde accounts, waartoe geautoriseerde applicaties, personeel van Klant, derde-partij dienstverleners van Klant en contractanten kunnen behoren, en is als enige verantwoordelijk voor (i) het controleren van alle gemachtigde gebruikers, met inbegrip van, maar niet beperkt tot, het verifiëren van de identiteit van elke geautoriseerde gebruiker; en (ii) het waarborgen dat uitsluitend geautoriseerde gebruikers zich toegang verschaffen tot de IBM SaaS.

Aan Geautoriseerde Individuen die klanten, patiënten of deelnemers aan een onderzoek van Klant zijn, mag uitsluitend toegang worden verleend ten behoeve van het uploaden van gegevens naar de IBM

SaaS, in welk geval de desbetreffende Geautoriseerde Individuen geen andere toegang tot de IBM SaaS krijgen.

8. Privacy

8.1 Algemene vereisten

Wat betreft de relatie tussen partijen geldt dat Klant de enige voor de verwerking van alle Persoonsgegevens van Klant verantwoordelijke partij is ("controller") en dat Klant IBM aanstelt als verwerker ("processor") van gegevens. Overeenkomstig de Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens heeft Klant het recht om IBM instructies te geven in samenhang met de verwerking van Persoonsgegevens van Klant door IBM.

Voor zover IBM Persoonsgegevens van Klant verwerkt, zal IBM:

a. alle Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens naleven; en

b. Persoonsgegevens van Klant niet in aanraking laten komen met gegevens uit andere bronnen, behoudens:

   - zoals noodzakelijk voor het leveren van de IBM SaaS, en dan niet voor enig ander doel, tenzij Klant daartoe uitdrukkelijk opdracht heeft gegeven; en
   - overeenkomstig de bepalingen van deze Gebruiksvoorwaarden en de SBCA Appendix.

Voor zover IBM Persoonsgegevens van Klant verwerkt, zal Klant:

a. alle Op Klant Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens naleven;

b. de verantwoordelijkheid dragen voor alle communicatie van Klant met Gelieerde Ondernemingen, patiënten, eindgebruikers, Betrokkenen en/of andere derde partijen van Klant;

c. overeenkomsten inzake gegevensverwerking aangaan met zijn voor de verwerking van Persoonsgegevens verantwoordelijke partijen, voor zover noodzakelijk om IBM als verwerker en zijn subverwerkers toestemming te verlenen om Persoonsgegevens van Klant te verwerken; en

d. fungeren als enkel aanspreekpunt voor IBM, en als enige verantwoordelijk zijn voor de interne coördinatie, controle en verzending van instructies of verzoeken van Gelieerde Ondernemingen van Klant die tegenover IBM andere voor de verwerking verantwoordelijke partijen zijn. IBM wordt ontheven van zijn verplichting om een Gelieerde Onderneming van Klant die optreedt als voor de verwerking verantwoordelijke partij, te informeren of in te lichten wanneer IBM dergelijke informatie of inlichtingen aan Klant heeft verstrekt. IBM heeft het recht om instructies die rechtstreekse afkomstig zijn van een Gelieerde Onderneming van Klant die optreedt als voor de verwerking verantwoordelijke partij, te weigeren.

Van geen der partijen wordt verlangd te handelen in strijd met de op de desbetreffende partij Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens.

8.2 Rechten van Klant op gegevens

Klant verklaart en garandeert (a) eigenaar te zijn van de gegevens die worden ingevoerd in de IBM SaaS, of (b) in het bezit te zijn van, of verantwoordelijk te zijn voor, alle noodzakelijke rechten, toestemmingen, goedkeuringen en autorisaties om IBM de rechten te verlenen voor het zich verschaffen van toegang tot, het gebruiken van en het openbaar maken van de Klantgegevens overeenkomstig deze Gebruiksvoorwaarden of de Overeenkomst, of zoals anderszins voor IBM noodzakelijk voor het leveren van de IBM SaaS. Klant verklaart en garandeert voorts dat de Klantgegevens uitsluitend gerelateerd zullen zijn aan hetzij (a) individuen die in de Verenigde Staten verblijven en dan uitsluitend in de IBM SaaS zullen worden ingevoerd in het datacenter dat zich in de Verenigde Staten bevindt; hetzij (b) individuen die in een of meer In-Scope Landen verblijven en dan uitsluitend in de IBM SaaS zullen worden ingevoerd in het (de) Aangewezen Datacenter(s).

8.3 Dataservices en verantwoordelijkheden

a. Klant verklaart uitsluitend analyses of aanvragen waarbij analysefuncties van IBM op de Klantgegevens worden uitgevoerd, te zullen uitvoeren in samenhang met activiteiten die hetzij "zorg-gerelateerde activiteiten" ("health care operations") hetzij onderzoek ("research") van Klant behelzen, elk zoals gedefinieerd onder HIPAA en/of vergelijkbare termen onder andere Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens, en dat Klant de Klantgegevens uitsluitend zal gebruiken, of IBM uitsluitend opdracht zal gegeven om de Klantgegevens te gebruiken, in overeenstemming met alle relevante vereisten (bijvoorbeeld, waar nodig, een oordeel of ontheffing van een institutionele beoordelingscommissie) onder deze of andere Op Klant Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens.

b. Klant is als enige verantwoordelijk voor het verkrijgen van alle registraties, toestemmingen, goedkeuringen en autorisaties die onder de voor Klant Van Toepassing Zijnde Wetgeving in elk In-Scope Land vereist zijn, met inbegrip van, maar niet beperkt tot, HIPAA en alle andere wetten, regels en voorschriften inzake bescherming van persoonsgegevens, zodat de Klantgegevens in de IBM SaaS kunnen worden ingevoerd en kunnen worden gebruikt en geopenbaard zoals onder deze Gebruiksvoorwaarden en de Overeenkomst, door Klant en door IBM en de toegestane subcontractanten van IBM. IBM draagt geen verantwoordelijkheid voor de vaststelling óf en wanneer dergelijke registraties, toestemmingen, goedkeuringen en autorisaties ontvangen dan wel vereist zijn.

c. Klant is als enige verantwoordelijk voor de garantie dat de in de IBM SaaS ingevoerde Klantgegevens beperkt zijn tot gegevens met betrekking tot individuen die in de Verenigde Staten of in een toepasselijk In-Scope Land verblijven.

d. IBM onderhoudt support centers met personeel dat is opgeleid in HIPAA en andere Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens met betrekking tot gegevens uit In-Scope Landen.

8.4 Beveiligingsmaatregelen en Beveiligingsincidenten

a. IBM zal de technische en organisatorische maatregelen (met inbegrip van organisatieprocessen en -procedures en specifieke beveiligingsverplichtingen die in deze Gebruiksvoorwaarden en de SBCA worden genoemd of waarnaar hierin wordt verwezen) doorvoeren, onderhouden en naleven teneinde de Persoonsgegevens van Klant te beschermen tegen onbevoegd gebruik, onbevoegde toegang, onbedoeld verlies, beschadiging, verandering, vernietiging, diefstal of onbevoegde openbaarmaking.

b. In geval IBM kennis krijgt van een Beveiligingsincident (zoals gedefinieerd door de SBCA) waarbij Verwerkte Gegevens van Klant betrokken zijn, zal IBM Klant inlichten overeenkomstig de SBCA en de Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens, en in de desbetreffende kennisgeving zal informatie worden opgenomen omtrent de bekende impact op Klant of enige Betrokkene op wie het desbetreffende Beveiligingsincident van invloed is, alsmede omtrent de herstelprocedure die IBM volgt of voorstelt.

8.5 Ontvangst van klachten en verzoeken om inlichtingen

IBM zal Klant onverwijld, en voor zover toegestaan onder de Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens niet later dan vijf (5) werkdagen na ontvangst daarvan door de Data Privacy Officer van IBM Watson Health, schriftelijk inlichten omtrent een door IBM ontvangen verzoek om inlichtingen, een mededeling of een klacht met betrekking tot Persoonsgegevens van Klant, afkomstig van:

a. een Betrokkene, met betrekking tot door IBM Verwerkte Persoonsgegevens van de desbetreffende Betrokkene. Klant zal al dergelijke mededelingen van Betrokkenen beantwoorden, en bij het assisteren van Klant om dergelijke mededelingen te beantwoorden, zal IBM de instructies van Klant naar redelijkheid uitvoeren. Indien de Op IBM Van Toepassing Zijnde Wetgeving zulks verlangt, zal IBM dergelijke mededelingen rechtstreeks beantwoorden, mits IBM Klant vooraf van een dergelijk antwoord in kennis stelt en mits IBM de vorm en inhoud van een dergelijk antwoord naar redelijkheid afstemt met Klant, wanneer dit onder de Op IBM Van Toepassing Zijnde Wetgeving toegestaan of anderszins mogelijk is;

b. een wettelijke of regelgevende instantie, met betrekking tot de Verwerking van Persoonsgegevens van Klant door IBM, met dien verstande dat IBM gehoor zal geven aan dergelijke verzoeken indien ontvangen van een overheidsinstantie met een dagvaarding of ander wettig document waarin IBM tot openbaarmaking wordt gedwongen, of zoals anderszins verplicht onder de Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens, met dien verstande dat IBM Klant vooraf van een dergelijke openbaarmaking in kennis zal stellen en IBM de vorm en inhoud van een dergelijke openbaarmaking naar redelijkheid zal afstemmen met Klant, wanneer dit wettelijk toegestaan of anderszins mogelijk is.

8.6 Verwerking van Persoonsgegevens van Klant

IBM zal de openbaarmaking van Persoonsgegevens van Klant beperken tot dat IBM Personeel dat noodzakelijk kan zijn voor assistentie bij het verlenen van de Services.

IBM zal voldoen aan elk redelijk verzoek van Klant om Persoonsgegevens van Klant te wijzigen, te corrigeren, te wissen of te blokkeren overeenkomstig de Van Toepassing Zijnde Wetgeving.

Op verzoek van een van beide partijen zullen IBM, Klant of hun Gelieerde Ondernemingen, ter bescherming van de Persoonsgegevens van Klant, wettelijk verplichte standaardovereenkomsten aangaan. De partijen stemmen ermee in (en zullen bewerkstelligen dat hun respectievelijke Gelieerde Ondernemingen ermee instemmen) dat dergelijke overeenkomsten, wat betreft vorderingen tussen de partijen, onderworpen zijn aan de aansprakelijkheidsbeperkingen en -uitsluitingen in deze Overeenkomst. Partijen zullen hun medewerking verlenen (of zullen bewerkstelligen dat hun Gelieerde Ondernemingen hun medewerking verlenen) aan het aangaan en naleven van verdere wederzijds overeengekomen bepalingen of overeenkomsten, voor zover de Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens dit verlangt.

8.7 Retourzending van Persoonsgegevens van Klant

Bij afloop of beëindiging van de Overeenkomst zal IBM het gebruik of de verwerking van alle Eigen Informatie van Klant en alle Persoonsgegevens van Klant staken, zal IBM al het IBM Personeel opdragen datzelfde te doen en zal IBM, naar keuze en op verzoek van Klant:

a. alle Eigen Informatie van Klant en Persoonsgegevens van Klant die in elektronische vorm opgeslagen zijn door IBM, onverwijld aan Klant retourneren in een indeling en op een opslagmedium waar Klant naar redelijkheid om heeft verzocht, en, na ontvangstbevestiging door Klant, alle Eigen Informatie van Klant en Persoonsgegevens van Klant (met inbegrip van kopieën en backups) wissen, vernietigen of anderszins onleesbaar of onontcijferbaar maken. IBM kan bedragen in rekening brengen voor de kosten van opslagmedia en bepaalde op verzoek van Klant uitgevoerde activiteiten (zoals het in een specifieke indeling leveren of op een specifieke wijze vernietigen van Eigen Informatie van Klant en Persoonsgegevens van Klant); en

b. alle Eigen Informatie van Klant en Persoonsgegevens van Klant (met inbegrip van kopieën en backups) direct wissen, vernietigen of anderszins onleesbaar of onontcijferbaar maken.

8.8 Business Associate Agreement

Voor zover HIPAA dit voorschrijft, zullen IBM en Klant een Business Associate Agreement ("BAA") aangaan, welke de verplichtingen van IBM als Zakenpartner van Klant regelt bij de levering van de IBM SaaS. Zonder de uitdrukkelijke verplichtingen van IBM onder de Overeenkomst en de BAA (indien van toepassing) te beperken, erkent Klant en gaat hij ermee akkoord verantwoordelijk te zijn voor het vaststellen van de toepasbaarheid van, en voor het naleven van, de Van Toepassing Zijnde Wetgeving en alle licentievereisten die van toepassing zijn op het gebruik of de andere activiteiten van Klant (met inbegrip van het gebruik of andere activiteiten door Geautoriseerde Gebruikers) met betrekking tot de IBM SaaS.

8.9 Europese Unie: Data Processing Addendum

Indien Klant IBM opdracht geeft om Persoonsgegevens uit de Europese Unie te verwerken, gaan IBM en Klant een Data Processing Addendum aan met daarin, zoals van toepassing, E.U. Modelclausules, waarbij de optionele clausules verwijderd zijn.

9. Aanvullende bepalingen voor IBM SaaS-aanbiedingen

9.1 Beveiliging

Deze IBM SaaS volgt IBM's grondslagen inzake gegevensbeveiliging en -bescherming voor IBM SaaS, welke beschikbaar zijn op http://www.ibm.com/cloud/data-security, alsmede de hieronder en in het Appendix Beveiliging en Bedrijfscontinuïteit van deze Gebruiksvoorwaarden gespecificeerde aanvullende bepalingen. Geen enkele wijziging in IBM's grondslagen inzake gegevensbeveiliging en -bescherming zal ertoe leiden dat de beveiliging van de IBM SaaS afneemt.

IBM Watson Health Core implementeert beveiligingsbeleid, -standaarden en -processen op basis van het ISO 27001-framework zoals verder beschreven in de beschrijving van de Beveiliging. In het kader van de beveiligingsmogelijkheden implementeert de oplossing onder meer:

a. Veilige operationele zones

   IBM Watson Health Core implementeert een diepgaande verdedigingsstrategie ("defense in depth") waarin er wordt gewerkt met meerdere beveiligingszones voor het beheer van cloud-integratiepunten zoals data onboarding en de ontwikkeling van applicaties op maat.

b. Versleuteling

   Alle Klantgegevens worden zowel tijdens opslag ("at rest") als tijdens de verzending ("in flight") versleuteld. Alle gegevens op weg van en naar IBM Watson Health Core worden versleuteld. Een gemeenschappelijke service verzorgt het beheer van codeersleutels (encryption keys). Klant is verantwoordelijk voor alle netwerkconnectiviteit en de kwaliteit van alle netwerken tussen IBM Watson Health Service en de proxyserver van Klant.

c. Security Event Monitoring

   IBM zet zijn security intelligence platform in ten behoeve van het beheer van beveiligingsinformatie en -events, logboekbeheer, forensisch onderzoek naar incidenten, detectie van dreigingen en beheer van kwetsbaarheden.

d. Identity Management

   - Watson Health Core ondersteunt met open standaarden werkende ID-providers voor grootschalige patiënten- en gebruikerspopulaties met behulp van OpenID Connect.
   - Bij gebruikerspopulaties waarvoor IBM de ID-provider is, werkt Watson Health Core wat betreft de authenticatie met passende directoryservices en mogelijkheden voor identiteitsbeheer.

e. Sterke authenticatie en toegang op basis van rollen

   - Watson Health Core ondersteunt authenticatie via SAML. Dit vormt voor klanten een mechanisme om hun SSO- (Single Sign On) of directoryservices te integreren.
   - Waar nodig werkt Watson Health Core met een oplossing voor toegangsbesturing en de bijbehorende componenten voor het beheer van beleidsdefinities.
   - Watson Health Core ondersteunt softwarematige two-factor authenticatie.
   - Watson Health Core biedt elementaire, op rollen gebaseerde toegangscontrole, zoals vereist. Watson Health Core ondersteunt de configuratie van onderzoeken, gebruikersprofielen, rollen en gebruikersgroepen via application programming interfaces ("API" of "API's") die op rollen gebaseerde toegang mogelijk maken.

9.2 Cookies

Klant is zich ervan bewust en gaat ermee akkoord dat IBM, in het kader van de normale exploitatie en ondersteuning van de IBM SaaS, met behulp van tracerings- en andere technologie persoonsgegevens van Klant (uw werknemers en contractanten) kan verzamelen, verband houdend met het gebruik van de IBM SaaS. IBM doet dit ten behoeve van het verzamelen van gebruikscijfers en informatie over de effectiviteit van onze IBM SaaS, gericht op het verbeteren van de gebruikerservaring en/of het op maat toesnijden van interacties met Klant. Klant bevestigt toestemming te zullen verkrijgen of te hebben verkregen om IBM in staat te stellen de verzamelde persoonsgegevens, overeenkomstig de toepasselijke wetgeving, te verwerken voor de bovengenoemde doeleinden binnen IBM, andere IBM ondernemingen en hun onderaannemers, overal waar IBM en haar onderaannemers zakendoen. IBM zal voldoen aan verzoeken van werknemers en contractanten van Klant om de over hun verzamelde persoonsgegevens in te zien, bij te werken, te corrigeren en/of te wissen.

9.3 Profijt genietende locaties

Waar van toepassing worden de belastingen gebaseerd op de locatie(s) waarvan Klant aangeeft dat deze profijt geniet(en) van de IBM SaaS. Tenzij Klant IBM aanvullende informatie verstrekt, berekent IBM de belastingen op basis van het bedrijfsadres zoals dat bij het bestellen van een IBM SaaS bij IBM bekend is. Klant is verantwoordelijk voor het actueel houden van de desbetreffende informatie en voor het doorgeven van wijzigingen aan IBM.

9.4 Continuous Delivery

Klant heeft recht op aan de oplossing toegevoegde mogelijkheden en in de oplossing aangebrachte verbeteringen die door IBM zijn geïmplementeerd in een zogenoemd "continuous cloud delivery model".

9.5 Backup en herstel

IBM Watson Health Core maakt backups van Klantgegevens in de productieomgeving (met inbegrip van de repository's Data Lake en Data Reservoir) teneinde de service in geval van een systeemstoring te kunnen terugzetten in de laatst bekende goed werkende staat.

9.6 High Availability

De componenten van IBM Watson Health Core in de productieomgeving worden geïmplementeerd in high-availability configuraties, met, omwille van de redundantie, geclusterde databaseservers, zodat de werkbelasting kan worden verdeeld en er zo min mogelijk single-points-of-failure ontstaan.

9.7 Disaster Recovery

IBM's aanpak van disaster recovery bestaat uit meerdere datacenters in geografisch ver van elkaar af gelegen gebieden, teneinde voor zijn Productieomgeving de volgende doelstellingen inzake bedrijfscontinuïteit te realiseren:

- RTO – binnen 36 uur nadat er een calamiteit is afgekondigd
- RPO – niet meer dan 24 uur verlies van content van Klant

9.8 Metingstools

De IBM SaaS maakt gebruik van een synthetische monitoringoplossing voor het monitoren, meten en melden van de beschikbaarheid of van outages ten opzichte van toegezegde serviceniveaus. Deze oplossing simuleert en volgt de gebruikersreacties en -ervaringen op algemeen niveau – zowel voor statische beschikbaarheid als voor transacties.

De IBM SaaS maakt tevens gebruik van een intern monitoringsysteem voor gebruikscijfers, events en alerts in de volledige oplossing.

9.9 Publiciteit

Klant gaat ermee akkoord dat IBM Klant in het openbaar in publicitaire of marketinguitingen mag noemen als abonnee van de IBM SaaS.

Bijlage A

1. IBM Watson Health Core

IBM Watson Health Core is een platform-as-a-service (PaaS) Geschikt Voor Gezondheidsgegevens, een ontwikkelplatform en een operationeel subsysteem voor het overeenkomstig de Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens opslaan, onderhouden en verwerken van beschermde gezondheidsgegevens (Protected Health Information, PHI), zoals gedefinieerd door HIPAA, en andere Gezondheidsgegevens die zich bevinden in een datacenter dat eigendom is van IBM of dat door IBM wordt gecontroleerd. Om de onderstaande mogelijkheden te kunnen gebruiken, dient Klant passende gebruiksrechten voor IBM Watson Health Core en IBM Watson Health Core Access te hebben verworven.

1.1 Watson Health Core - Gebruiksomgevingen

Het gebruiksrecht voor Watson Health Core beslaat drie operationele cloud-omgevingen Geschikt Voor Gezondheidsgegevens, bedoeld om Klant in staat te stellen Gezondheidsgegevens te verwerken:

- Pilot

  Vormt een sandbox-omgeving waarin Klant met behulp van de IBM SaaS gebouwde applicaties kan ontwikkelen en testen. In de pilot-omgeving zijn alle beveiligingsmaatregelen van HIPAA geïmplementeerd, met uitzondering van Disaster Recovery, high availability en backup van systems-of-record.

- Productieomgeving

  Vormt een omgeving op volledige schaal, waarin Klant workloads met Gezondheidsgegevens kan implementeren. De productieomgeving is een highly-available, load-balanced omgeving die in staat is om terug te vallen ("fail over") op een Disaster Recovery-locatie.

- Disaster Recovery

  Vormt een gespiegelde replica van de Productieomgeving en bevindt zich in een afzonderlijke datacentervestiging.

1.2 Applicatieontwikkeling

IBM Watson Health Core maakt applicatieontwikkeling mogelijk, alsmede het veilig verzamelen van gegevens van apparaten van Klant of apparaten van geautoriseerde gebruikers van Klant. API's bevatten programma-interfaces en documentatie die door de geautoriseerde gebruikers van klant, met inbegrip van de derde-partij serviceproviders van Klant, kunnen worden gebruikt voor het ontwikkelen van applicaties en het uitwisselen van gegevens met de IBM SaaS. Voor het gebruik van de API's door Klant of zijn ontwikkelaars is naleving van de API Developer Requirements een voorwaarde.

- REST API's

  Watson Health Core biedt een aantal REST API's en services voor het Watson Health Core-platform. Tot de mogelijkheden van API's behoren onder meer mechanismen voor het verkrijgen van toegang tot de gegevensrepository's, de service voor gegevensonderhoud, gebruikersbeheer en auditlogboeken.

- Apple HealthKit en Apple ResearchKit

  Watson Health Core ondersteunt de integratie met het API-framework van Apple ResearchKit voor onderzoek onder het besturingssysteem iOS, waarbij Apple HealthKit de welzijnsgegevens vastlegt.

1.3 Data Governance

- Consent Management

  Watson Health Core verzorgt het framework voor het vastleggen van toestemmingen verleend door patiënten of onderzoeksdeelnemers en is in staat om de toestemmingen veilig en los van de gegevenspayload op te slaan wanneer een individu zich inschrijft voor een toestemmings-geschikte applicatie van Klant.

- Data Masking

  Watson Health Core biedt de mogelijkheid om naam-ID's te scheiden van gestructureerde gegevenspayloads. Watson Health Core ontvangt gegevens in de cloud via programma-API's. De

API's maken het mogelijk om de naam-ID's van patiënten of individuen te scheiden van de rest van de gegevenspayload, voor opslag in een afzonderlijke, versleutelde datastore. De gegevenspayload wordt toegewezen aan een geanonimiseerd token dat kan worden gebruikt om in de toekomst de herkomst te achterhalen.

1.4 Health Data Services

Watson Health Core verzorgt het verzamelen, opslaan en synchroniseren van gegevens, met inbegrip van exogene Gezondheidsgegevens en andere persoonsgegevens, zowel gestructureerd als ongestructureerd.

- Data Ingestion

  Watson Health Core biedt de mogelijk om, via programma-API's, gegevens op te nemen uit patiëntenapplicaites of apparaten. Watson Health Core geeft elke van de Geautoriseerde Individuen van Klant het recht om gedurende de looptijd van het contract jaarlijks maximaal 25 MB aan gegevens te uploaden. De service biedt ruimte aan maximaal 10 uploads per Individu per dag.

- Operational Data Lake

  Ruwe gegevens van Klant en ruwe patiëntengegevens worden in hun oorspronkelijke ("native") vorm in Watson Health Core opgeslagen totdat ze nodig zijn voor analytics en modellering.

- Extract Transform Load (ETL)

  Binnen het operationele subsysteem worden de gegevens omgezet in een genormaliseerde indeling. Een op branchestandaarden voor de zorgsector gebaseerde Enterprise Service Bus maakt de integratie van verschillende applicaties en protocollen van Klant mogelijk.

- Data Reservoir

  Na te zijn opgeschoond worden de gegevens overgebracht naar het Data Reservoir. Watson Health Core maakt voor het normaliseren van zakelijke en technische gezondheidsgegevens ten behoeve van analytics gebruik van het IBM Unified Data Model for Healthcare.

- Master Person Index

  Watson Health biedt tools voor Master Data Management, teneinde gegevens vanuit meerdere bronnen samen te voegen, zodat er een Longitudinal Person Record (LPR) ontstaat.

2. Optionele functionaliteit/kenmerken

2.1 IBM Watson Health Core Terminology Service

Deze add-on service verzorgt de gegevensintegratie en interoperabiliteit tussen ongelijksoortige gezondheidssystemen en zorgt voor een consistent gebruik van de klinische terminologie binnen alle applicaties van Watson Health Cloud. Deze service vormt het functionele platform voor alle taken waarin terminologie, codesystemen en gestructureerde content een rol spelen, zoals:

- aanmaak van nieuwe codesystemen;
- vertaling van internationale codesystemen; en
- koppelingen ("mappings") tussen lokale codelijsten en internationale standaarden.

Bijlage B

IBM levert de volgende overeenkomst inzake het serviceniveau (service level agreement, "SLA") voor de beschikbaarheid van de IBM SaaS zoals aangegeven in een Bewijs van Gebruiksrecht. De SLA is geen garantie. De SLA is uitsluitend beschikbaar voor Klant en geldt uitsluitend voor gebruik in een productie-omgeving.

1. Beschikbaarheidskrediet

Er zijn uitsluitend beschikbaarheidskortingen beschikbaar voor abonnementen met gebruiksrechten op basis van Individuen.

Klant dient een ondersteuningsticket van Severity 1 te hebben geregistreerd bij de helpdesk van IBM Technical Support, en wel binnen 24 uur nadat het Klant voor het eerst duidelijk werd dat de Gebeurtenis negatieve gevolgen had voor de beschikbaarheid van de IBM SaaS. Klant dient IBM naar redelijkheid te assisteren bij het diagnosticeren en oplossen van het probleem.

Een vordering wegens niet-nakoming van een SLA moet worden ingediend binnen drie werkdagen na het eind van de contractmaand. Een geldige SLA-vordering wordt vergoed in de vorm van een krediet dat kan worden gebruikt voor toekomstige facturen voor de IBM SaaS, op basis van de tijdsduur gedurende welke de verwerking door de productiesystemen voor de IBM SaaS niet beschikbaar was ("Downtime"). Downtime wordt gemeten vanaf het tijdstip waarop Klant de gebeurtenis meldt tot het tijdstip waarop de IBM SaaS is hervat. Van Downtime zijn uitgesloten: tijd die verband houdt met gepland of aangekondigd onderhoud; oorzaken waar IBM geen invloed op heeft; problemen met content, technologie ontwerpen of instructies van een Klant of een derde partij; niet-ondersteunde systeemconfiguraties en platforms of andere fouten van Klant; en door Klant veroorzaakte beveiligingsincidenten dan wel door Klant uitgevoerde beveiligingstests. IBM kent de hoogste van toepassing zijnde vergoeding toe op basis van de cumulatieve beschikbaarheid van de IBM SaaS tijdens elke contractmaand, zoals aangegeven in de onderstaande tabel. De totale vergoeding met betrekking tot enige contractmaand is in geen geval hoger dan 20 procent van een twaalfde deel (1/12e) van het jaarbedrag voor de IBM SaaS.

2. Serviceniveaus

Beschikbaarheid van de IBM SaaS tijdens een contractmaand

Beschikbaarheid tijdens een contractmaand	**Vergoeding (% van maandelijks Individueel abonnementsbedrag* voor de contractmaand waarop een vordering betrekking heeft)**
< 99,95%	10%
< 99,0%	20%

* Indien de IBM SaaS is aangekocht bij een IBM Business Partner wordt het maandelijkse abonnementsbedrag berekend op basis van de op dat moment geldende catalogusprijs voor de IBM SaaS voor de contractmaand waarop een vordering betrekking heeft, onder aftrek van een korting van 50%. IBM stelt een korting onmiddellijk beschikbaar aan Klant.

Beschikbaarheid, uitgedrukt als een percentage, wordt als volgt berekend: het totaal aantal minuten in een contractmaand minus het totaal aantal minuten Downtime in een contractmaand, gedeeld door het totaal aantal minuten in een contractmaand.

Voorbeeld: Totaal 108 minuten Downtime gedurende een contractmaand

Totaal 43.200 minuten in een contractmaand van 30 dagen - 108 minuten Downtime = 43.092 minuten _____ Totaal 43.200 minuten	= 10% Beschikbaarheidskrediet voor 99,75% beschikbaarheid tijdens de contractmaand

3. Uitzonderingen

Deze SLA is niet van toepassing op het volgende:

- Afgezien van servermonitoring geldt de SLA niet voor gehoste virtuele machines ter ondersteuning van applicaties op maat of applicaties van Klant.
- Indien Klant enige materiële verplichting onder de actuele contractuele verplichtingen niet is nagekomen.

Bijlage C

Deze Bijlage Beveiliging en Bedrijfscontinuïteit ("BBBC") beschrijft bepaalde vereisten en verplichtingen waar IBM bij het leveren van de IBM SaaS aan Klant aan gebonden is. De hierin beschreven vereisten en verplichtingen vormen een aanvulling op datgene wat is beschreven als de uitgangspunten voor gegevensbeveiliging voor IBM SaaS, te vinden op http://www.ibm.com/cloud/data-security. Termen met hoofdletters die hierin niet worden gedefinieerd, hebben de in de Overeenkomst of Gebruiksvoorwaarden aangegeven betekenis.

1. Informatiebeveiligingsprogramma

IBM hanteert een intern beveiligingsbeleid en interne beveiligingsstandaarden en -processen op basis van het ISO 27001-framework en controlegebieden. Dit beleid, deze standaarden en deze processen worden aangestuurd door de divisie IBM Corporate Security en worden regelmatig onderworpen aan interne audits.

Met betrekking tot de verwerking, opslag en transmissie van content van Klant onderhoudt IBM een informatiebeveiligingsprogramma bestaande uit organisatorische, operationele, administratieve, fysieke en technische maatregelen die voldoen aan de vereisten van de SBCA.

Op verzoek van Klant zal IBM informatie over het informatiebeveiligingsprogramma van IBM Watson Health met Klant delen, zodat Klant redelijkerwijs kan vaststellen of dat programma nog steeds geschikt, adequaat en effectief is. Het informatiebeveiligingsprogramma van IBM Watson Health zal van tijd tot tijd worden bijgewerkt om in de pas te blijven lopen met de algemeen gangbare werkwijzen binnen de branche en met de Op IBM Van Toepassing Zijnde Wetgeving.

2. Toegangsbesturing

IBM zal content van Klant uitsluitend vrijgeven aan zijn werknemers, subcontractanten of derden die uit hoofde van hun functie toegang moeten hebben tot content van Klant teneinde IBM te assisteren bij het uitvoeren van zijn verplichtingen jegens Klant of andere personen, zoals noodzakelijk voor het leveren van de IBM SaaS overeenkomstig de Van Toepassing Zijnde Wetgeving, de Overeenkomst of een Bijbehorend Document, zoals van toepassing. In geval IBM een Zakenpartner van Klant is, zullen IBM en Klant Gezondheidsgegevens uitsluitend vrijgeven overeenkomstig de bepalingen van een daarop van toepassing zijnde Zakenpartner Overeenkomst tussen partijen.

IBM werkt met een formeel toegangsbesturingsproces voor interne gebruikers waarbij de toegang formeel wordt aangevraagd, na identiteitscontrole wordt goedgekeurd en wordt verleend op basis van noodzaak om op de hoogte te zijn van de informatie ("need to know"), volgens het beginsel dat alleen strikt noodzakelijke rechten worden toegekend. De toegang tot content van Klant blijft beperkt tot actieve gebruikers en actieve gebruikersaccounts. IBM werkt met een formeel proces voor periodieke controle op de verlening van de interne toegang van actieve gebruikersaccounts.

IBM werkt met een veilige authenticatieprotocollen voor gebruikers, zoals het toewijzen van unieke identificaties en sterke wachtwoorden aan actieve gebruikersaccounts op systemen die worden gebruikt voor het verlenen van services aan Klant, overeenkomstig het bedrijfsbeleid en de bedrijfsstandaarden inzake beveiliging;

a. Wachtwoorden zijn nooit door de leverancier aangeleverde standaardwachtwoorden en worden altijd bewaard op een locatie en/of in een indeling die geen gevaar oplevert voor de beveiliging van de gegevens die door die wachtwoorden worden beschermd.

b. De wachtwoorden moeten bij weergave of afdruk gemaskeerd, onderdrukt of anderszins onzichtbaar gemaakt worden, zodat onbevoegden niet in staat zijn om ze waar te nemen of nadien terug te halen. Wachtwoorden mogen bij het invoeren niet worden geregistreerd of vastgelegd. Gebruikerswachtwoorden mogen niet worden opgeslagen in de vorm van gewone tekst.

c. Wachtwoorden voor elke technologie waaruit de IBM SaaS is opgebouwd, moeten zodanig worden gekozen dat ze een zo gering mogelijk risico opleveren geassocieerd te worden met bekende kwetsbaarheden inzake wachtwoordlengte, en moeten worden gedocumenteerd.

d. Indien het gebruik van interne, gemachtigde, gemeenschappelijke functionele ID's om operationele redenen noodzakelijk is, werkt IBM, teneinde de individuele verantwoordelijkheid te onderhouden, met gemeenschappelijke, functionele en/of Systeem ID's waarvoor het uitchecken van wachtwoorden verplicht is.

Op alle systemen en applicaties die worden gebruikt voor de opslag van Content van Klant wordt er gewerkt met inactiviteitstimeouts.

Indien nodig zal er, op verzoek van Klant en na formele goedkeuring van IBM, toegang op afstand tot stand worden gebracht tot het netwerk, de systemen en de applicaties van IBM die worden gebruikt voor de opslag van Content van Klant, en al dergelijke verbindingen op afstand zullen worden beveiligd met behulp van sterke authenticatie- en encryptieprotocollen. Alle activiteiten met toegang op afstand worden geregistreerd en gemonitord.

Voor zover het voor het leveren van de IBM SaaS noodzakelijk is dat IBM zich op afstand toegang verschaft tot systemen die zich binnen de interne netwerken van Klant bevinden, wordt al dergelijke toegang op afstand uitsluitend uitgevoerd met behulp van systemen en protocollen voor veilige toegang op afstand en met behulp van door Klant aan IBM verstrekte toegangslegitimatiegegevens. Toegang op afstand tot het netwerk van Klant wordt uitsluitend tot stand gebracht op verzoek van IBM en na goedkeuring van Klant, en overeenkomstige het op dat moment geldende beleid van Klant, hetwelk vooraf aan IBM beschikbaar wordt gesteld. Voor het gebruik van de interne netwerken van Klant door IBM geldt het IT gebruiks- en beveiligingsbeleid van Klant, hetwelk vooraf aan IBM beschikbaar wordt gesteld.

IBM heeft scheiding van verantwoordelijkheden ingevoerd voor beveiligingsbeheer, toegangscontrole en onderzoek naar inbreuk op de beveiliging.

De Klant-specifieke opslag, hosting en verwerking van content van Klant vindt gescheiden van die van andere door IBM bediende klanten plaats. In gevallen waarin Klant toestemming heeft gegeven voor een gemeenschappelijk werkgebied voor de opslag, hosting of verwerking, werkt IBM met procedures en voorzorgsmaatregelen die stroken met de vereisten zoals vastgelegd in deze SBCA, bedoeld om onbevoegde bekendmaking van dergelijke content van Klant te voorkómen.

IBM hanteert 'clean desk'- en 'leeg scherm'-beleid om te waarborgen dat content van Klant nooit onbewaakt achterblijft op een openbaar toegankelijke plaats.

3. Overdracht en versleuteling

Bij het verzenden van content van Klant (via fax, e-mail, koerier, etc.) neemt IBM passende voorzorgsmaatregelen om te garanderen dat de juiste contactgegevens van de ontvanger worden gebruikt en maakt IBM vooraf afspraken met de beoogde ontvanger om de ontvangst van dergelijke informatie te beveiligen.

IBM werkt in verband met de verwerking van content van Klant, waaronder begrepen de overdracht, communicatie, toegang op afstand en opslag (met inbegrip van backup opslag) van content van Klant, te allen tijde met passende vormen van versleuteling en zal er zorg voor dragen dat IBM Personeel dit eveneens doet. Bijvoorbeeld: IBM zal, met behulp van geschikte versleuteling volgens branchestandaard, zorg dragen voor de versleuteling van alle records en bestanden met content van Klant:

a. opgeslagen op IBM laptops, draagbare apparatuur of draagbare elektronische media, met inbegrip van backup tapes onderweg naar een externe opslaglocatie;

b. door IBM opgeslagen of vervoerd buiten de fysiek beveiligde burelen en terreinen van Klant of IBM, met uitzondering van afgedrukte papieren documenten;

c. tijdens het vervoer over openbare netwerken door IBM;

d. tijdens de overdracht van de systemen van IBM naar Klant;

e. tijdens de draadloze overdracht door IBM; en

f. door IBM opgeslagen op servers en databases.

4. Netwerkbeveiliging

IBM werkt met redelijk recente versies van systeembeveiligingssoftware zoals firewalls, proxy's, webapplicatiefirewalls en interfaces. Dergelijke software moet zijn uitgerust met bescherming tegen malware en met redelijk recente patches en virusdefinities. Overeenkomstig het bedrijfsbeleid is er, waar technisch haalbaar, antivirussoftware geïnstalleerd op werkstations, servers en verwante endpoints, en

wordt de software overeenkomstig het bedrijfsbeleid beheerd met interne oplossingen voor systeembeheer.

IBM monitort de IBM SaaS teneinde beveiligingsincidenten in een zo vroeg mogelijk stadium te detecteren en te identificeren. IBM zal, als minimum, inbraakdetectietools en preventie-, monitoring- en reactieprocessen volgens de branchestandaard onderhouden, op een wijze die geschikt is voor de detectie van zowel interne als externe kwetsbaarheden en risico's die zouden kunnen leiden tot onbevoegde onthulling, misbruik, wijziging of vernietiging van content van Klant of informatiesystemen die worden gebruikt voor het verlenen van services aan Klant.

IBM is geabonneerd op inlichtingendiensten inzake kwetsbaarheden (vulnerability intelligence services) of op informatiebeveiligingswaarschuwingen en andere relevante bronnen die actuele informatie verschaffen over kwetsbaarheden van systemen. IBM voert geregeld kwetsbaarheidsbeoordelingen en -verbeteringen van zijn netwerk uit.

IBM monitort de IBM SaaS teneinde Beveiligingsincidenten in te detecteren, te identificeren, onder controle te houden en op te lossen.

IBM valideert de beschikbaarheid, integriteit en effectiviteit van de netwerkbeveiligingsinfrastructuur waarop de IBM SaaS beschikbaar wordt gesteld, via de IBMreleasemanagementprocessen.

5. Afhandeling en kennisgeving van incidenten

De teams van IBM Watson Health werken samen met het IBM Cybersecurity Incident Response Team, een mondiaal team dat de ontvangst, het onderzoek en de interne coördinatie van beveiligingsincidenten met betrekking tot IBM-aanbiedingen op zich neemt, teneinde de preventieve maatregelen te nemen die noodzakelijk zijn voor het beperken van software-gerelateerde beveiligingsproblemen. Een "Beveiligingsincident" is een geval van geslaagde onbevoegde toegang, gebruik, openbaarmaking, wijziging of verstoring van de werking van, of gegevens in, een informatiesysteem dat door IBM wordt gebruikt voor het leveren van de IBM SaaS. Indien er een Beveiligingsincident wordt ontdekt (via routinematige scans, alerts, drempel-events etc.), zal IBM Klant waarschuwen en informeren:

a. omtrent elk bevestigd Beveiligingsincident waarbij content van Klant betrokken is, en wel zo spoedig als haalbaar is, maar in geen geval later dan 2 werkdagen na het onderzoeken en bevestigen van het desbetreffende Beveiligingsincident;

b. onmiddellijk na elk verzoek om toegang tot, of informatie over, content van Klant vanwege enige overheidsfunctionaris (met inbegrip van een enige autoriteit voor gegevensbescherming of wetshandhavingsinstantie), tenzij dit van rechtswege of op grond van een dwangbevel verboden is; en

c. behoudens zoals toegestaan in het artikel Toegangsbesturing van deze SBCA, voorafgaand aan enige openbaarmaking of overdracht van, of verlening van toegang tot, content van Klant aan een derde.

6. Logboekregistratie

IBM onderhoudt naar redelijkheid, overeenkomstig het beleid en de werkwijzen van IBM en de algemeen gangbare werkwijzen binnen de sector, monitoring van systemen op onbevoegd gebruik van, of onbevoegde toegang tot, Verwerkte Gegevens van Klant. Elke schending van het aanmeldingsbeleid of de toegangsbesturing en elke poging daartoe wordt geregistreerd.

IBM houdt gegevens bij omtrent alle toegangsverzoeken en registreert alle toegangsactiviteiten voor alle systemen die worden gebruikt voor de opslag, toegang, verwerking en transmissie van Klantgegevens en Gezondheidsgegevens en bewaart deze gegevens gedurende de door HIPAA en andere Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens voorgeschreven termijn.

De logboeken en rapporten omvatten ten minste: (i) alle aanmeldingspogingen, al dan niet geslaagd, met inbegrip van identificatiegegevens naar redelijkheid; (ii) alle wijzigingen in systeem- en netwerkconfiguraties, met inbegrip van de installatie van applicaties, wijzigingen in het gebruikersbeheer en aanpassingen in de toegangsmachtigingen voor bestanden; (iii) toegangspogingen tot resources, al dan niet geslaagd, met inbegrip van pogingen om toegang te krijgen tot enig bestand, netwerkshare, logboek of welke andere resource dan ook; en (iv) downloads van gegevens, met inbegrip van het contenttype van de desbetreffende gegevens en het voor de download in kwestie gebruikte toegangsprotocol.

7. Softwareapplicatieontwikkeling en wijzigingsbeheer

IBM hanteert bij het ontwikkelen en coderen van applicaties veilige werkwijzen waarmee de integriteit van productieapplicaties en de bijbehorende broncode wordt beschermd tegen onbevoegde en niet-geteste wijzigingen.

Wat betreft wijzigingsbeheer volgt IBM een proces dat bestaat uit: (a) de registratie en formele goedkeuring van wijzigingen, alsmede procedures voor het ongedaan maken van wijzigingen; en (b) passende tests van dergelijke wijzigingen, met inbegrip van gebruikersacceptatietests waar dit passend wordt geacht, alsmede beveiligingstests.

IBM volgt een patch-beheerproces dat bestaat uit het testen van patches alvorens deze worden geïnstalleerd op systemen waarop content van Klant wordt opgeslagen, benaderd of overgebracht, of op systemen die worden gebruikt voor het verlenen van Services, met inbegrip van IBM SaaS, aan Klant.

IBM verlangt van zijn systeembeheerders dat zij volledige, nauwkeurige en actuele informatie bijhouden betreffende de configuratie van alle informatiesystemen waarop content van Klant wordt opgeslagen, benaderd of overgebracht.

8. Fysieke beveiliging en beveiliging van omgeving

Het IBM Watson Health Core-platform wordt geïmplementeerd in de gegevensinfrastructuur van IBM SoftLayer. IBM SoftLayer onderhoudt fysieke en omgevingsgerichte beveiliging, toegangsbesturing, controles en processen teneinde de gegevens van Klant te beschermen tegen inbreuk of beïnvloeding door personen, vanuit de omgeving of met behulp van techniek.

De algemene toegang tot de gebouwen waarin de IBM SaaS wordt gehost, wordt gecontroleerd met behulp van een kaarttoegangssysteem. Overal op de vestigingen zijn er monitoringcamera's geïnstalleerd waarvan de beelden door beveiligingspersoneel worden gemonitord. Bepaalde toegangsdeuren zijn van alarm voorzien en dit alarm wordt gemonitord door beveiligingspersoneel.

De toegang tot gecontroleerde zones wordt beperkt met behulp van kaarttoegangssystemen en/of aanvullende biometrische controle. Alle personen zonder geautoriseerde toegang tot de gecontroleerde zone moeten zich aanmelden en moeten worden begeleid door een persoon met goedgekeurde toegang tot de gecontroleerde zone. Alle nooduitgangen van gecontroleerde zones zijn van alarm voorzien en dit alarm wordt gemonitord door beveiligingspersoneel. De werking van de alarms wordt periodiek gecontroleerd en gedocumenteerd, en de desbetreffende documentatie wordt bewaard. De toegangsrechten tot gecontroleerde zones worden elke drie maanden volledig opnieuw beoordeeld. Bij beëindiging van het dienstverband wordt de toegang tot gecontroleerde zones ingetrokken.

De gebouwen worden tegen omgevingsfactoren zoals brand, overstroming en hitte beschermd met behulp van brandalarms, brandblusapparatuur, rookmelders en brandonderdrukkings- en -blussystemen. De gebouwen worden tegen stroomstoringen beschermd met behulp van UPS-systemen (Uninterruptible Power Supply) en noodaggregaten, welke geregeld worden onderhouden en getest.

Informatie en rapporten omtrent de naleving van deze werkwijzen door IBM SoftLayer is te vinden op: http://www.softlayer.com/compliance.

9. Continuïteit van de bedrijfsvoering

IBM werkt met bedrijfscontinuïteits- en calamiteitenplannen die bedoeld zijn om een serviceniveau te onderhouden dat strookt met zijn verplichtingen onder de Overeenkomst. Deze bedrijfscontinuïteits- en calamiteitenplannen worden van tijd tot tijd bijgewerkt en getest (ten minste eens per jaar). IBM implementeert alle wijzigingen in de bedrijfscontinuïteits- en calamiteitenplannen die naar redelijkheid noodzakelijk zijn om aan de algemeen gangbare werkwijzen binnen de branche te blijven voldoen, in elk geval zonder de IBM SaaS of de bij Klant in gebruik zijnde productieomgeving onredelijk te verstoren.

In geval van een calamiteit als gevolg waarvan de IBM SaaS niet meer beschikbaar is voor Klant, zal IBM Klant onverwijld inlichten en zal IBM het bedrijfscontinuïteits- en/of calamiteitenplan in werking stellen. Wanneer er een calamiteit wordt afgekondigd, is de doelstelling inzake bedrijfscontinuïteit van de IBM SaaS dat de toegang van Klant tot de IBM SaaS als volgt wordt hersteld: in geval van uitval ("outage") geldt er een Recovery Time Objective (RTO) om de productieomgeving van IBM Watson Health binnen 36 uur na het afkondigen van de calamiteit te herstellen. Als Recovery Point Objective (RPO) geldt dat er niet meer dan 24 uur aan content van Klant binnen de productieomgeving verloren gaat. Voor specifieke Watson Health-oplossingen kunnen de doelstellingen inzake bedrijfscontinuïteit hiervan afwijken.

IBM's aanpak van disaster recovery bestaat uit meerdere datacenters in geografisch ver van elkaar af gelegen gebieden.

Alle datacenters van IBM SoftLayer werken met meerdere elektriciteitsingangen, glasvezelverbindingen, noodaggregaten en backupbatterijen. Bij de bouw ervan is er gewerkt met toonaangevende hardware en apparatuur die de hoogste mate van performance, betrouwbaarheid en interoperabiliteit biedt. Elk onderdeel van het datacenter, waaronder bijvoorbeeld redundante n+1 voedings- en koelingsapparatuur, worden geïnspecteerd om de stabiliteit binnen de datacenters te waarborgen.

10. Naleving

IBM's werkwijzen inzake beveiliging zijn gebaseerd op ISO 27001-27002. Deze werkwijzen bieden controlestructuren voor onder meer Risicoanalyse, Fysieke beveiliging, Calamiteitenplannen, Onderzoek, Informatiebescherming, Educatie, Gegevensbescherming en Bedrijfsvoering.

IBM controleert of de activiteiten in het kader van beveiliging en privacy voldoen aan IBM's werkwijzen inzake beveiliging.

IBM voldoet binnen de In-Scope Landen aan de Op IBM Van Toepassing Zijnde Wetgeving Inzake Persoonsgegevens.

De juiste behandeling van vertrouwelijke informatie van Klant wordt tevens verplicht gesteld onder IBM's Zakelijke Gedragsregels (Business Conduct Guidelines). Alle werknemers dienen deze Zakelijke Gedragsregels jaarlijks door te nemen en dienen officieel te verklaren dit gedaan te hebben.

11. Diversen

IBM garandeert dat al zijn overeenkomsten met subcontractanten en/of derden die betrokken zijn bij de levering van de IBM SaaS, bepalingen bevatten die de content van Klant ten minste dezelfde mate van bescherming bieden als de bepalingen in deze SBCA en elk van toepassing zijnd Bijbehorend Document, elk voor zover de desbetreffende bepalingen van toepassing zijn op de door de subcontractant en/of derde in kwestie verleende services.