IBM Watson Health Core

Uvjeti upotrebe ("ToU") sastoje se od ovih IBM-ovih Uvjeta upotrebe – Uvjeti za određene SaaS ponude ("Uvjeti za određene SaaS ponude") i dokumenta nazvanog IBM-ovi Uvjeti upotrebe – Opći uvjeti ("Opći uvjeti") dostupnom na sljedećem URL-u: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

U slučaju sukoba, SaaS Uvjeti za određene SaaS ponude imaju prednost pred Općim uvjetima. Naručivanjem, pristupanjem ili korištenjem IBM SaaS-a Klijent prihvaća Uvjete upotrebe (ToU).

Uvjete upotrebe (ToU) uređuje IBM Međunarodni Passport Advantage ugovor, IBM Međunarodni Passport Advantage Express ugovor ili IBM Međunarodni ugovor za Izabrane IBM SaaS ponude, ovisno što se primjenjuje ("Ugovor"), koji zajedno s Uvjetima upotrebe čine cjeloviti ugovor.

1. IBM SaaS

Ovi Uvjeti za određene SaaS ponude odnose se na sljedeće IBM SaaS ponude:

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

2. Metrike naplate

IBM SaaS se prodaje u skladu sa sljedećom metrikom ili metrikama naplate navedenim u Transakcijskom dokumentu:

a. **Pristup** – je jedinica mjere po kojoj se može dobiti IBM SaaS. Pristup je pravo korištenja IBM SaaS-a. Klijent mora dobiti jedno pravo Pristupa da bi mogao koristiti IBM SaaS za vrijeme perioda mjerenja koji je naveden u Dokazu o ovlaštenju (PoE) ili Transakcijskom dokumentu Klijenta.

b. **Pojedinac** – je jedinica mjere po kojoj se može dobiti IBM SaaS. Pojedinac je jedna stvar ili ljudsko biće. Moraju se dobiti dostatna ovlaštenja za pokrivanje svakog Pojedinca kojeg obrađuje ili kojim upravlja IBM SaaS tijekom perioda mjerenja navedenog u Klijentovom Dokazu o ovlaštenju (PoE) ili Transakcijskom dokumentu.

   Za potrebe ovog IBM SaaS-a, Pojedinac mogu biti osobe, uređaj ili mobilna aplikacije čijim podacima upravlja IBM SaaS.

c. **Instanca** - je jedinica mjere po kojoj se može dobiti IBM SaaS. Instanca označava pristup određenoj konfiguraciji IBM SaaS-a. Moraju se pribaviti dostatna ovlaštenja za svaku Instancu IBM SaaS-a, koja je dostupna za pristup i korištenje tijekom perioda mjerenja navedenog u Klijentovom PoE-u ili Transakcijskom dokumentu.

3. Naknade i naplata

Iznos koji se plaća za IBM SaaS naveden je u transakcijskom dokumentu.

3.1 Djelomične mjesečne naknade

Na temelju razmjerne procjene može se izračunati djelomična mjesečna naknada, kako je navedeno u Transakcijskom dokumentu.

3.2 Naknade za prekomjernu upotrebu

Ako Klijentova stvarna upotreba IBM SaaS-a za vrijeme perioda mjerenja premašuje Klijentovo ovlaštenje navedeno u PoE-u, Klijentu će se izdati račun za prekomjerni iznos, kako je navedeno u Transakcijskom dokumentu.

4. Opcije trajanja i obnavljanja

Trajanje IBM SaaS-a počinje na datum kada IBM obavijesti Klijenta o njegovom pristupu Pilot operativnoj okolni IBM SaaS-a, kako je dokumentirano u dokumentu Narudžbe. Period pretplate za Pojedinačna ovlaštenja počinje kada IBM obavijesti Klijenta o njegovom pravu pristupa Proizvodnoj operativnoj okolini. Dokument narudžbe će određivati obnavlja li se IBM SaaS automatski, nastavlja li se na temelju kontinuirane upotrebe ili se raskida na kraju perioda.

Za automatsko obnavljanje, ako Klijent ne dostavi pisanu obavijest o neobnavljanju barem 90 dana prije datuma isteka, IBM SaaS će se automatski obnoviti u trajanju navedenom u PoE-u.

Kod kontinuirane upotrebe, IBM SaaS će biti dostupan na mjesečnoj osnovi dok Klijent ne dostavi pisanu obavijest o raskidu 90 dana unaprijed. IBM SaaS će biti dostupan do kraja kalendarskog mjeseca nakon takvog perioda od 90 dana.

5. Tehnička podrška

IBM će pružiti Priručnik za podršku za IBM Software as a Service, koji sadrži informacije o kontaktiranju tehničke podrške, termine održavanja i druge informacije i procese. Kontakt informacije za tehničku podršku i druge detalje vezane za operacije podrške mogu se pronaći u Priručniku za podršku za IBM SaaS na: https://support.ibmcloud.com.

Tehnička podrška i jednostavni konfiguracijski zahtjevi za IBM SaaS se pružaju elektroničkim putem. Tehnička podrška nudi se uz IBM SaaS i nije dostupna kao zasebna ponuda.

Osobni podaci (PI), uključujući Zaštićene zdravstvene informacije (PHI) i osjetljive osobne podatke (SPI), ne smiju se stavljati u bilo kakvu dokumentaciju ili u informacije kada se prijavljuje problem.

6. Definicije

Mjerodavno pravo – označava zakone, statute ili pravne odluke, pravila, propise, direktive, mandate, dekrete ili druge zahtjeve donesene od strane upravnog autoriteta ili bilo koji općenito priznati industrijski standardi, koji su mjerodavni za izvedbu ovih Uvjeta upotrebe

API – znači sučelje aplikativnog programiranja, koje se sastoji od rutina, protokola i alata za izgradnju softverskih aplikacija. API specificira kako međudjeluju softverske komponente, a koristi se kada se programiraju komponente grafičkog korisničkog sučelja (GUI).

Ovlašteni administrator – je zaposlenik Klijenta, odobreni Klijentov ugovaratelj, pojedinac ili grupa, odgovorna za upravljanje održavanja i pouzdanog rada platforme. Odgovornosti mogu uključivati konfiguraciju, podršku te upravljanje korisnicima i računima. Administrator može također biti klinički istražitelj odgovoran za postavljanje studije u Watson Health sustavu.

Ovlašteni pojedinac – je ovlaštena osoba, mobilna aplikacija ili uređaj, kojem je dodijeljeno pravo pristupa pristupnim pravima za slanje podataka u Watson Health Core. To može biti Klijent ili učesnici studije, korisnici ili pacijenti Klijenata.

Zakoni o podacima primjenjivi na Klijenta – znači Zakoni o podacima primjenjivi na izvedbu Klijentovih obveza pod ovim Ugovorom, Pridruženim dokumentima i primjenjivim Opisima usluga, Dokumentima narudžbe i Opisima posla između strana.

Podaci Klijenta – znači bilo koji ulaz podataka u IBM SaaS od strane Klijenta ili za Klijenta, bilo da su to Klijentovi vlastiti podaci ili podaci koje je unijo Klijent ili su uneseni u ime Klijentovog korisnika ili bilo koje treće strane, a uključuju bilo kakve podatke iz zdravstvenog uređaja treće strane.

Zakoni o podacima – znači Mjerodavno pravo koje se odnose na zaštitu podataka, privatnost ili sigurnost.

Predmet podataka – znači pojedinac, identificirani ili koji se može identificirati, na kojeg se odnose Osobni podaci.

Namjenski centar podataka – znači centar(ri) podataka specificirano kao primarni ili centri podataka za obnavljanje od katastrofe, specificirani u Transakcijskom dokumentu, u kojima se izvodi Klijentova instanca IBM SaaS-a, ako je primjenjivo.

Zdravstveni podaci – znači bilo koji podaci ili informacije, uključujući slike, koji se odnose na zdravstvene Osobne podatke.

Omogućeni zdravstveni podaci – znači, u okviru IBM SaaS-a, sposobnost IBM SaaS-a da zadovolji mjerodavne standarde sigurnosti i privatnosti, zakone i propise u nadležnostima zemalja opsega za Zdravstvene podatke, uključujući specifikacije implementacija navedene u Dijelu 164, Poddijelovi A i C, za propise koji implementiraju HIPAA (modificirani s HITECH zakonom) i druge mjerodavne propise vezane za Zdravstvene podatke, ali ne znači da IBM djeluje u funkciji Poslovnog suradnika ili Kontrolora podataka.

HIPAA – znači Health Insurance Portability and Accountability Act (Zakon o prenosivosti i odgovornosti zdravstvenog osiguranja) iz 1996., promijenjen uključuje zakon Health Information Technology for

Economic and Clinical Health Act (kratko "HITECH Act")(Zakon o tehnologiji zdravstvenih informacija za ekonomsko i kliničko zdravlje) iz zakona American Recovery and Reinvestment Act (Američki zakon o oporavku i reinvestiranju) od 2009, neke propise koji su proglašeni pod HIPAA-om od strane Ministarstva zdravstva i socijalne skrbi Sjedinjenih Država u 45 C.F.R. Dijelovima 160 i 164 i određene propise proglašene u skladu s HITECH zakonom.

Zakoni o podacima primjenjivi na IBM – znači Zakoni o podacima primjenjivi na izvedbu IBM-ovih obveza pod ovim Ugovorom, Pridruženim dokumentima i primjenjivim Opisima usluga, Dokumentima narudžbe i Opisima posla između strana.

IBM Osoblje – znači (a) IBM, njegova Povezana društva i podugovarači te zaposlenici prethodno navedenih; i (b) bilo koji dobavljač treće strane; u svakom slučaju onaj koji izvodi usluge u ime IBM-a u skladu s Ugovorom i primjenjivim Pridruženim dokumentima ili koga je IBM ovlastio za pristup Osobnim podacima Klijenta.

Zemlje opsega – znači 28 zemalja članica Europske Unije i Švicarska, i one zemlje koje IBM možda doda na ovu listu od vremena do vremena.

Osobni podaci ili **Osobne informacije** – znači informacije na bilo kojem mediju ili formatu, uključujući elektroničke i papirnate zapise, koji se odnose pojedinca, identificiranog ili koji se može identificirati, gdje je "pojedinac koji se može identificirati" netko tko se može identificirati, izravno ili posredno, posebice putem referentnog identifikacijskog broja ili jednog ili više faktora specifičnih za fizički, fiziološki, mentalni, ekonomski, kulturološki ili društveni identitet.

Proces i njegove inačice, na primjer **obrada** (pisano velikim ili malim početnim slovom) – znači bilo koju operaciju ili skup operacija koje se izvode na podacima, automatski ili ne, na primjer skupljanje, zapisivanje, organizacija, pohrana, prilagodba ili promjena, dohvat, konzultacija, upotreba, otkrivanje putem prijenosa, širenje ili na drugi način činiti dostupnim, poravnanje ili kombiniranje, blokiranje, brisanje ili uništavanje.

Obrađeni podaci – znači bilo koji podaci, povjerljive ili u vlasništvu informacije ili materijali, uključujući Zdravstvene podatke i Osobne podatke, koje obrađuje IBM u skladu s Ugovorom, Pridruženim dokumentom i/ili Opisom usluga, Dokumentom narudžbe i/ili Opisom posla.

Sigurnosni incident – ima značenje izneseno u SBCA.

7. Upravljanje računima

IBM SaaS je dostupan ovlaštenim korisnicima Klijenta (samo "**Ovlašteni administratori**" ili "**Ovlašteni pojedinci**"). Klijent će kontrolirati račune ovlaštene za pristup IBM SaaS-u, što može uključivati ovlaštene aplikacije, osoblje Klijenta, Klijentove pružatelje usluga treće strane i ugovaratelje, Klijent je isključivo odgovoran za (i) kontroliranje svih ovlaštenih korisnika, uključujući, ali bez ograničenja na, provjeru identiteta bilo kojeg ovlaštenog korisnika; i (ii) osiguravanja pristupa IBM SaaS-u samo ovlaštenim korisnicima.

Ovlaštenim pojedincima koji su ujedno korisnici, pacijenti ili sudionici studije koju provodi Klijent, može se dodijeliti pravo pristupa isključivo u svrhu punjenja podataka u IBM SaaS, u tom slučaju Ovlašteni pojedinci neće imati druge vrste prava pristupa IBM SaaS-u.

8. Privatnost

8.1 Opći zahtjevi

Između strana, Klijent je isključivi kontrolor svih Klijentovih Osobnih podatka, Klijent imenuje IBM kao svojeg obrađivača podataka. U skladu s Primjenjivim zakonima o podacima, Klijent ima pravo uputiti IBM u vidu IBM-ove obrade Klijentovih Osobnih podataka.

U opsegu u kojem IBM obrađuje Klijentove Osobne podatke, IBM će:

a. poštivati sve Zakone o podacima primjenjive na IBM; i

b. neće miješati Klijentove Osobne podatke s podacima iz drugih izvora osim:

- kada je potrebno podatke pružiti IBM SaaS-u, ne za bilo koju svrhu već po posebnim uputama Klijenta da tako napravi; ili
- u skladu s odredbama ovih Uvjeta upotreba i SBCA dodatka.

U opsegu u kojem IBM obrađuje Klijentove Osobne podatke, Klijent će:

a. poštivati sve Zakone o podacima primjenjive na Klijenta;

b. biti odgovoran za sve komunikacije između Klijenta i Klijentovih povezanih društava, pacijenata, krajnjih korisnika Predmeta podataka i/ili drugih Klijentovih trećih strana;

c. sklopiti ugovore za obradu podataka sa svojim kontrolorima, koji su potrebni da bi IBM kao obrađivač podataka sa svojim podobrađivačima mogao obraditi Klijentove Osobne podatke; i

d. biti jedini kontakt za IBM i isključivo je odgovoran za unutarnju koordinaciju, pregled i slanje uputa ili zahtijeva Klijentovih povezanih društava, koji služe IBM-u kao drugi kontrolori. IBM će biti oslobođen svoje obveze informiranja ili obavještavanja Klijentovih povezanih društava koja predstavljaju kontrolore kada proslijedi takve informacije ili obavijesti Klijentu. IBM ima pravo odbiti upute koje dolaze izravno od bilo kojeg Klijentovog povezanog društva koje predstavlja kontrolora, a nije Klijent.

Nijedna strana neće morati poduzeti radnje koje krše Primjenjive zakone o podacima neke strane.

8.2 Klijentova prava na podatke

Klijent izjavljuje i jamči (a) da je vlasnik podataka koje će unijeti u IBM SaaS ili (b) da je stekao i odgovoran je za održavanje svih potrebnih prava, dozvola, pristanaka i ovlaštenja kako bi dodijelio IBM-u pravo pristupa, korištenja i otkrivanja Klijentovih podataka u skladu s odredbama navedenim u ovim Uvjetima upotrebe ili Ugovoru ili na drugi način što je inače potrebno IBM-u kako bi osigurao IBM SaaS. Klijent nadalje izjavljuje i jamči da su Klijentovi podaci samo ili (a) vezani za pojedince nastanjene u Sjedinjenim Državama i bit će samo unijeti u IBM SaaS u centru podataka u Sjedinjenim državama ili (b) vezani za pojedince nastanjene u jednoj ili više zemalja opsega i bit će samo unijeti u IBM SaaS u imenovanom centru(ima) podataka.

8.3 Usluge podataka i odgovornosti

a. Klijent pristaje da će samo izvoditi analitiku ili zahtijevati da IBM izvede analitiku na Klijentovim podacima, a koji se odnose na aktivnosti koje sačinjavaju ili Klijentove "operacije zdravstvene skrbi" ili "istraživanje" jer je svako od toga definirano u HIPAA i/ili sličnim pojmovima pod drugim Primjenjivim zakonima o podacima i da će Klijent koristiti Klijentove podatke ili uputiti IBM da koristi samo Klijentove podatke u skladu sa svim relevantnim zahtjevima (npr. odluka ili odricanje institucijskog odbora za reviziju gdje je to potrebno) pod ovim i bilo kojim drugim Zakonima o podacima primjenjivim na klijenta.

b. Klijent je isključivo odgovoran za nabavu svih registracija, pristanaka, ovlaštenja i dozvola koje zahtijevaju Zakoni primjenjivi na Klijenta u svakoj Zemlji opsega u kojoj se primjenjuje, uključujući, ali ne ograničavajući se na, HIPAA i bilo koje druge mjerodavne propise, pravila i odredbe o privatnosti i sigurnosti podataka, da bi se podaci Klijenta mogli unijeti u IBM SaaS te koristiti i otkriti kako se smatra pod ovim Uvjetima upotrebe i u Ugovoru između Klijenta i IBM-a i IBM-ovih podugovarača. IBM nije odgovoran za nadgledanje kada su dobivene ili potrebne takve registracije, pristanci, ovlaštenja i dozvole.

c. Klijent je isključivo odgovoran osigurati da su svi Klijentovi podaci unijeti u IBM SaaS ograničeni na podatke koji se odnose na pojedince nastanjene u Sjedinjenim Državama ili u zemlji opsega gdje je to primjenjivo.

d. IBM će imati centre podrške s osobljem osposobljenim za HIPAA i druge Zakone o podacima primjenjive na IBM za podatke iz zemalja opsega.

8.4 Sigurnosne mjere i sigurnosni incidenti

a. IBM će primijeniti, održavati i poštivati tehničke i organizacijske mjere (uključujući organizacijske procese i postupke, uključujući sve posebne sigurnosne obveze navedene ili referencirane u ovim Uvjetima upotrebe i u SBCA kako bi zaštito Klijentove Osobne podatke od neovlaštene upotrebe ili pristupa, slučajnog gubitka, oštećenja, mijenjanja, uništenja, krađe ili neovlaštenog otkrivanja.

b. U slučaju ako IBM uoči Sigurnosni incident (prema SCBA definiciji) koji uključuje Klijentove Obrađene podatke, IBM će obavijestiti Klijenta u skladu s odredbama SBCA i Zakonima o podacima primjenjivim na IBM, takva obavijest će sadržavati informacije koje se odnose na bilo koji poznati utjecaj na Klijenta ili na Predmete podatak (ako postoje) pod utjecajem takvog Sigurnosnog incidenta te o poduzetoj korektivnoj radnji ili o prijedlogu takve radnje koju će poduzeti IBM.

8.5 Primanje upita i žalbi

IBM će obavijestiti Klijenta pisanim putem odmah i u mjeri dozvoljenoj Zakonima o podacima primjenjivim na IBM, ne kasnije od pet (5) dana nakon primitka upita, komunikacije ili žalbe od službenika privatnosti podataka IBM Watsona upućene IBM-u vezane za Klijentove osobne podatke:

a. bilo kojeg Subjekta podataka, vezano za Osobne podatke o tom Predmetu podataka koje je obradio IBM. Klijent će odgovoriti na takve zahtjeve Predmeta podataka i IBM će pristati na razumne upute Klijenta kako bi pomogao Klijentu da odgovori na takve zahtjeve. Ako to zahtijevaju Zakoni primjenjivi na IBM, IBM može izravno odgovoriti na takve zahtjeve, uz uvjet da IBM obavijesti Klijenta unaprijed o takvom odgovoru i razumno koordinira s Klijentom u vidu oblika i pristanka na takav odgovor, kada to dozvoljavaju Zakoni primjenjivi na IBM ili na drugi način;

b. bilo kojeg pravnog ili regulatornog autoriteta, koji se odnose na IBM-ovu Obradu Klijentovih osobnih podataka, uz uvjet da IBM može odgovorite na takve zahtjeve upućene iz upravnog tijela sa sudskim pozivom ili sličnim pravnim dokumentom, koji prisiljava IBM na otkrivanje ili se na drugi način zahtijeva radi mjerodavnog Zakona o podacima, uz uvjet da IBM unaprijed obavijesti Klijenta o takvom otkrivanju i razumno koordinira s Klijentom u vidu oblika i sadržaja takvog odgovora, u mjeri dozvoljenoj zakonom ili omogućeno na drugi način.

8.6 Obrada Klijentovih osobnih podataka

IBM će ograničiti otkrivanje Klijentovih osobnih podataka na ono IBM osoblje, koje je obvezno pomoći u pružanju Usluga.

IBM će pristati na razumne zahtjeve Klijenta koji zahtijevaju da IBM popravi, ispravi, izbriše ili blokira Klijentove osobne podatke u skladu s Mjerodavnim pravom.

Na zahtjev bilo koje strane, IBM-a, Klijenta ili njegovih Povezanih društava, sklopit će se ugovori koje zahtijevaju propisi za zaštitu Klijentovih osobnih podataka. Strane se slažu (i pribavit će pristanak svojih pripadnih povezanih društava) da su takvi ugovori predmet ograničenja i isključivanja od odgovornosti ovog Ugovora u svrhu potraživanja između Strana. Strane će surađivati prilikom sklapanja (ili pribavljanja pristanka povezanih društva strane za sklapanje) i poštivanja daljnjih zajednički dogovorenih odredbi ili ugovora ako tako zahtijevaju Primjenjivi zakoni o podacima.

8.7 Vraćanje Klijentovih osobnih podataka

Po isteku ili raskidu Ugovora, IBM će, kao i svo njegovo osoblje, prestati koristiti ili obrađivati informacije u vlasništvu Klijenta i sve Klijentove osobne podate, prema volji i zahtjevu Klijenta, će:

a. odmah vratiti, u formatu i na mediju za pohranu kojeg Klijent razumno zatraži, sve podatke u vlasništvu Klijenta, a Klijentove osobne podatke, koje IBM sprema u elektroničkom obliku, nakon Klijentove potvrde o primitku, izbrisati, uništiti ili na drugi način učiniti trajno nečitljivima ili da se ne mogu dešifrirati, Informacije u vlasništvu Klijenta i Klijentove osobne podatke, uključujući kopije i sigurnosne kopije. IBM može naplatiti naknadu za medij pohrane i za određene radnje izvedene na zahtjev Klijenta (na primjer, dostava informacija u vlasništvu Klijenta i Klijentovih osobnih podataka u određenom formatu ili uništavanje informacija u vlasništvu Klijenta i Klijentovih osobnih informacija na određeni način); i

b. izravno izbrisati uništavanjem ili na drugi način učiniti trajno nečitljivim ili da se ne mogu dešifrirati informacije u vlasništvu Klijenta i Klijentove osobne podatke, uključujući kopije i sigurnosne kopije.

8.8 Ugovor s poslovnim suradnikom

U mjeri koja je prikladna i koju zahtijeva HIPAA, IBM i Klijent će sklopiti Ugovor s poslovnim suradnikom ("BAA"), koji uređuje IBM-ove obveze kao poslovnog suradnika Klijenta tijekom pružanja usluge ovog IBM SaaS-a. Bez ograničavanja IBM-ovih izričitih obveza iz Ugovora i BAA ako je primjenjivo, Klijent potvrđuje i pristaje na odgovornost utvrđivanja mjerodavnosti i poštivanja svih Mjerodavnih propisa i zahtjeva licenciranja, koji se odnose na Klijentovo korištenje i druge aktivnosti u odnosu na (uključujući korištenje ili druge aktivnosti Ovlaštenih korisnika) IBM SaaS.

8.9 Dodatak za obradu podataka Europske Unije

Ako Klijent zahtijeva od IBM-a da obradi Osobne podatke Europske Unije, IBM i Klijent će sklopiti Dodatak za obradu podataka, koji uključuje, ako je prikladno, klauzule E.U. modela s uklonjenim opcijskim klauzulama.

9. Dodatni uvjeti za IBM SaaS ponude

9.1 Sigurnost

Ovaj IBM SaaS slijedi IBM-ova načela sigurnosti i privatnosti podataka za IBM SaaS, dostupna na http://www.ibm.com/cloud/data-security, kao i dodatne odredbe navedene dolje i u Dodatku Sigurnost i poslovni kontinuitet ovih Uvjeta upotrebe. Bilo koja promjena IBM-ovih načela sigurnosti i privatnosti podataka neće degradirati sigurnost IBM SaaS-a.

IBM Watson Health Core implementira sigurnosne politike, standarde i procese bazirane na ISO 27001 građi detaljnije opisane u Opisu sigurnosti. Među ostalim sigurnosnim mogućnostima, ovo rješenje implementira sljedeće:

a. Sigurne operativne zone

   IBM Watson Health Core primjenjuje dubinsku strategiju zaštite, koristi višestruke sigurnosne zone za upravljanje integracijskim točkama clouda, poput učitavanja podataka i razvoja prilagođenih aplikacija.

b. Šifriranje

   Svi Klijentovi podaci su šifrirani u mirovanju i u prijenosu. Svi podaci u tranzitu u i iz IBM Watson Health Corea su šifrirani. Dijeljena usluga osigurava upravljanje ključevima šifriranja. Klijent je odgovoran za svu povezanost i kvalitetu mreže između IBM Watson Health Servicea i Klijentovog proxy poslužitelja.

c. Nadgledanje sigurnosnih događaja

   IBM koristi svoju platformu sigurnosne inteligencije za sigurnosne informacije i upravljanje događajima, upravljanje dnevnicima, forenziku incidenata, otkrivanje prijetnji i upravljanje s ranjivosti.

d. Upravljanje identitetom

   - Watson Health Core podržava pružatelje identiteta otvorenog standarda za velike populacije pacijenata i korisnika, koji koriste OpenID Connect.
   - Za populacije korisnika kod kojih je IBM pružatelj identiteta, Watson Health Core koristi odgovarajuće usluge imenika i mogućnosti upravljanja identitetom za rukovanje provjerom identiteta.

e. Jaka provjera identiteta i pristup baziran na ulogama

   - Watson Health Core podržava provjeru identiteta putem SAML-a kao mehanizma s kojim Klijenti integriraju svoj Single Sign On (SSO) ili usluge imenika.
   - Watson Health Core koristi rješenje za upravljanje pristupom i povezane komponente za upravljanje politikama sigurnosti tamo gdje je potrebno.
   - Watson Health Core podržava softversku provjeru identiteta s dva faktora.
   - Watson Health Core nudi osnovnu kontrolu pristupa baziranu na ulogama prema potrebi; Watson Health Core podržava konfiguraciju studije, korisničke profile, uloge i korisničke grupe putem programskih sučelja aplikacijskog programiranja ("API" ili "API-i"), koji omogućuju pristup na temelju uloga.

9.2 Cookieji

Klijent je svjestan i prihvaća da IBM može, kao dio uobičajene aktivnosti i podrške za IBM SaaS, prikupiti osobne podatke od Klijenta (vaših zaposlenika i ugovaratelja) koje se odnose na korištenje IBM SaaS-a, kroz praćenje i druge tehnologije. IBM to radi da bi prikupio korisne statističke podatke i informacije o učinkovitosti našeg IBM SaaS-a u svrhu poboljšanja korisničkog iskustva i/ili podešavanja interakcije s Klijentom. Klijent potvrđuje da će pribaviti ili je pribavio pristanak koji dozvoljava IBM-u da obrađuje prikupljene osobne podatke za gore navedenu svrhu unutar IBM-a, drugih IBM-ovih poduzeća i njihovih podugovarača, na svim lokacijama gdje mi i naši podugovarači poslujemo u skladu sa zakonom. IBM će se pridržavati zahtjeva Klijentovih zaposlenika i ugovaratelja vezanih za pristup, ažuriranje, ispravke ili brisanje njihovih prikupljenih osobnih podataka.

9.3 Lokacije koje primaju izvedenu korist

Gdje je to primjenjivo, porezi se temelje na lokaciji (ili lokacijama) za koje Klijent navede da primaju korist od IBM SaaS-a. IBM će primijeniti poreze koristeći poslovnu adresu navedenu kod naručivanja IBM SaaS-a kao primarnu lokaciju koja prima korist, osim ako Klijent ne dostavi dodatne informacije IBM-u. Klijent je odgovoran održavati takve podatke ažurnima i dostaviti sve promjene IBM-u.

9.4 Kontinuirana isporuka

Klijent ima ovlaštenje za mogućnosti i poboljšanja napravljena na rješenju i implementirana od strane IBM-a u kontinuiranom modelu isporuke clouda.

9.5 Sigurnosno kopiranje i vraćanje

IBM Watson Health Core osigurava sigurnosno kopiranje Klijentovih podataka iz proizvodne okoline (uključujući Data Lake i Data Reservoir spremišta) u zadnjem poznatom dobrom stanju za potrebe vraćanja usluge u slučaju kvara na sustavu.

9.6 Visoka dostupnost

IBM Watson Health Core komponente u proizvodnoj okolini se implementiraju u konfiguracijama visoke dostupnosti, u klastere redundantnih poslužitelja baza podataka, radi distribuiranja radnog opterećenja i eliminiranja pojedinačne točke kvara.

9.7 Obnavljanje od katastrofe

IBM-ov pristup obnavljanju od katastrofe sastoji se od višestrukih centara podataka u geografski rasprostranjenim područjima, radi postizanja ciljeva poslovnog kontinuiteta svoje proizvodne okoline, na sljedeći način:

- RTO – unutar 36 sati od proglašenja katastrofe
- RPO – ne više od 24 sata gubitka Klijentove povezanosti

9.8 Alati za mjerenja

IBM SaaS koristi sintetičko rješenje nadgledanja za nadgledanje, mjerenje i prijavu vezanu za dostupnost ili prekid rada u odnosu na obvezne razine usluga. Ovo rješenje simulira i prati odgovor korisnika i korisničko iskustvo na globalnoj razini - za statičku dostupnost i za transakcije.

IBM SaaS također koristi unutarnji sustav nadgledanja metrika, događaja i uzbuna kroz cijelo rješenje.

9.9 Publicitet

Klijent prihvaća da IBM može javno navesti Klijenta kao pretplatnika IBM SaaS ponuda u javnoj ili marketinškoj komunikaciji.

Dodatak A

1. IBM Watson Health Core

IBM Watson Health Core je platforma s omogućenim zdravstvenim podacima u obliku usluge (PaaS), platforma za razvoj i operativni podsustav za spremanja, sastavljanje i obradu Zaštićenih zdravstvenih informacija (PHI), kako je definirano u HIPAA i drugim zdravstvenim podacima u skladu sa Zakonima o podacima primjenjivim na IBM, koje se nalaze u centru podataka u vlasništvu ili pod upravom IBM-a. Klijent mora pribaviti odgovarajuća ovlaštenja za IBM Watson Health Core i IBM Watson Health Core Access kako bi omogućio dolje opisane funkcije i mogućnosti.

1.1 Watson Health Core operativne okoline

Ovlaštenje za Watson Health Core obuhvaća tri cloud operativne okoline s omogućenim zdravstvenim podacima, dizajnirano je da Klijentu omogući obradu zdravstvenih podataka:

- Pilot

  Nudi sandbox okolinu u kojoj Klijenti mogu razvijati i testirati aplikacije uz korištenje IBM SaaS-a. Pilot okolina ima implementirane sve HIPAA sigurnosne kontrole za obnavljanje od katastrofe, visoku dostupnost i sigurnosno kopiranje sustava zapisa.

- Proizvodna okolina

  Nudi potpunu okolinu u koju Klijenti mogu postaviti radna opterećenja zdravstvenih podataka. Proizvodna okolina je visoko dostupna s raspoređenim opterećenjem i osposobljena je za nadilaženje grešaka na lokaciji namijenjenoj za obnavljanje od katastrofe.

- Obnavljanje od katastrofe

  Nudi zrcalnu repliku proizvodne okolina i nalazi se na zasebnoj lokaciji centra podataka.

1.2 Razvoj aplikacija

IBM Watson Health Core omogućuje razvoj aplikacija i sigurno skupljanje podataka iz Klijentovih uređaja ili uređaja Klijentovih ovlaštenih korisnika. API-i nude programska sučelja i dokumentaciju, koju Klijentovi ovlašteni korisnici, uključujući Klijentove pružatelje usluga treće strane, mogu koristiti za razvoj aplikacija i razmjenu podataka s IBM SaaS-om. Korištenje API-a od strane Klijenta ili njegovih razvijatelja softvera podliježe poštivanju zahtjeva za razvoja API-a.

- REST API-i

  Watson Health Core nudi niz REST API-a i usluga za Watson Health Core platformu. API mogućnosti uključuju, ali nisu ograničene na, mehanizme pristupa spremištima podataka, uslugu sastavljanja podataka, upravljanje korisnicima i dnevnike revizije.

- Apple HealthKit i Apple ResearchKit

  Watson Health Core podržava integraciju sa istraživačkim studijama koje se temelje na Apple ResearchKit API građi za iOS i s Apple HealthKitom za hvatanje wellness podataka.

1.3 Uređivanje podataka

- Upravljanje pristancima

  Watson Health Core nudi građu za hvatanje pristanaka pacijenata ili učesnika studija i može sigurno spremiti zapis pristanka zasebno od korisničkih podataka kada se pojedinac prijavi putem Klijentove aplikacije s omogućenim pristankom.

- Maskiranje podataka

  Watson Health Core nudi mogućnost odvajanja identifikatora imena od strukturiranih korisničkih informacija. Watson Health Core prima podatke u cloud kroz programske API-e. API-i omogućuju odvajanje pacijenta ili identifikatora imena pojedinaca od ostatka korisničkih informacija, a spremaju se u zasebno šifrirano spremište podataka. Korisničkim podacima se dodjeljuje anonimizirani token, koji se može koristiti u budućem praćenju porijekla.

1.4 Usluge zdravstvenih podataka

Watson Health Core nudi skupljanje, pohranu i sinkroniziranje podataka, uključujući egzogene zdravstvene podatke i druge Osobne podatke, strukturirane i nestrukturirane.

- Konzumiranje podataka

  Watson Health Core nudi mogućnost konzumiranja podataka iz prijava pacijenata ili iz uređaja putem programskih API-a. Watson Health Core daje ovlaštenje svakom ovlaštenom pojedincu Klijenta za punjenje do 25 MB podataka u Health Core svake godine ugovornog razdoblja. Usluga prihvaća do 10 punjenja po pojedincu po danu.

- Operativni Data Lake

  Neobrađeni podaci Klijenta ili pacijenata se spremaju u Watson Health Core u svom originalnom obliku dok ne zatrebaju za analitiku i modeliranje.

- Extract Transform Load (ETL)(Izdvoji Pretvori Napuni)

  Podaci se pretvaraju u normalizirani format u operativnim podsustavima. Industrijski standardi bazirani na Enterprise Service Bus za zdravstvo omogućuje integraciju različitih aplikacija i protokola Klijenta.

- Data Reservoir

  Jednom kad su sastavljeni, podaci se premještaju u Data Reservoir. Watson Health Core koristi aspekte IBM Unified Data Model for Healthcare za normaliziranje poslovnih i tehničkih zdravstvenih informacija za njihovo korištenje u analitici.

- Master indeks osobe

  Watson Health nudi Master Data Management alate za konsolidiranje podataka iz višestrukih izvora i kreiranje longitudinalnog zapisa osobe (Longitudinal Person Record - LPR).

2. Fakultativne komponente

2.1 IBM Watson Health Core Terminology Service

Ovaj dodatak usluge omogućuje integraciju podataka i interoperabilnost između disparitetnih zdravstvenih sustava, nudi korištenje dosljedne kliničke terminologije u svim Watson Health Cloud aplikacijama. Ova usluga nudi funkcionalnu platformu za sve zadatke koje uključuju terminologije, sustave šifriranja i strukturirani sadržaj, poput:

- kreiranja novih sustava šifriranja;
- prijevod međunarodnih sustava šifriranja; i
- mapiranje između lokalnih šifarnika i međunarodnih standarda.

Dodatak B

IBM pruža sljedeći ugovor o dostupnosti razine usluge ("SLA") za IBM SaaS, kako je navedeno u PoE-u. SLA nije jamstvo. SLA je dostupan samo Klijentu i odnosi se samo na upotrebu u proizvodnim okolinama.

1. Odobrenja dostupnosti

Popust za dostupnost je primjenjiva samo na naknade za pretplatu za Pojedinačna ovlaštenja.

Klijent mora odjelu za pomoć IBM-ove tehničke podrške dostaviti prijavu podrške Ozbiljnosti 1 unutar 24 sata od trenutka kada prvi put shvati da postoji događaj koji ima utjecaja na dostupnost IBM SaaS-a. Klijent mora u razumnoj mjeri pomoći IBM-u kod bilo kakve dijagnoze problema i rješavanja.

Zahtjev kojim se podrški prijavljuje neispunjenje SLA-a mora se predati unutar tri radna dana nakon završetka ugovornog mjeseca. Naknada za važeći SLA zahtjev bit će odobrenje na budućem izdanom računu za IBM SaaS koje će se temeljiti na vremenu tijekom kojeg je nedostupan proizvodni sustav koji izvodi obradu za IBM SaaS ("Vrijeme prekida rada"). Vrijeme prekida rada mjeri se od trenutka kada Klijent prijavi događaj do trenutka ponovnog uspostavljanja IBM SaaS-a i ne uključuje vrijeme koje se odnosi na planirane ili najavljene prekide rada zbog održavanja; uzroke izvan IBM-ove kontrole; probleme sa sadržajem ili tehnologijom te dizajnima ili uputama Klijenta ili treće strane; nepodržane konfiguracije sustava i platforme ili druge Klijentove propuste; sigurnosne probleme koje uzrokuje Klijent ili Klijentovo testiranje sigurnosti. IBM će primijeniti najvišu primjenjivu naknadu na temelju kumulativne dostupnosti IBM SaaS-a u svakom ugovorenom mjesecu, kao što je prikazano u tablici navedenoj ispod. Ukupna naknada, uzevši u obzir bilo koji ugovoreni mjesec, ne može premašiti dvadeset posto jedne dvanaestine (1/12) godišnje naknade za IBM SaaS.

2. Razine usluge

Dostupnost IBM SaaS-a u ugovorenom mjesecu

Dostupnost tijekom ugovorenog mjeseca	**Naknada (% mjesečne naknade za Pojedinačnu pretplatu* za ugovoreni mjesec koji je predmet zahtjeva)**
< 99,95%	10%
< 99,0%	20%

* Ako je IBM SaaS kupljen preko IBM-ovog Poslovnog partnera, naknada mjesečne pretplate će se izračunavati prema tada važećoj navedenoj cijeni za IBM SaaS koja je na snazi za ugovoreni mjesec koji je predmet Zahtjeva, uz popust od 50%. IBM će Klijentu izravno omogućiti popust.

Dostupnost, izražena u postotku, računa se na sljedeći način: ukupan broj minuta u ugovorenom mjesecu minus ukupan broj minuta Vremena prekida rada u ugovorenom mjesecu, podijeljeno s ukupnim brojem minuta u ugovorenom mjesecu.

Primjer: 108 minuta ukupnog Vremena prekida tijekom ugovorenog mjeseca

43 200 ukupnih minuta u 30 dana ugovorenog mjeseca
- 108 minuta Vremena prekida
= 43 092 minuta

Ukupno 43 200 minuta

= 10% Odobrenja dostupnosti za 99.75% dostupnosti tijekom ugovorenog mjeseca

3. Isključenja

Ovaj SLA ne odnosi se na sljedeće slučajeve:

- Osim nadgledanja poslužitelja, SLA se ne odnosi na hostane virtualne strojeve za podršku prilagođenih ili Klijentovih aplikacija.
- Ako je Klijent prekršio bilo koje bitne obveze unutar obveza trenutnog ugovora.

Dodatak C

Ovaj Dodatak o sigurnosti i poslovnom kontinuitetu (ovaj "SBCA") definira određene zahtjeve i obveze IBM-a prilikom pružanja IBM SaaS-a Klijentu. Zahtjevi i obveze su ovdje navedeni kao dodatak navedenima u opisu načela sigurnosti podataka za IBM SaaS, a koji su dostupni su na http://www.ibm.com/cloud/data-security. Pojmovi napisani s velikim početnim slovom, a koji nisu ovdje definirani, bit će definirani u Ugovoru ili u Uvjetima upotrebe.

1. Program sigurnosti informacija

IBM ima implementirane unutarnje sigurnosne politike, standarde i procese koji se temelje na ISO 27001 građi i kontrolnim područjima. Osim što uređuju IBM korporativnu sigurnost organizacije, ove politike, standardi i procesi predmet su redovnih unutarnjih revizija.

IBM održava program sigurnosti informacija sastavljen od organizacijskih, operativnih, administrativnih, fizičkih i tehničkih zaštita, koje se brinu za obradu, pohranu i prijenos Klijentovog sadržaja, i njihov minimum je konzistentan sa zahtjevima ovog SBCA.

IBM, na zahtjev Klijenta, s Klijentom će podijeliti informacije o IBM Watson Health programu sigurnosti informacija tako da Klijent može razumno utvrditi je li i dalje pogodan, odgovarajući i učinkovit. IBM Watson Health program za sigurnost informacija povremeno će se ažurirati kako bi ostao u tijeku s općenito prihvaćenim industrijskim postupcima i zakonima primjenjivim na IBM.

2. Kontrole pristupa

IBM će otkriti Klijentov sadržaj samo svojim zaposlenicima, podugovaračima ili trećim stranama, kojima je pravovaljano potreban pristup takvom Klijentovom sadržaju radi obavljanja posla, kako bi omogućili IBM-u da ispuni svoje obveze prema Klijentu ili drugim osobama prema potrebi, pružanjem IBM SaaS-a u skladu s Mjerodavnim propisima, Ugovorom ili Pridruženim dokumentom, ako je primjenjivo. U slučaju kada je IBM poslovni suradnik Klijenta, IBM i Klijent će otkriti Osobne zdravstvene informacije samo u skladu s odredbama mjerodavnog ugovora s poslovnim suradnikom koji je sklopljen između strana.

IBM ima formalan, unutarnju proces upravljanja pristupom korisnika, po kojem se pristup korisnika formalno zahtijeva, odobrava nakon provjere identiteta i dodjeljuje onima koji moraju znati, pri čemu se koristi koncept najniže povlastice. Pristup Klijentovom sadržaju bit će ograničen samo na aktivne korisnika i aktivne korisničke račune. IBM ima formalan proces periodičnih provjera unutarnjeg pristupa aktivnih korisničkih računa.

IBM koristi sigurne protokole provjere identiteta korisnika, uključujući dodjelu jedinstvenih identifikacija i jakih lozinki za aktivne korisničke račune na sustavima, koji se koriste za pružanje usluga Klijentu u skladu s IBM-ovim korporativnim standardima i politikama sigurnosti:

a. Lozinke ne smiju biti defaultne lozinke dobavljača, a čuvaju se na lokaciji i/ili u formatu koji ne kompromitira sigurnost podataka koje čuvaju.

b. Prikaz i ispis lozinki mora bit maskiran, potisnut ili na drugi način skriven tako da neovlaštene strane nisu u mogućnosti vidjeti ih ili ih vratiti. Lozinke se ne smiju zapisivati ili hvatati tijekom unosa. Korisničke lozinke se ne smiju spremati kao jednostavan tekst.

c. Lozinke pojedinih tehnologija koje sačinjavaju IBM SaaS se biraju da bi se smanjio rizik vezan za ranjivost uslijed poznate duljine lozinke i moraju se dokumentirati.

d. Kada su potrebni interni, dijeljeni funkcijski ID-ovi s povlasticama radi operativnih razloga, IBM upravlja s dijeljenim, funkcijskim ID-ovima i/ili ID-ovima sustava koji zahtijevaju odjavu lozinki kako bi se zadržala odgovornost pojedinaca.

Vremenska prekoračenja neaktivnosti se postavljaju za sve sustave i aplikacije, u koje se pohranjuje Klijentov sadržaj.

Ako je potrebno, udaljeni pristup IBM-ovoj mreži, sustavima i aplikacijama u koje se pohranjuje Klijentov sadržaj bit će uspostavljen nakon zahtjeva Klijenta i formalnog odobrenja IBM-a, sva takva udaljena povezivanja bit će osigurana s jakim protokolima provjere identiteta i šifriranjem. Aktivnost udaljenog pristupa će se zapisivati u dnevnik i nadgledati.

U mjeri u kojoj isporuka IBM SaaS-a zahtijeva IBM-ov udaljeni pristup bilo kojem sustavu unutar Klijentove unutarnje mreže, sav takav udaljeni pristup izvodit će se isključivo korištenjem Klijentovih

sustava i protokola za sigurni udaljeni pristup, uz korištenje vjerodajnica pristupa koje IBM dobije od Klijenta. Udaljeni pristup Klijentovoj mreži uspostavit će se samo nakon zahtjeva IBM-a i Klijentovog odobrenja, u skladu s Klijentovim tada važećim politikama, koje će dostaviti IBM-u unaprijed. IBM-ovo korištenje Klijentovih unutarnjih mreža predmet je Klijentovog korištenja IT-a i politika sigurnosti, koje će dostaviti IBM-u unaprijed.

IBM implementira odvajanje dužnosti administracije sigurnosti, revizije pristupa i istrage sigurnosnih prekršaja.

Pohrana, hosting i obrada Klijentovog sadržaja koji je specifičan za klijenta se logički odvaja od ostalih klijenata kojima IBM pruža usluge. U slučajevima kada Klijent odobri korištenje dijeljene pohrane, hostinga ili radnog područja za obradu, IBM će uspostaviti procedure i zaštite u skladu sa zahtjevima navedenim u ovom SBCA, dizajnirane za sprječavanje neovlaštenog otkrivanja takvog Klijentovog sadržaja.

IBM implementira politike praznog stola/praznog ekrana kako bi bio siguran da Klijentov sadržaj nije ostavljen bez nadzora na nijednom javnom mjestu u bilo koje vrijeme.

3. Prijenos i šifriranje

IBM će poduzeti odgovarajuće mjere opreza prilikom prijenosa Klijentovog sadržaja (putem faksa, e-maila, kurira, itd.), osigurati će da se koriste ispravne kontakt informacije primatelja i prethodno dogovoriti s primateljem siguran primitak takvih informacija.

IBM koristi i zahtijevat će da IBM osoblje koristi odgovarajuće oblike šifriranja ili druge sigurne tehnologije svaki puta kada radi s obradom Klijentovog sadržaja, uključujući povezivanje radi prijenosa, komunikacije, udaljenog pristupa ili pohrane (uključujući pohranu sigurnosnih kopija) Klijentovog sadržaja. Na primjer, IBM će šifrirati, korištenjem odgovarajućeg industrijski standardnog šifriranja, sve zapise i datoteke koje sadrže Klijentov sadržaj:

a. pohranjen na IBM laptope, prijenosne uređaje ili prijenosne elektroničke medije, uključujući trake sigurnosnih kopija koje se prenose u skladišta koja nisu na lokaciji ureda;

b. pohranjen ili kojeg transportira IBM izvan Klijentovih ili IBM-ovih osiguranih ureda i objekata, isključujući kopije dokumenata na papiru;

c. kada ih IBM prenosi kroz javne mreže;

d. tijekom prijenosa iz IBM-ovih sustava Klijentu;

e. kada ih IBM prenosi bežičnim putem; i

f. kada ih IBM pohranjuje na poslužitelje i u baze podataka.

4. Sigurnost mreže

IBM koristi razumno suvremene verzije softvera za sigurnost sustava poput vatrozida, proxya, vatrozida i sučelja web aplikacija. Takav softver mora sadržavati zaštitu od zlonamjernog koda (malware) i razumno ažurne zakrpe i definicije virusa. U skladu s korporativnim standardima, antivirusni softver bit će instaliran na radne stanice, poslužitelje i povezane krajnje točke gdje je tehnički izvedivo, a softverom se upravlja prema korporativnim politikama putem unutarnjih rješenja upravljanja.

IBM nadgleda IBM SaaS kako bi otkrio i prepoznao sigurnosne incidente što ranije. IBM će održavati, minimalno, industrijski standardne alate za otkrivanje upada te procese sprječavanja, nadgledanja i odgovora, na način kojim će identificirati i unutarnje i vanjske ranjivosti i rizike, koji za posljedice mogu imati neovlašteno otkrivanje, zloporabu, promjenu ili uništavanje Klijentovog sadržaja ili informacijskih sustava, koji se koriste za isporuku usluga Klijentu.

IBM je pretplaćen na usluge inteligencije ranjivosti ili na savjetnike sigurnosti informacija i druge relevantne izvore, koji nude trenutne informacije o ranjivostima sustava. IBM izvodi redovne procjene ranjivosti i ispravljanja na svojim mrežama.

IBM nadgleda IBM SaaS kako bi otkrio, identificirao, suzbio i riješio sigurnosne incidente.

IBM provjerava dostupnost, integritet i učinkovitost infrastrukture sigurnosti mreža na kojima je dostupan IBM SaaS, kroz procese IBM upravljanja izdanjima.

5. Upravljanje incidentima i obavještavanje

IBM Watson Health timovi rade zajedno s IBM timom za odgovor na incidente cyber sigurnosti, to je globalni tim koji zaprima, istražuje i koordinira sigurnosnim incidentima vezanim za IBM ponude na

međunarodnoj razini, također implementira preventivne korake potrebne za smanjenje problema vezanih za sigurnost. "Sigurnosni incident" je uspješan neovlašteni pristup, korištenje, otkrivanje, modificiranje ili ometanje operacija sustava ili podataka u informacijskom sustavu koji IBM koristi za pružanje IBM SaaS-a. Ako se otkrije Sigurnosni incident (putem skeniranja rutina, uzbuna, događaja vezanih za pragove, itd.), IBM će informirati i obavijestiti Klijenta:

a. o potvrđenom Sigurnosnom incidentu u kojem sudjeluje Klijentov sadržaj čim je to praktično moguće, a nikako kasnije od 2 radna dana nakon istrage i potvrde takvog Sigurnosnog incidenta;

b. odmah po zahtjevu za pristup ili informacije o Klijentovom sadržaju od strane državnog službenika (uključujući bilo koju agenciju za zaštitu podataka ili za provedbu zakona) osim ako to zabranjuje zakon ili relevantni nalog; i

c. osim kako je dozvoljeno u odjeljku s naslovom Kontrole pristupa ovog SBCA, unaprijed o bilo kojem otkrivanju ili prijenosu ili pristupu Klijentovom sadržaju ili od treće strane.

6. Zapisivanje aktivnosti

IBM održava, u skladu s IBM-ovim politikama i postupcima i općenito prihvaćenim industrijskim postupcima, razumno nadgledanje sustava za neovlaštenu upotrebu ili pristup Klijentovim obrađenim podacima. Stvarni ili pokušani prekršaj prijave i prekršaj pristupa se zapisuje u dnevnik.

IBM održava zapise o svim zahtjevima za prijavu i dnevnike aktivnosti pristupa za sve sustave na koje se pohranjuju, kojima se pristupa, prenosi ili na kojima se obrađuju Klijentovi podaci i Zdravstveni podaci u trajanju koliko god to zahtijeva HIPAA i drugi Zakoni o podacima primjenjivi na IBM.

Dnevnici i izvještaji sadrže minimalno: (i) sve pokušaje prijave, bilo uspješne ili neuspješne, uključujući razumne identifikacijske informacije; (ii) sve promjene konfiguracije sustava i mreža, uključujući instalacije aplikacija, promjene upravljanja korisnicima i promjene na dozvolama pristupa datotekama; (iii) pokušaje pristupa resursima, bilo uspješne ili neuspješne, uključujući pokušaje pristupa nekoj datoteci, dijelu mreže, dnevniku ili drugom resursu; i (iv) preuzimanja podataka, uključujući tip sadržaja podataka i protokol pristupa koji je korišten za postizanje preuzimanja.

7. Razvoj softverskih aplikacija i upravljanje promjenama

IBM slijedi siguran razvoj aplikacija i postupke kodiranja, koji štite integritet proizvodnih aplikacija i povezanog izvornog koda od neovlaštenih i netestiranih promjena.

IBM slijedi proces upravljanja promjenama koji uključuje (a) zapisivanje formalnog odobrenja promjena i postupke vraćanja; i (b) odgovarajuće testiranje takvih promjena, uključujući testiranje prihvata od strane korisnika ako je prikladno, kao i testiranje sigurnosti.

IBM slijedi proces upravljanja zakrpama koji uključuje testiranje zakrpa prije instalacije na svim sustavima korištenim za pohranu, pristup i prijenos Klijentovog sadržaja ili se koriste za isporuku usluga Klijentu, uključujući IBM SaaS.

IBM zahtijeva da administratori sustava održavaju potpune, točne i ažurne informacije o konfiguracijama svih informacijskih sustava koji se koriste za spremanje, pristup ili prijenos Klijentovog sadržaja.

8. Fizička sigurnost i sigurnost okoline

IBM Watson Health Core platforma se postavlja na IBM SoftLayer infrastrukturu podataka. IBM SoftLayer održava fizičku i okolinsku sigurnost, kontrolu pristupa, kontrole i procese za zaštitu Klijentovih podataka od ljudskih, okolinskih i tehničkih povreda ili utjecaja.

Opći pristup objektima u kojima se nalazi IBM SaaS kontrolira se putem sustava pristupnih kartica. Televizijske kamere zatvorenog kruga (CCTV) su instalirane na svim lokacijama i prati ih osoblje sigurnosti. Izabrana pristupna vrata opremljena su s alarmima, a njih nadgleda osoblje sigurnosti.

Pristup kontroliranim područjima je ograničen putem korištenja pristupnih kartica i/ili dodatnih biometričkih identifikacija. Sve osobe bez ovlaštenog pristupa za kontrolirana područja moraju se prijaviti i prati ih osobe s odobreni pristupom kontroliranom području. Izlazi u slučaju opasnosti iz kontroliranih područja opremljeni su s alarmima, a osoblje sigurnosti nadgleda alarme. Periodične provjere funkcioniranja alarma se izvode, dokumentiraju i održavaju. Prava pristupa kontroliranim područjima se u potpunosti provjeravaju na kvartalnoj osnovi. Pristup kontroliranom području se povlači nakon otkaza zaposlenja.

Objekti su zaštićeni od okolinskih faktora poput vatre, vode i topline s vatrogasnim alarmima, aparatima za gašenje požara, dimnim alarmima te sustavima za suzbijanje i gašenje požara. Objekti su zaštićeni od

prekida dovoda električne energije ili kvarova putem sustava neprekidnih izvora napajanja (Uninterruptible Power Supply - UPS) i rezervnih generatora, koji se redovno održavaju i testiraju.

IBM SoftLayer informacije i izvještaji o usklađenosti mogu se pronaći na : http://www.softlayer.com/compliance.

9. Kontinuitet poslovnih operacija

IBM ima planove poslovnog kontinuiteta i obnavljanja od katastrofe, koji su dizajnirani za održavanje razine usluge u skladu s obvezama pod ovim Ugovorom. Planovi poslovnog kontinuiteta o obnavljanja od katastrofe periodički se ažuriraju i testiraju (najmanje jednom godišnje). IBM će implementirati sve razumne promjene poslovnog kontinuiteta i obnavljanja od katastrofe potrebne za održavanje usklađenosti s općenito prihvaćenim industrijskim postupcima, u svakom slučaju bez nerazumnog ometanja IBM SaaS-a ili proizvodne okoline koju koristi Klijent.

U slučaju katastrofe koja će učiniti IBM SaaS nedostupnim Klijentu, IBM će odmah obavijestiti Klijenta i aktivirati plan poslovnog kontinuiteta i/ili obnavljanja od katastrofe. Kada se proglasi katastrofa, cilj poslovnog kontinuiteta IBM SaaS-a je vratiti Klijentu pristup do IBM SaaS-a ovako: u slučaju prekida, Ciljano vrijeme obnavljanja ili Recovery Time Objective (RTO) za vraćanje IBM Watson Health proizvodne okoline je unutar 36 sati od proglašavanja katastrofe. Ciljana točka obnavljanja ili Recovery Point Objective (RPO) je najviše 24 sata gubitka Klijentovog sadržaja unutar proizvodne okoline. Određeni ciljevi Watson Health rješenja poslovnog kontinuiteta mogu se razlikovati.

IBM-ov pristup obnavljanju od katastrofe sastoji se od više centara podataka u geografski rasprostranjenim područjima.

Svi IBM SoftLayer centri podataka održavaju višestruka napajanja električnom energijom, fiber veze, namjenske generatore i rezervne akumulatore. Napravljeni su od industrijski vodećeg hardvera i opreme, nude najvišu razinu performansi, pouzdanosti i međuoperabilnosti. Sve uključene komponente centra podataka prolaze inspekciju, kao i n+1 redundantni resursi napajanja i hlađenja, kako bi se održala stabilnost centara podataka.

10. Usklađenost

IBM-ovi sigurnosni postupci se temelje na ISO 27001-27002. Ovi postupci pružaju strukturu kontrole za, ali se ne ograničavaju na, Analizu rizika, Fizičku sigurnost, Planiranje u kriznim okolnostima, Zaštitu informacija, Obrazovanje, Zaštitu podataka i Operacije.

IBM provodi reviziju radnji vezanih za sigurnosti i privatnost radi usklađenosti s IBM-ovim sigurnosnim postupcima.

IBM poštuje Zakone o podacima primjenjive na IBM u pravnim nadležnostima zemalja opsega.

Ispravno rukovanje Klijentovim povjerljivim informacijama također je obavezno u skladu s IBM-ovim smjernicama poslovnog ponašanja, koje su dužni pročitati svi zaposlenici (i to potvrditi) svake godine.

11. Razno

IBM će osigurati da odredbe ugovora s podugovaračima i/ili trećim stranama uključenim u isporuku IBM SaaS-a, štite Klijentov sadržaj najmanje onoliko koliko to čine odredbe ovog SBCA i primjenjivi Pridruženi dokument, u mjeri u kojoj su takve odredbe primjenjive na usluge koje će izvesti pojedini podugovarači i/ili treće strane.