IBM Watson Health Core

Bruksbetingelsene ("Bruksbetingelsene" eller "ToU") består av denne IBM Bruksbetingelser – Betingelser for et bestemt IBM SaaS-tilbud ("Betingelser for et bestemt IBM SaaS-tilbud") og dokumentet med tittelen IBM Bruksbetingelser – Generelle betingelser ("Generelle betingelser") som er tilgjengelig på følgende URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Hvis det oppstår motstrid, gjelder Betingelser for et bestemt IBM SaaS-tilbud foran de Generelle betingelsene. Kunden aksepterer Bruksbetingelsene ved å bestille, åpne eller bruke IBM SaaS.

Bruksbetingelsene er underlagt IBM International Passport Advantage Agreement, IBM International Passport Advantage Express Agreement eller IBM International Agreement for Selected IBM SaaS Offerings, avhengig av hva som er aktuelt, ("Avtalen"), som sammen med Bruksbetingelsene utgjør den fullstendige avtalen.

1. IBM SaaS

Følgende IBM SaaS-løsninger er dekket av disse Betingelsene for et bestemt IBM SaaS-tilbud:

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

2. Målenheter for omkostninger

IBM SaaS selges under en av følgende målenhet(er) for omkostninger som spesifisert i Transaksjonsdokumentet:

a. **Tilgang** (Access) er en målenhet for anskaffelse av IBM SaaS. En Tilgang gir rett til å bruke IBM SaaS. Kunden må anskaffe en enkelt Tilgang-rettighet for å kunne bruke IBM SaaS i måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

b. **Individ** (Individual) er en målenhet for anskaffelse av IBM SaaS. Et Individ er en enkelt ting eller en enkelt person. Det må anskaffes tilstrekkelig antall rettigheter for å dekke hvert Individ som behandles eller administreres av IBM SaaS i løpet av måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

   For denne IBM SaaS-løsningen er et Individ en person, enhet eller mobilapplikasjon som IBM SaaS administrerer data for.

c. **Forekomst** (Instance) er en målenhet for anskaffelse av IBM SaaS. En Forekomst er tilgang til en bestemt konfigurasjon av IBM SaaS. Det må anskaffes tilstrekkelig antall rettigheter for hver Forekomst av IBM SaaS som gjøres tilgjengelig for tilgang og bruk i løpet av måleperioden som er oppgitt i Kundens Kjøpsbevis (PoE) eller Transaksjonsdokument.

3. Priser og fakturering

Beløpet som skal betales for IBM SaaS, er oppgitt i et Transaksjonsdokument.

3.1 Pris for del av måned

Prisen for en del av en måned som fremkommer i Transaksjonsdokumentet, kan være en forholdsmessig beregnet pris.

3.2 Priser for ekstra volum

Hvis Kundens faktiske bruk av IBM SaaS i måleperioden overstiger rettighetene som fremkommer i Kundens kjøpsbevis (PoE), blir Kunden fakturert for slikt ekstra volum i samsvar med det som er oppgitt i Transaksjonsdokumentet.

4. Alternativer for avtaleperiode og fornyelse

Avtaleperioden for IBM SaaS starter den dagen IBM varsler Kunden om at Kunden har tilgang til Pilot-driftsmiljøet i IBM SaaS, som beskrevet i Bestillingsdokumentet. Abonnementsperioden for Individ-rettigheter starter når IBM varsler Kunden om at Kunden har tilgang til driftsmiljøet for produksjon. Bestillingsdokumentet angir om IBM SaaS-abonnementet fornyes automatisk, løper videre eller opphører ved slutten av abonnementsperioden.

Ved automatisk fornyelse er det slik at hvis Kunden ikke minst 90 dager før utløpsdatoen for avtaleperioden sender et skriftlig varsel om at Kunden ikke ønsker fornyelse, blir IBM SaaS-abonnementet fornyet automatisk for avtaleperioden som er angitt i Kjøpsbeviset.

Ved fortløpende bruk vil IBM SaaS fortsette å være tilgjengelig på månedsbasis til Kunden sender et 90 dagers skriftlig forhåndsvarsel om oppsigelse. IBM SaaS fortsetter å være tilgjengelig til slutten av kalendermåneden etter en slik periode på 90 dager.

5. Teknisk støtte

IBM vil gjøre IBM Software as a Service Support Handbook tilgjengelig for Kunden, og denne håndboken inneholder kontaktinformasjon for teknisk støtte, vedlikeholdstider samt informasjon om prosesser og annen informasjon. Kontaktinformasjon for teknisk støtte og andre detaljer om støtte finnes i IBM SaaS Support Handbook: https://support.ibmcloud.com.

Teknisk støtte og behandling av enkle konfigureringsforespørsler vedrørende IBM SaaS leveres elektronisk. Teknisk støtte tilbys sammen med IBM SaaS og er ikke tilgjengelig som en egen løsning.

Ingen personopplysninger, inkludert beskyttede helseopplysninger og sensitive personopplysninger skal tas med i dokumentasjonen eller informasjonen når en problemhendelse rapporteres.

6. Definisjoner

API er et programmeringsgrensesnitt, som er et sett med rutiner, protokoller og verktøy for bygging av programvareapplikasjoner. APIer oppgir hvordan programvarekomponenter skal virke sammen, og APIer brukes ved programmering av komponenter i et grafisk brukergrensesnitt (GUI).

Autorisert administrator er en ansatt hos Kunden, en kontraktør godkjent av Kunden, en person eller en gruppe som er ansvarlig for å administrere vedlikehold og pålitelig drift av plattformen. Ansvarsområder kan omfatte konfigurering, støtte og bruker- og kontoadministrasjon. Administratoren kan også være en klinisk forsker som er ansvarlig for å sette opp en studie i Watson Health-systemet.

Autorisert individ er en autentisert person, mobilapplikasjon eller enhet som er gitt tilgangsrettigheter for å sende data til Watson Health Core. Dette kan omfatte Kunden eller Kundens studiedeltakere, kunder eller pasienter.

Behandlede data er data, konfidensiell eller rettslig beskyttet informasjon eller materiale, inkludert Helsedata og Personopplysninger, som behandles av IBM i henhold til Avtalen, et Tilhørende dokument, et Bestillingsdokument og/eller en Tjenestebeskrivelse.

Gjeldende lovgivning er lover, vedtekter eller lovbestemmelser, regler, forskrifter, direktiver, påbud, forordninger eller andre krav utstedt av en offentlig myndighet, eller generelt anerkjente bransjestandarder som gjelder for oppfyllelsen av disse Bruksbetingelsene.

Gjeldende lovgivning for IBM om personvern er Lovgivningen om personvern som gjelder for oppfyllelsen av IBMs forpliktelser i henhold til Avtalen, Tilhørende dokumenter, Bestillingsdokumenter og Tjenestebeskrivelser mellom Partene.

Gjeldende lovgivning for Kunden om personvern er Lovgivningen om personvern som gjelder for oppfyllelsen av Kundens forpliktelser i henhold til Avtalen, Tilhørende dokumenter, Bestillingsdokumenter og Tjenestebeskrivelser mellom Partene.

Helsedata er data eller informasjon, inkludert bilder, som er helserelaterte Personopplysninger.

Helsedataklargjort er, for IBM SaaS, IBM SaaS' evne til å overholde gjeldende standarder, lovgivning og forskrifter for sikkerhet og personvern for Helsedata i Omfattede jurisdiksjoner, inkludert implementeringsspesifikasjonene som fremgår i Part 164, Subpart A og C, i forskrifter som implementerer HIPAA (endret av HITECH) samt annen Gjeldende lovgivning vedrørende Helsedata, men betyr ikke at IBM fungerer i egenskap av Forretningspartner eller Behandlingsansvarlig.

HIPAA er USAs Health Insurance Portability and Accountability Act fra 1996, med endringer, inkludert av Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act fra 2009 ("HITECH"), enkelte forskrifter kunngjort under HIPAA av United States Department of Health and Human Services i 45 C.F.R. Part 160 og 164, samt enkelte forskrifter kunngjort i henhold til HITECH.

IBMs personell er (a) IBM, IBMs Tilknyttede selskaper og IBMs underleverandører, og for hver av de foregående, deres ansatte; og (b) alle tredjepartsleverandører; i hvert tilfelle personell som utfører

tjenester på vegne av IBM i henhold til Avtalen og aktuelle Tilhørende dokumenter, eller som IBM på annen måte gir tilgang til Kundens Personopplysninger.

Kundedata er alle data som legges inn i IBM SaaS av eller for Kunden, enten det er Kundens egne data eller data som er lagt inn av eller på vegne av Kundens kunde eller en tredjepart, og inkludert data fra en tredjeparts helseregistreringsenhet.

Lovgivning om personvern er all gjeldende lovgivning vedrørende beskyttelse av personopplysninger, personvern eller sikkerhet.

Omfattede land er de 28 medlemslandene i Den europeiske union og Sveits, samt land som IBM fra tid til annen kan tilføye til denne listen.

Personopplysninger er informasjon på ethvert medium eller i ethvert format, inkludert elektroniske registreringer og papirregistreringer, som er knyttet til en identifisert eller identifiserbar person, der en "identifiserbar person" er en person som kan identifiseres, direkte eller indirekte, spesielt ved henvisning til et identifikasjonsnummer eller til en eller flere faktorer som er spesifikke for personens fysiske, fysiologiske, mentale, økonomiske, kulturelle eller sosiale identitet.

Prosess eller ord som **behandling** (med stor forbokstav eller ikke) er enhver operasjon eller ethvert sett med operasjoner som utføres på data, enten det skjer automatisk eller på annen måte, som innsamling, registrering, organisering, lagring, tilpasning eller endring, henting, konsultasjon, bruk, avgivelse ved overføring, distribusjon eller annen form for tilgjengeliggjøring, justering eller kombinering, blokkering, sletting eller tilintetgjøring.

Registrert er en identifisert eller identifiserbar person som Personopplysninger er knyttet til.

Sikkerhetshendelse har betydningen som fremgår i Vedlegget for sikkerhet og driftskontinuitet.

Utvalgt datasenter er et datasenter som er oppgitt som primært datasenter og datasenter for katastrofehåndtering i Transaksjonsdokumentet, og som kjører Kundens forekomst av IBM SaaS, hvis aktuelt.

7. Kontoadministrasjon

IBM SaaS er kun tilgjengelig for Kundens autoriserte brukere ("**Autoriserte administratorer**" eller "**Autoriserte individer**"). Kunden skal styre hvilke kontoer som autoriseres for tilgang til IBM SaaS, som kan omfatte autoriserte applikasjoner, Kundens personale og Kundens tredjeparts tjenesteleverandører og kontraktører, og er alene ansvarlig for å (i) kontrollere alle autoriserte brukere, inkludert, uten begrensning, å verifisere identiteten til enhver autorisert bruker; og (ii) sørge for at bare autoriserte brukere får tilgang til IBM SaaS.

Autoriserte individer som er Kundens kunder, pasienter eller studiedeltakere, kan få tilgang kun for å laste opp data til IBM SaaS, og i slike tilfeller har slike Autoriserte individer ingen annen tilgang til IBM SaaS.

8. Personvern

8.1 Generelle krav

Når det gjelder forholdet mellom partene, er Kunden eneste behandlingsansvarlige for alle Kundens Personopplysninger, og Kunden utpeker IBM som databehandler. I henhold til Gjeldende lovgivning om personvern har Kunden rett til å instruere IBM i forbindelse med IBMs behandling av Kundens Personopplysninger.

I den utstrekning IBM behandler Kundens Personopplysninger, skal IBM

a. overholde all Gjeldende lovgivning for IBM om personvern; og

b. ikke sammenblande Kundens Personopplysninger med data fra andre kilder, unntatt

- slik det er nødvendig for å levere IBM SaaS, og ikke for noen andre formål med mindre Kunden spesifikt har instruert IBM om å gjøre det; eller
- i henhold til betingelsene i disse Bruksbetingelsene og Vedlegget for sikkerhet og driftskontinuitet.

I den utstrekning IBM behandler Kundens Personopplysninger, skal Kunden

a. overholde all Gjeldende lovgivning for Kunden om personvern;

b. være ansvarlig for all kommunikasjon mellom Kunden og Kundens Tilknyttede selskaper, pasienter, sluttbrukere, Registrerte og/eller andre av Kundens tredjeparter;

c. inngå databehandlingsavtaler med Kundens behandlingsansvarlige, som kreves for å tillate at IBM som behandler og IBMs underbehandlere behandler Kundens Personopplysninger; og

d. være eneste kontaktpunkt for IBM og alene være ansvarlig for intern koordinering, gjennomgang og overlevering av instruksjoner eller forespørsler fra Kundens Tilknyttede selskaper som er andre behandlingsansvarlige, til IBM. IBM skal fritas for sin forpliktelse til å informere eller varsle et av Kundens Tilknyttede selskaper som fungerer som en behandlingsansvarlig, når IBM har overlevert slik informasjon eller varsel til Kunden. IBM har rett til å avslå å motta instruksjoner direkte fra et av Kundens Tilknyttede selskaper som fungerer som en behandlingsansvarlig som ikke er Kunden.

Det kan ikke pålegges noen av partene å handle på en måte som er i strid med den aktuelle partens Gjeldende lovgivning om personvern.

8.2 Rettigheter til Kundedata

Kunden bekrefter og garanterer at Kunden (a) eier dataene Kunden vil legge inn i IBM SaaS, eller (b) har innhentet, og er ansvarlig for å opprettholde, alle nødvendige rettigheter, tillatelser, godkjennelser og autorisasjoner for å gi IBM rettigheter for tilgang, bruk og avgivelse av Kundedataene i samsvar med betingelsene som fremkommer i disse Bruksbetingelsene eller Avtalen, eller slik det på annen måte er nødvendig for at IBM skal kunne levere IBM SaaS. Kunden bekrefter og garanterer videre at Kundedataene kun skal være (a) knyttet til personer som er bosatt i USA, og da kun skal legges inn i IBM SaaS ved USAs datasenter, eller (b) knyttet til personer som er bosatt i ett eller flere Omfattede land, og da kun skal legges inn i IBM SaaS ved det eller de Utvalgte datasentrene.

8.3 Datatjenester og forpliktelser

a. Kunden bekrefter at Kunden kun skal utføre analyser eller be IBM om å utføre analyser på Kundedataene i forbindelse med aktiviteter som utgjør Kundens helsetjenesteoperasjoner ("health care operations") eller forskning ("research"), slik disse begrepene er definert i HIPAA, og/eller liknende betegnelser i annen Gjeldende lovgivning om personvern, og at Kunden skal bruke Kundedataene eller pålegge IBM å bruke Kundedataene kun i samsvar med alle relevante krav (f.eks. beslutninger fra en komité for medisinsk og helsefaglig forskningsetikk, eller kravsfrafall der det er nødvendig) i lovgivning nevnt ovenfor og annen Gjeldende lovgivning for Kunden om personvern.

b. Kunden er alene ansvarlig for å innhente enhver av og alle registreringer, tillatelser, autorisasjoner og godkjennelser som ifølge Gjeldende lovgivning for Kunden i hvert aktuelt Omfattet land, inkludert, uten begrensning, HIPAA og andre gjeldende lover, regler og forskrifter vedrørende personvern og datasikkerhet, kreves for at Kundedataene skal kunne legges inn i IBM SaaS og brukes og avgis som tiltenkt under disse Bruksbetingelsene og Avtalen av Kunden og av IBM og IBMs tillatte underleverandører. IBM har ingen forpliktelser vedrørende overvåking av når slike registreringer, godkjennelser, autorisasjoner og tillatelser er mottatt eller kreves.

c. Kunden er alene ansvarlig for å sørge for at alle Kundedata som legges inn i IBM SaaS, kun er data som gjelder personer bosatt i USA eller i et gjeldende Omfattet land.

d. IBMs støttesentre skal ha personell som er spesialister på HIPAA og annen Gjeldende lovgivning for IBM om personvern fra Omfattede land.

8.4 Sikkerhetstiltak og sikkerhetshendelser

a. IBM skal implementere, vedlikeholde og overholde tekniske og organisasjonsmessige tiltak (inkludert organisasjonsmessige prosesser og prosedyrer, og inkludert bestemte forpliktelser vedrørende sikkerhet som er angitt eller det er henvist til i disse Bruksbetingelsene og SBCA) for å beskytte Kundens Personopplysninger mot uautorisert bruk eller tilgang, tilfeldig tap, skade, endring, tilintetgjøring, tyveri eller uautorisert avgivelse.

b. Hvis IBM blir oppmerksom på en Sikkerhetshendelse (slik en "security incident" er definert i SBCA) som omfatter Kundens Behandlede data, skal IBM informere Kunden i henhold til betingelsene i SBCA og Gjeldende lovgivning for IBM om personvern, og et slikt varsel skal inneholde informasjon om enhver kjent innvirkning på Kunden eller noen Registrerte (om det finnes noen) som er berørt av en slik Sikkerhetshendelse, og om korrigerende tiltak som er utført eller foreslått av IBM.

8.5 Mottak av forespørsler og klager

IBM skal straks varsle Kunden skriftlig og, i den utstrekning det er tillatt ifølge Gjeldende lovgivning for IBM om personvern, ikke senere enn fem (5) arbeidsdager etter at den ansvarlige for personvern i IBM

Watson Health har mottatt en forespørsel, henvendelse eller klage som er mottatt av IBM i tilknytning til Kundens Personopplysninger, fra

a. en Registrert angående Personopplysninger om den Registrerte, som er behandlet av IBM. Kunden skal svare på slike forespørsler fra Registrerte, og IBM skal følge rimelige instruksjoner fra Kunden for å hjelpe Kunden med å svare på slike forespørsler. Hvis det ifølge Gjeldende lovgivning for IBM kreves, kan IBM svare direkte på slike forespørsler, forutsatt at IBM varsler Kunden på forhånd om et slikt svar og i rimelig grad koordinerer med Kunden hvilken form og innhold et slikt svar skal ha, når dette er tillatt ifølge Gjeldende lovgivning for IBM eller mulig på andre måter:

b. en juridisk eller annen ansvarlig myndighet vedrørende IBMs behandling av Kundens Personopplysninger, forutsatt at IBM kan svare på slike forespørsler mottatt fra en offentlig myndighet med en stevning eller liknende juridisk dokument som ber om avgivelse fra IBM, eller slik det på annen måte kreves ifølge Gjeldende lovgivning om personvern, forutsatt at IBM varsler Kunden på forhånd om en slik avgivelse og i rimelig grad koordinerer med Kunden hvilken form og innhold et slikt svar skal ha, når dette er tillatt ifølge lovgivning eller mulig på andre måter.

8.6 Behandling av Kundens Personopplysninger

IBM skal begrense avgivelse av Kundens Personopplysninger til det av IBMs personell som muligens må hjelpe IBM med leveringen av Tjenestene.

IBM skal etterkomme alle rimelige forespørsler fra Kunden som krever at IBM må endre, korrigere, slette eller blokkere Kundens Personopplysninger i henhold til Gjeldende lovgivning.

På forespørsel fra en av Partene vil IBM, Kunden, eller deres Tilknyttede selskaper inngå standardavtaler slik loven krever det, for beskyttelse av Kundens Personopplysninger. Partene aksepterer (og bekrefter at deres respektive Tilknyttede selskaper aksepterer) at slike avtaler skal være underlagt ansvarsbegrensningene i denne Avtalen med henblikk på krav som oppstår mellom Partene. Partene skal samarbeide om å inngå (eller kreve at en Partenes Tilknyttede selskaper inngår) og overholde videre omforente betingelser eller avtaler slik det kan kreves ifølge Gjeldende lovgivning om personvern.

8.7 Retur av Kundens Personopplysninger

Ved utløp eller opphør av Avtalen skal IBM, og alt IBMs personell, slutte å bruke eller behandle Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger, og skal etter Kundens eget valg og på forespørsel

a. straks returnere i et format og på et lagringsmedium som Kunden med rimelighet kan be om, all Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger som IBM har lagret elektronisk, og når det er bekreftet mottatt av Kunden, slette, tilintetgjøre eller på annen måte gjøre varig uleselig eller umulig å dechiffrere Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger, inkludert kopier og sikkerhetskopier. IBM kan kreve betaling for kostnader til lagringsmedium og visse aktiviteter som utføres på forespørsel fra Kunden, for eksempel å levere Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger i et bestemt format eller å tilintetgjøre Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger på en bestemt måte; og

b. umiddelbart slette, tilintetgjøre eller på annen måte gjøre varig uleselig eller umulig å dechiffrere Kundens Rettslig beskyttede informasjon og Kundens Personopplysninger, inkludert kopier og sikkerhetskopier.

8.8 BAA-avtale

I den utstrekning det er riktig og nødvendig ifølge HIPAA, skal IBM og Kunden inngå en avtale av typen Business Associate Agreement ("BAA"), som skal regulere IBMs forpliktelser som en forretningspartner (Business Associate) av Kunden i leveringen av IBM SaaS. Uten å begrense IBMs uttrykkelige forpliktelser i henhold til Avtalen og BAA der det er aktuelt, bekrefter og aksepterer Kunden at Kunden er ansvarlig for å fastslå, og overholde, alle krav i Gjeldende lovgivning samt lisensieringskrav som gjelder for Kundens bruk av eller andre aktiviteter knyttet til (inkludert bruk eller andre aktiviteter fra Autoriserte brukeres side) IBM SaaS.

8.9 Tilleggsbetingelser for databehandling for Den europeiske union

Hvis Kunden pålegger IBM å behandle Personopplysninger fra Den europeiske union, skal IBM og Kunden inngå en avtale med tilleggsbetingelser for databehandling (Data Processing Addendum) som inkluderer, der det er aktuelt, EUs standardkontrakt med valgfrie klausuler fjernet.

9. Tilleggsbetingelser for IBM SaaS

9.1 Sikkerhet

Denne IBM SaaS-løsningen følger IBMs retningslinjer for datasikkerhet og personvern for IBM SaaS, som er tilgjengelig på adressen http://www.ibm.com/cloud/data-security, samt tilleggsbetingelsene som fremkommer nedenfor og i Vedlegget for sikkerhet og driftskontinuitet til disse Bruksbetingelsene. Endringer i IBMs retningslinjer for datasikkerhet og personvern vil ikke redusere IBM SaaS-løsningens sikkerhet.

IBM Watson Health Core implementerer sikkerhetspolicyer, standarder og prosesser basert på ISO 27001-rammeverket som nærmere beskrevet i sikkerhetsbeskrivelsen. Løsningen implementerer følgende sikkerhetsfunksjonalitet:

a. Sikre driftssoner

   IBM Watson Health Core implementerer en dyptgående forsvarsstrategi som benytter flere sikkerhetssoner til administrasjon av skyintegreringspunkter, som klargjøring (onboarding) av data og tilpasset applikasjonsutvikling.

b. Kryptering

   Alle Kundedata er kryptert både når de er lagret og ved overføring. Alle data som er under overføring til og fra IBM Watson Health Core, er kryptert. En delt tjeneste sørger for administrasjon av krypteringsnøkler. Kunden er ansvarlig for all nettverkstilkobling og nettverkskvalitet mellom IBM Watson Health Service og Kundens proxyserver.

c. Overvåking av sikkerhetshendelser

   IBM benytter sin Security Intelligence-plattform til administrasjon av sikkerhetsinformasjon og sikkerhetshendelser, loggadministrasjon, hendelsesvurdering, trusseloppdaging og sårbarhetshåndtering.

d. Identitetskontroll

   - Watson Health Core støtter identitetsleverandører med åpen standard for pasient- og brukerpopulasjoner i stor skala, ved bruk av OpenID Connect.
   - For brukerpopulasjoner der IBM er identitetsleverandør, benytter Watson Health Core passende katalogtjenester og identitetsstyringsfunksjonalitet til håndtering av autentisering.

e. Sterk autentisering og rollebasert tilgang

   - Watson Health Core støtter autentisering gjennom SAML som mekanisme for Kunder som ønsker å integrere sin tjeneste for enkeltpålogging (SSO) eller katalogtjeneste.
   - Watson Health Core benytter en løsning for tilgangsstyring og tilhørende komponenter til administrasjon av sikkerhetspolicyer, der dette er aktuelt.
   - Watson Health Core støtter programvarebasert tofaktorautentisering.
   - Watson Health Core har grunnleggende rollebasert tilgangskontroll der det kreves, og Watson Health Core støtter konfigurering av studier, brukerprofiler, roller og brukergrupper gjennom programmeringsgrensesnitt ("API" eller "APIer") som aktiverer rollebasert tilgang.

9.2 Informasjonskapsler (cookies)

Kunden er innforstått med og aksepterer at IBM som en del av normal drift og støtte for IBM SaaS kan samle inn personopplysninger fra Kunden (Kundens ansatte og kontraktører) knyttet til bruken av IBM SaaS, gjennom sporing og andre typer teknologi. IBM gjør dette for å samle inn bruksstatistikk og informasjon om hvor effektivt IBM SaaS er, med formål å forbedre brukeropplevelsen og/eller tilpasse interaksjonen med Kunden. Kunden bekrefter at Kunden skal innhente eller har innhentet samtykke til at IBM kan behandle de innsamlede personopplysningene for formålet beskrevet ovenfor, innenfor IBM, andre IBM-selskaper og deres underleverandører, der IBM og IBMs underleverandører driver virksomhet, i henhold til gjeldende lovgivning. IBM skal etterkomme forespørsler fra Kundens ansatte og kontraktører om tilgang til og oppdatering, retting eller sletting av deres innsamlede personopplysninger.

9.3 "Derived Benefit Locations"

Der det er aktuelt, er skatter og avgifter basert på steder der Kunden oppgir å dra fordel av IBM SaaS. IBM skal benytte skatter og avgifter basert på forretningsadressen som er oppgitt ved bestilling av en IBM SaaS-løsning, som primært fordelssted (primary benefit location), med mindre Kunden oppgir annen

informasjon til IBM. Kunden er ansvarlig for å holde slik informasjon oppdatert, og informere IBM om eventuelle endringer.

9.4 Fortløpende levering

Kunden har rett til funksjonalitet og forbedringer som lages til løsningen, og som distribueres av IBM ifølge en modell for fortløpende levering.

9.5 Sikkerhetskopiering og gjenoppretting

IBM Watson Health Core sørger for sikkerhetskopiering av Kundedata i produksjonsmiljøet (inkludert Data Lake- og Data Reservoir-datalageret) til sist kjente fungerende status, med formål å gjenopprette tjenesten i tilfelle en systemfeil.

9.6 Høy tilgjengelighet

IBM Watson Health Core-komponentene i produksjonsmiljøet er implementert i konfigurasjoner for høy tilgjengelighet, med databaseservere i klynger for redundans, som gir fordeling av arbeidsbelastningen og eliminerer enkeltpunktfeil.

9.7 Katastrofehåndtering

IBMs tilnærming til katastrofehåndtering består i flere datasentre i spredtliggende geografiske områder for å oppnå følgende mål for driftskontinuitet for produksjonsmiljøet:

- Mål for gjenopprettingstid (RTO) – innen 36 timer etter en katastrofeerklæring
- Mål for gjenopprettingspunkt (RPO) – maksimalt 24-timers tap av Kundens innhold

9.8 Verktøy for målinger

IBM SaaS bruker en syntetisk overvåkingsløsning til overvåking, måling og rapportering av tilgjengelighet eller nedetid mot forpliktende servicenivåer. Denne løsningen simulerer og sporer brukerrespons og brukeropplevelse på globalt nivå – både for statisk tilgjengelighet og for transaksjoner.

IBM SaaS bruker også et internt overvåkingssystem for måleverdier, hendelser og varsler på tvers av hele løsningen.

9.9 Offentlighet

Kunden aksepterer at IBM kan referere til Kunden som abonnent på IBM SaaS i reklame- eller markedsføringsmateriell.

Vedlegg A

1. IBM Watson Health Core

IBM Watson Health Core er en Helsedataklargjort Platform as a Service (PaaS), utviklingsplattform og driftsdelsystem for lagring, kuratering og behandling av Beskyttede helseopplysninger (Protected Health Information (PHI)), slik dette er definert i HIPAA, og andre Helsedata i henhold til Gjeldende lovgivning for IBM om personvern, i et datasenter eid eller kontrollert av IBM. Kunden må anskaffe passende rettigheter til IBM Watson Health Core og IBM Watson Health Core Access for å aktivere funksjonene og funksjonaliteten som er beskrevet nedenfor.

1.1 Driftsmiljøer for Watson Health Core

Watson Health Core-rettigheter omfatter tre Helsedataklargjorte nettskybaserte driftsmiljøer som er utformet for at Kunden skal kunne behandle Helsedata:

- Pilot

  Gir et sandkassemiljø der Kunden kan utvikle og teste applikasjoner som bygges ved hjelp av IBM SaaS. Pilotmiljøet implementerer alle HIPAA-sikkerhetskontroller unntatt katastrofehåndtering, høy tilgjengelighet og sikkerhetskopiering av systemer og registreringer.

- Produksjonsmiljø

  Gir et fullskalamiljø der Kunden kan implementere Helsedata-arbeidsbelastninger. Produksjonsmiljøet er et høyt tilgjengelig, belastningsbalansert miljø og kan failover-overføres til en lokalitet for katastrofehåndtering.

- Katastrofehåndtering

  Gir et speilreplikat av produksjonsmiljøet og er plassert i et eget datasenter.

1.2 Applikasjonsutvikling

IBM Watson Health Core muliggjør applikasjonsutvikling og sikker datainnsamling fra Kundens enheter eller Kundens autoriserte brukeres enheter. APIer gir programgrensesnitt og dokumentasjon som Kundens autoriserte brukere, inkludert Kundens tredjeparts tjenesteleverandører, kan bruke til å utvikle applikasjoner og utveksle data med IBM SaaS. Kunden eller Kundens utvikleres bruk av APIene må skje i overensstemmelse med kravene til utviklere (API Developer Requirements).

- REST-APIer

  Watson Health Core er utstyrt med en serie med REST-APIer og tjenester for Watson Health Core-plattformen. API-funksjonaliteten omfatter, men er ikke begrenset til, mekanismer for tilgang til datalagre, datakurateringstjenester, brukeradministrasjon og revisjonslogger.

- Apple HealthKit og Apple ResearchKit

  Watson Health Core støtter integrering med Apple ResearchKit API-rammeverket for iOS-baserte forskningsstudier, og med Apple HealthKit for registrering av helsedata.

1.3 Datastyring

- Behandling av samtykke

  Watson Health Core gir et rammeverk for registrering av samtykke fra pasienter eller studiedeltakere, og kan på sikker måte lagre en post for samtykke atskilt fra datanyttelasten når personen blir registrert via en av Kundens applikasjoner som er aktivert for samtykke.

- Datamaskering

  Watson Health Core gjør det mulig å atskille navneidentifikatorer fra strukturerte datanyttelaster. Watson Health Core mottar data i nettskyen og gjennom program-APIer. APIene aktiverer atskillelse av pasientens eller personens navneidentifikator fra resten av datanyttelasten, og lagrer den i et separat kryptert datalager. Datanyttelasten får tildelt et anonymisert token som kan brukes i fremtidig sporing av opprinnelse.

1.4 Helsedatatjenester

Watson Health Core utfører innsamling, lagring og synkronisering av data, inkludert Helsedata og Personopplysninger av fremmed opprinnelse, både strukturerte og ustrukturerte data.

- Datainnføring

  Watson Health Core gjør det mulig å innføre data fra pasientapplikasjoner eller enheter gjennom program-APIer. Watson Health Core gir hver av Kundens Autoriserte individer rett til å laste opp inntil 25 MB med data til Health Core hvert år i avtaleperioden. Tjenesten er innrettet for inntil 10 opplastinger per Individ per dag.

- Data Lake-datalager

  Rå Kundedata eller pasientdata lagres i Watson Health Core i ubehandlet form til det er behov for dem til analyse eller modellering.

- Extract Transform Load (ETL)

  Data transformeres til et normalisert format i driftsdelsystemet. En bransjestandardbasert Enterprise Service Bus for helsetjenester muliggjør integrering på tvers av forskjellige av Kundens applikasjoner og protokoller.

- Data Reservoir-datalager

  Når dataene er kuratert, blir de flyttet til Data Reservoir-datalageret. Watson Health Core benytter aspekter av IBM Unified Data Model for Healthcare til normalisering av forretningsmessige og tekniske helsedata til bruk i analyser.

- Hovedindeks for personer

  Watson Health har Master Data Management-verktøy til bruk ved konsolidering av data fra forskjellige kilder for å opprette en LPR-post (Longitudinal Person Record).

2. Valgbare funksjoner

2.1 IBM Watson Health Core Terminology Service

Denne tilleggstjenesten muliggjør dataintegrering og interoperabilitet mellom uensartede helsesystemer, og gir konsistent bruk av klinisk terminologi på tvers av alle Watson Health Cloud-applikasjoner. Denne tjenesten leverer den funksjonelle plattformen for alle oppgaver som involverer terminologi, kodesystemer og strukturert innhold, som følgende:

- opprettelse av nye kodesystemer;
- oversettelse av internasjonale kodesystemer; og
- tilordninger mellom lokale kodelister og internasjonale standarder.

Vedlegg B

IBM leverer følgende servicenivåavtale ("Servicenivåavtale" (SLA)) for IBM SaaS, som angitt i et Kjøpsbevis (PoE). Servicenivåavtalen er ikke en garanti. Servicenivåavtalen er kun tilgjengelig for Kunden og gjelder kun for bruk i produksjonsmiljøer.

1. Tilgjengelighetskrediteringer

Tilgjengelighetsrefusjoner gjelder bare for abonnementspriser for Individ-rettigheter.

Kunden må logge en problempost med Alvorsgrad 1 hos IBMs Help Desk for teknisk støtte innen 24 timer etter at Kunden først ble oppmerksom på en hendelse som påvirket tilgjengeligheten av IBM SaaS. Kunden må i rimelig grad hjelpe IBM med å utføre problemdiagnose og finne en løsning for problemet.

Et krav knyttet til en problempost ved mangel på oppfyllelse av en Servicenivåavtale må sendes senest tre arbeidsdager etter slutten av avtalemåneden. Kompensasjon for et gyldig SLA-krav gis i form av en kreditering mot en fremtidig faktura for IBM SaaS basert på hvor lenge produksjonssystembehandlingen for IBM SaaS ikke har vært tilgjengelig ("Nedetid"). Nedetid måles fra tidspunktet Kunden rapporterer hendelsen til tidspunktet IBM SaaS er gjenopprettet, og omfatter ikke tid i forbindelse med en planlagt eller annonsert nedetid for vedlikehold; årsaker utenfor IBMs kontroll; problemer med Kundens eller en tredjeparts innhold eller teknologi, design eller instruksjoner; systemkonfigurasjoner og plattformer som ikke støttes, eller andre feil fra Kundens side; eller sikkerhetshendelser forårsaket av Kunden eller Kundens testing av sikkerheten. IBM skal benytte høyeste aktuelle kompensasjon basert på kumulativ tilgjengelighet av IBM SaaS i løpet av hver avtalemåned, som vist i tabellen nedenfor. Samlet kompensasjon for en avtalemåned skal ikke overstige 20 prosent av en tolvdel (1/12) av det årlige beløpet Kunden betaler for IBM SaaS.

2. Servicenivåer

Tilgjengelighet av IBM SaaS i løpet av en avtalemåned

Tilgjengelighet i løpet av en avtalemåned	**Kompensasjon (% av månedlig Individ-abonnementspris* for avtalemåneden som kravet gjelder)**
< 99,95 %	10 %
< 99,0 %	20 %

* Hvis IBM SaaS ble kjøpt fra en IBM Business Partner, blir den månedlige abonnementsprisen beregnet basert på den gjeldende listeprisen for IBM SaaS på det aktuelle tidspunktet, gjeldende for avtalemåneden som Kravet gjelder, redusert med 50 %. IBM gir Kunden en direkte tilgjengelig refusjon.

Tilgjengelighet beregnes prosentvis på følgende måte: totalt antall minutter i en avtalemåned, minus totalt antall minutter med Nedetid i en avtalemåned, dividert på totalt antall minutter i avtalemåneden.

Eksempel: 108 minutter samlet Nedetid i en avtalemåned

43.200 minutter i en avtalemåned med 30 dager - 108 minutter med Nedetid = 43.092 minutter _____ 43.200 minutter	= 10 % Tilgjengelighetskreditering for 99,75 % tilgjengelighet i løpet av avtalemåneden

3. Unntak

Denne Servicenivåavtalen gjelder ikke følgende:

- Bortsett fra serverovervåking gjelder Servicenivåavtalen ikke for vertede virtuelle maskiner til støtte for tilpassede eller Kundens applikasjoner.
- Hvis Kunden har misligholdt sine forpliktelser i henhold til gjeldende avtaleforpliktelser.

Vedlegg C

Dette Vedlegget for sikkerhet og driftskontinuitet angir visse av IBMs krav og forpliktelser i forbindelse med IBMs levering av IBM SaaS til Kunden. Kravene og forpliktelsene som er beskrevet i dette punktet, kommer i tillegg til de som er angitt i beskrivelsen av prinsippene for datasikkerhet for IBM SaaS, som er tilgjengelig på adressen http://www.ibm.com/cloud/data-security. Betegnelser med stor forbokstav som ikke er definert her, skal ha betydningen som er angitt i Avtalen eller Bruksbetingelsene.

1. Program for informasjonssikkerhet

IBM har interne sikkerhetspolicyer, standarder og prosesser basert på ISO 27001-rammeverket og kontrollområdene i ISO 27001. I tillegg til IBM Corporate Security Organization-styringsfunksjonene er disse policyene, standardene og prosessene jevnlig underlagt interne revisjoner.

IBM håndhever et program for informasjonssikkerhet med organisasjonsmessige, driftsmessige, administrative, fysiske og tekniske beskyttelsestiltak som styrer behandlingen, lagringen og overføringen av Kundens innhold, og som minst er konsistent med kravene i dette Vedlegget for sikkerhet og driftskontinuitet.

IBM skal, på forespørsel fra Kunden, gi Kunden informasjon om IBM Watson Health-programmet for informasjonssikkerhet, slik at Kunden i rimelig grad kan vurdere programmets fortsatte velegnethet, tilstrekkelighet og effektivitet. IBM Watson Health-programmet for informasjonssikkerhet blir oppdatert fra tid til annen, slik at det løpende holdes oppdatert ifølge generelt akseptert bransjepraksis og Gjeldende lovgivning for IBM.

2. Tilgangskontroll

IBM skal gjøre Kundens innhold kjent kun for IBMs ansatte, underleverandører eller tredjeparter som har et berettiget forretningsmessig behov for å få tilgang til Kundens innhold for å hjelpe IBM med å utføre IBMs forpliktelser overfor Kunden eller andre personer, slik det er nødvendig for å levere IBM SaaS i henhold til Gjeldende lovgivning, Avtalen eller et Tilhørende dokument, avhengig av hva som er aktuelt. Hvis IBM er Kundens Forretningspartner, skal IBM og Kunden avgi Personlige helseopplysninger kun i henhold til betingelsene i en gjeldende BAA-avtale (Business Associate Agreement) mellom Partene.

IBM har en formell, intern prosess for administrasjon av brukertilgang, der brukertilgang forespørres, godkjennes etter verifisering av identitet, og tildeles basert på prinsippet om kunnskapsbehov ("need to know") og prinsippet om lavest mulig rettighet ("least privilege"). Tilgang til Kundens innhold begrenses til kun aktive brukere og aktive brukerkontoer. IBM har en formell prosess for periodisk intern revalidering av tilgang for aktive brukerkontoer.

IBM bruker sikre protokoller for brukerautentisering, inkludert at det tildeles unike identifikasjoner og sterke passord til aktive brukerkontoer på systemer som brukes til å levere tjenester til Kunden, i henhold til IBM Corporate Security-standarder og -retningslinjer.

a. Passord skal ikke være leverandørleverte standardpassord, og de skal oppbevares på et sted og/eller i et format som ikke setter sikkerheten til dataene de beskytter, i fare.

b. Visning og utskrift av passord må være maskert, blokkert eller på annen måte skjult slik at uautoriserte parter ikke kan iaktta eller senere gjenopprette dem. Passord må ikke logges eller registreres når de skrives inn. Brukerpassord må ikke lagres i klartekst.

c. Passord for hver teknologi som utgjør IBM SaaS, blir valgt for å redusere risikoen som er knyttet til kjent sårbarhet for passordlengde, og må dokumenteres.

d. Når bruk av interne, privilegerte, delte funksjons-IDer er nødvendig av driftsmessige årsaker, administrerer IBM delte funksjons- og/eller system-IDer som krever uthenting av passord, for å kunne fastslå den enkeltes ansvar.

Tidsgrenser for uvirksomhet etableres for alle systemer og applikasjoner som lagrer Kundens innhold.

Ved behov etableres det, på forespørsel fra Kunden og med IBMs formelle godkjennelse, ekstern tilgang til IBMs nettverk, systemer og applikasjoner som lagrer Kundens innhold, og alle slike eksterne tilkoblinger sikres med sterke autentiserings- og krypteringsprotokoller. Aktivitet med ekstern tilgang skal logges og overvåkes.

I den utstrekning levering av IBM SaaS krever at IBM får ekstern tilgang til et system i Kundens interne nettverk, skal all slik ekstern tilgang skje kun ved bruk av Kundens sikre systemer og protokoller for ekstern tilgang og tilgangslegitimasjon Kunden fremskaffer for IBM. Ekstern tilgang til Kundens nettverk skal kun etableres på forespørsel fra IBM og med godkjennelse fra Kunden, og i henhold til Kundens gjeldende retningslinjer på det aktuelle tidspunktet, som leveres IBM på forhånd. IBMs bruk av Kundens interne nettverk skal skje i henhold til Kundens retningslinjer for IT-bruk og sikkerhet, som leveres IBM på forhånd.

IBM implementerer oppgavedifferensiering for sikkerhetsadministrasjon, tilgangsgjennomgåelse og undersøkelser av brudd på sikkerheten.

Lagring, verting og behandling av innhold som er spesifikt for Kunden, holdes logisk atskilt fra andre kunders innhold som betjenes av IBM. I situasjoner der delt arbeidsområde for lagring, verting og behandling er godkjent av Kunden, skal IBM ha prosedyrer og sikkerhetstiltak som er konsistente med kravene som fremkommer i dette Vedlegget for sikkerhet og driftskontinuitet, og som er utformet for å forhindre uautorisert avgivelse av Kundens innhold.

IBM implementerer retningslinjer for tomt skrivebord og tom skjerm, for å sikre at Kundens innhold ikke på noe tidspunkt forlates uten tilsyn på et offentlig sted.

3. Overføring og kryptering

IBM skal ta passende forholdsregler ved overføring av Kundens innhold (via faks, e-post, kurer, osv.) for å sørge for at riktige kontaktopplysninger blir brukt for mottakeren, samt gjøre avtale på forhånd med tiltenkt mottaker for å sikre mottaket av slik informasjon.

IBM bruker, og skal sørge for at IBMs personell bruker, riktige former for kryptering eller andre sikre teknologier i forbindelse med all behandling av Kundens innhold, inkludert i forbindelse med overføring, kommunikasjon, ekstern tilgang eller lagring (inkludert lagring av sikkerhetskopier) av Kundens innhold. IBM skal for eksempel kryptere, ved hjelp av passende bransjestandard for kryptering, alle poster og filer som inneholder Kundens innhold

a. som er lagret på IBMs PCer, bærbare enheter eller flyttbare elektroniske medier, inkludert magnetbånd med sikkerhetskopier, når de er under overføring til et eksternt lagringssted;
b. som er lagret eller transporteres av IBM utenfor Kundens eller IBMs fysisk sikrede kontorer og anlegg, unntatt trykte papirdokumenter;
c. ved overføring på tvers av offentlig tilgjengelige nettverk utført av IBM;
d. ved overføring fra IBMs systemer til Kunden;
e. ved trådløs overføring utført av IBM; og
f. som er lagret av IBM på servere og i databaser.

4. Nettverkssikkerhet

IBM bruker rimelig oppdaterte versjoner av programvare for systemsikkerhet, som brannmurer, proxyer, webapplikasjonsbrannmurer og grensesnitt. Slik programvare må omfatte beskyttelse mot skadelig programvare og rimelig oppdaterte rettelser og virusdefinisjoner. I henhold til selskapets standarder skal antivirusprogramvare være installert på arbeidsstasjoner, servere og tilhørende sluttpunkter der det er teknisk mulig, og programvaren administreres ifølge selskapets retningslinjer for internt administrerte løsninger.

IBM overvåker IBM SaaS for å oppdage og identifisere hendelser så tidlig som mulig. IBM skal som et minimum benytte standardverktøy for innbruddspåvisning og standardprosesser for beskyttelse, overvåking og reaksjoner, på en måte som er utformet for å identifisere både intern og ekstern sårbarhet og risiko som kan føre til uautorisert avgivelse, misbruk, endring eller tilintetgjøring av Kundens innhold eller informasjonssystemer som brukes til å levere tjenester til Kunden.

IBM abonnerer på tjenester for innsamling av informasjon om sårbarhet eller på anbefalinger for informasjonssikkerhet samt andre relevante kilder som leverer oppdatert informasjon om systemsårbarhet. IBM utfører jevnlig sårbarhetsvurderinger og utbedringer av sine nettverk.

IBM overvåker IBM SaaS for å oppdage, identifisere, forhindre og løse Sikkerhetshendelser.

IBM validerer tilgjengeligheten, integriteten og effektiviteten til nettverkssikkerhetsinfrastrukturen der IBM SaaS er tilgjengelig, gjennom IBM Release Management-prosesser.

5. Håndtering og varsling av hendelser

IBM Watson Health-teamene samarbeider med IBM Cybersecurity Incident Response Team, et globalt team som håndterer mottak, undersøkelse og intern koordinering av sikkerhetshendelser knyttet til IBM-løsninger, og implementerer nødvendige tiltak for å redusere programvarerelaterte sikkerhetsproblemer. En "Sikkerhetshendelse" er gjennomført, uautorisert tilgang til, bruk, avgivelse eller endring av, eller inngrep i systemoperasjoner eller data i et informasjonssystem som brukes av IBM for levering av IBM SaaS. Hvis en Sikkerhetshendelse blir oppdage (via rutineavsøking, varsler, terskelhendelser eller liknende), skal IBM informere og varsle Kunden

a. om enhver bekreftet Sikkerhetshendelse som omfatter Kundens innhold, så snart som mulig og under ingen omstendighet senere enn 2 arbeidsdager etter undersøkelsen og bekreftelsen av en slik Sikkerhetshendelse;

b. umiddelbart etter en forespørsel om tilgang til, eller informasjon om, noe av Kundens innhold fra en representant for en offentlig myndighet (inkludert fra en personvernmyndighet eller rettshåndhevende myndighet), med mindre dette er forbudt ifølge lovgivning eller relevant forordning; og

c. unntatt slik det er tillatt ifølge punktet Tilgangskontroll i dette Vedlegget for sikkerhet og driftskontinuitet, før noen avgivelse eller overføring av, eller tilgang til, Kundens innhold til eller av en tredjepart.

6. Logging

IBM håndhever, i henhold til IBMs retningslinjer og praksis samt generelt akseptert bransjepraksis, rimelig overvåking av systemer med henblikk på uautorisert bruk av og tilgang til Kundens behandlede data. Faktiske eller forsøk på påloggingsovertredelser og tilgangsovertredelser blir logget.

IBM oppbevarer registreringer av alle tilgangsforespørsler og logger over tilgangsaktiviteter for alle systemer som lagrer, får tilgang til, behandler eller overfører Kundedata og Helsedata, så lenge som det kreves ifølge HIPAA og annen Gjeldende lovgivning for IBM om personvern.

Loggene og rapportene omfatter som et minimum (i) alle påloggingsforsøk, enten de er vellykkede eller ikke, inkludert rimelig identifiserende informasjon; (ii) alle endringer av system- og nettverkskonfigurasjon, inkludert installering av applikasjoner, brukeradministrasjonsendringer og endringer av filtilgangstillatelser; (iii) forsøk på tilgang til ressurser, enten de er vellykkede eller ikke, inkludert forsøk på tilgang til en fil, nettverksdeling, logg eller annen ressurs; og (iv) datanedlastinger, inkludert innholdstypen til dataene og tilgangsprotokollen som ble brukt til å utføre nedlastingen.

7. Utvikling av programvareapplikasjoner og endringshåndtering

IBM følger sikker praksis for applikasjonsutvikling og koding, som beskytter integriteten til produksjonsapplikasjoner og tilhørende kildekode mot uautoriserte og utestede endringer.

IBM følger en endringshåndteringsprosess som omfatter (a) registrering og formell godkjennelse av endringer samt tilbaketrekkingsprosedyrer; og (b) passende testing av slike endringer, inkludert testing av brukeraksept der det er aktuelt, så vel som sikkerhetstesting.

IBM følger en prosess for administrasjon av rettelser, som omfatter testing av rettelser før installering på alle systemer som brukes til å lagre, få tilgang til og overføre Kundens innhold, eller som brukes til å levere tjenester, inkludert IBM SaaS, til Kunden.

IBM krever at systemadministratorer opprettholder fullstendig, nøyaktig og oppdatert informasjon om konfigurasjonen av alle informasjonssystemer som brukes til å lagre, få tilgang til eller overføre Kundens innhold.

8. Fysisk sikkerhet og miljøsikkerhet

IBM Watson Health Core-plattformen er implementert på IBM SoftLayer-datainfrastrukturen. IBM SoftLayer opprettholder fysisk og miljømessig sikkerhet, tilgangskontroll, kontroller og prosesser for å beskytte Kundedata mot menneskelig, miljømessig og teknisk mislighold eller påvirkning.

Generell adgang til anleggene der IBM SaaS vertes, er kontrollert ved hjelp av et system med adgangskort. CCTV-kameraer er installert i hele anlegget og overvåkes av sikkerhetspersonell. Utvalgte adgangsdører har alarm, og sikkerhetspersonell overvåker disse alarmene.

Adgang til kontrollerte områder er begrenset gjennom bruk av adgangskort og/eller biometrisk tilleggskontroll. Alle personer som ikke har autorisert adgang til de kontrollerte områdene, må registreres

og ledsages av en person med godkjent adgang til det kontrollerte området. Alle nødutganger i kontrollerte områder har lydalarm, og sikkerhetspersonell overvåker disse alarmene. Det utføres periodisk kontroll av at alarmene fungerer, og dette dokumenteres og arkiveres. Adgangsrett til kontrollerte områder godkjennes på nytt hvert kvartal. Adgang til kontrollerte områder inndras når et arbeidsforhold opphører.

Anleggene er beskyttet mot miljøfaktorer som brann, vann og varme gjennom brannalarmer, brannslukkingsapparater, røykvarslere samt brannvern- og brannslukkingssystemer. Anleggene er beskyttet mot strømavbrudd eller strømfeil gjennom UPS-systemer (Uninterruptible Power Supply) og reservegeneratorer, som regelmessig vedlikeholdes og testes.

Informasjon og rapporter vedrørende IBM SoftLayer-sikkerhet finnes her: http://www.softlayer.com/compliance.

9. Driftskontinuitet

IBM har planer for driftskontinuitet og katastrofehåndtering, som er utformet for å opprettholde et servicenivå som er i overensstemmelse med IBMs forpliktelser i henhold til Avtalen. Slike planer for driftskontinuitet og katastrofehåndtering skal oppdateres og testes jevnlig (minst en gang per år). IBM skal implementere alle rimelige endringer i planer for driftskontinuitet og katastrofehåndtering, som er nødvendige for å overholde generelt akseptert bransjepraksis, i hvert enkelt tilfelle uten i urimelig grad å gripe forstyrrende inn i IBM SaaS eller produksjonsmiljøet som Kunden bruker.

Dersom det skulle inntreffe en katastrofe som gjør IBM SaaS utilgjengelig for Kunden, skal IBM straks varsle Kunden og aktivere planen for driftskontinuitet og/eller katastrofehåndtering. Når en katastrofe er erklært, er målet for driftskontinuitet for IBM SaaS å gjenopprette Kundens tilgang til IBM SaaS som følger: Ved nedetid er Målet for gjenopprettingstid (RTO) å gjenopprette IBM Watson Health-produksjonsmiljøet innen 36 timer etter katastrofeerklæringen. Målet for gjenopprettingspunkt (RPO) er maksimalt 24-timers tap av Kundens innhold i produksjonsmiljøet. Målene for driftskontinuitet for bestemte Watson Health-løsninger kan variere.

IBMs tilnærming til katastrofehåndtering består i flere datasentre i spredtliggende geografiske områder.

Alle IBM SoftLayer-datasentre har flere strømtilførselsenheter, fiberlinjer, reserverte generatorer og reservebatterier. De er oppbygd av bransjeledende maskinvare og utstyr, og har høyeste nivå av ytelse, pålitelighet og interoperabilitet. Alle datasenterkomponenter som inkluderes, for eksempel redundante n+1-ressurser for strømtilførsel og kjøling, blir inspisert for å opprettholde stabilitet i datasentrene.

10. Overholdelse

IBMs sikkerhetspraksis er basert på ISO 27001-27002. Slik praksis gir kontrollstrukturer for, men ikke begrenset til, risikoanalyse, fysisk sikkerhet, planlegging for katastrofehåndtering, undersøkelser, beskyttelse av informasjon, opplæring, personvern og drift.

IBM kontrollerer at aktiviteter knyttet til sikkerhet og personvern er i overensstemmelse med IBMs sikkerhetspraksis.

IBM overholder Gjeldende lovgivning for IBM om personvern i Omfattede jurisdiksjoner.

Riktig håndtering av Kundens konfidensielle informasjon kreves også ifølge IBMs retningslinjer for forretningspraksis (Business Conduct Guidelines), som alle ansatte årlig må gjennomgå (og bekrefte at de har gjennomgått).

11. Diverse

IBM skal sørge for at IBMs avtaler med underleverandører og/eller tredjeparter som er engasjert i leveringen av IBM SaaS, har betingelser som beskytter Kundens innhold minst like godt som betingelsene i dette Vedlegget for sikkerhet og driftskontinuitet, og i ethvert gjeldende Tilhørende dokument, i begge tilfeller i den utstrekning slike betingelser gjelder for tjenestene som skal utføres av slike underleverandører og/eller tredjeparter.