IBM Watson Health Core

Pogoje uporabe ("pogoji uporabe") sestavljajo ti IBM-ovi pogoji uporabe – pogoji posebne ponudbe SaaS ("pogoji posebne ponudbe SaaS") in dokument IBM-ovi pogoji uporabe – splošni pogoji ("splošni pogoji"), ki so na voljo na naslednjem naslovu URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

V primeru navzkrižja med splošnimi pogoji in pogoji posebne ponudbe SaaS prevladajo slednji. Naročnik z naročilom ali uporabo ponudbe IBM SaaS oziroma dostopanjem do nje soglaša s pogoji uporabe.

Pogoje uporabe ureja veljavna IBM-ova pogodba International Passport Advantage oz. International Passport Advantage Express ali IBM International Agreement for Selected IBM SaaS Offerings, karkoli je ustrezno ("pogodba"), ki skupaj s pogoji uporabe predstavlja celotno pogodbeno dokumentacijo.

1. IBM SaaS

Ti pogoji posebne ponudbe SaaS veljajo za naslednje ponudbe IBM SaaS:

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

2. Metrike zaračunavanja

Ponudba IBM SaaS se prodaja v skladu z eno od naslednjih metrik zaračunavanja, kot je določeno v transakcijskem dokumentu:

a. **Dostop** je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Dostop je pravica do uporabe ponudbe IBM SaaS. Naročnik mora pridobiti eno samo pooblastilo za dostop, da lahko med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu, uporablja ponudbo IBM SaaS.

b. **Posameznik** je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Posameznik je ena sama stvar ali človek. Naročnik mora pridobiti zadostna pooblastila, da pokrije vse posameznike, ki jih ponudba IBM SaaS obdeluje ali upravlja med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

   Za namene te ponudbe IBM SaaS je posameznik oseba, naprava ali mobilna aplikacija, katere podatke upravlja ponudba IBM SaaS.

c. **Primerek** je merska enota, na podlagi katere je mogoče pridobiti ponudbo IBM SaaS. Primerek je dostop do posamezne konfiguracije ponudbe IBM SaaS. Naročnik mora pridobiti zadostna pooblastila za vsak primerek ponudbe IBM SaaS, do katerega je mogoče dostopati in ga uporabljati med meritvenim obdobjem, navedenim v naročnikovem dokazilu o upravičenosti ali transakcijskem dokumentu.

3. Stroški in zaračunavanje

Znesek, ki ga je treba plačati za ponudbo IBM SaaS, je naveden v transakcijskem dokumentu.

3.1 Delni mesečni stroški

Delni mesečni strošek, kot je naveden v transakcijskem dokumentu, se lahko oceni na osnovi sorazmernega deleža.

3.2 Zaračunavanje presežkov

Če naročnikova dejanska uporaba ponudbe IBM SaaS med meritvenim obdobjem presega pooblastila, navedena v dokazilu o upravičenosti, se naročniku zaračuna presežek, kot je opredeljeno v transakcijskem dokumentu.

4. Obdobje trajanja in možnosti podaljšanja

Naročniško obdobje na ponudbo IBM SaaS se začne z dnem, ko IBM obvesti naročnika, da ima na voljo dostop do pilotnega operacijskega okolja ponudbe IBM SaaS, kot je navedeno v naročilnici. Naročniško obdobje za pooblastila za posameznike se začne, ko IBM obvesti naročnika, da ima dostop do produkcijskega operacijskega okolja. V naročilnici bo navedeno, ali se naročnina na ponudbo IBM SaaS

podaljša samodejno, se nadaljuje na podlagi neprekinjene uporabe ali se konča ob izteku naročniškega obdobja.

Na podlagi samodejnega podaljšanja se bo naročnina na ponudbo IBM SaaS samodejno podaljševala za obdobje, navedeno v dokazilu o upravičenosti, razen če naročnik posreduje pisno obvestilo o prenehanju podaljšanja najmanj 90 dni pred iztekom naročniškega obdobja.

Na podlagi neprekinjene uporabe bo ponudba IBM SaaS neprestano na voljo iz meseca v mesec, dokler naročnik ne posreduje pisnega obvestila o odpovedi z 90-dnevnim odpovednim rokom. Ponudba IBM SaaS bo na voljo do konca koledarskega meseca po izteku takega 90-dnevnega obdobja.

5. Tehnična podpora

IBM bo omogočil dostop do Priročnika o podpori za IBM-ovo programsko opremo kot storitev (SaaS), ki vsebuje kontaktne informacije za tehnično podporo, časovne termine za vzdrževanje ter druge informacije in postopke. Kontaktne informacije za tehnično podporo in druge podrobnosti glede postopkov podpore so na voljo na naslovu: Priročnik o podpori za IBM-ovo programsko opremo kot storitev (SaaS): https://support.ibmcloud.com.

Tehnična podpora in preproste zahteve za konfiguracijo za ponudbo IBM SaaS so na voljo elektronsko. Tehnična podpora je vključena v ponudbo IBM SaaS in ni na voljo kot ločena, samostojna ponudba.

Pri poročanju o težavah v nobeno dokumentacijo ali informacije ne smejo biti vključeni nobeni osebni podatki, vključno z zaščitenimi zdravstvenimi podatki in občutljivimi osebnimi podatki.

6. Opredelitve

Veljavna zakonodaja pomeni vso zakonodajo, statute ali zakonodajne akte, pravila, predpise, direktive, odredbe, uredbe ali druge zahteve, ki jih izdajo vladne oblasti, ali vsakršne splošno priznane panožne standarde, ki veljajo za izpolnjevanje teh pogojev uporabe.

API pomeni aplikacijski programerski vmesnik, ki je nabor rutin, protokolov in orodij za gradnjo programske opreme. API določa način interakcije med komponentami strojne opreme, in API-je se uporablja pri programiranju komponent grafičnega uporabniškega vmesnika (GUI).

Pooblaščeni skrbnik je vsak naročnikov zaposleni, odobreni naročnikov pogodbenik, posameznik ali skupina, odgovorna za upravljanje vzdrževanja in zanesljivo delovanje platforme. Odgovornosti lahko vključujejo konfiguriranje, podporo ter upravljanje uporabnikov in računov. Skrbnik je lahko tudi klinični raziskovalec, odgovoren za vzpostavitev študije v sistemu Watson Health.

Pooblaščeni posameznik je vsaka pooblaščena oseba, mobilna aplikacija ali naprava, ki ima dostop do pravic za dostop za pošiljanje podatkov v sistem Watson Health Core. To lahko vključuje naročnika; ali naročnikove udeležence v študijah, stranke ali paciente.

Za naročnika zadevna zakonodaja o podatkih pomeni zakonodajo o podatkih, ki zadeva izvajanje naročnikovih obveznosti po tej pogodbi, povezanih dokumentih ter ustreznih opisih storitev, naročilnicah in dogovorih o obsegu del med pogodbenima strankama.

Naročnikovi podatki pomeni vse vnose podatkov v ponudbo IBM SaaS s strani naročnika, ki so lahko naročnikovi lastni podatki ali podatki, ki jih vnese naročnikova stranka ali tretja oseba ali pa jih v njunem imenu vnese naročnik, ter podatki iz zdravstvenih naprav drugih ponudnikov.

Zakonodaja o podatkih pomeni vso veljavno zakonodajo, ki zadeva zaščito, zasebnost ali varnost podatkov.

Subjekt podatkov pomeni prepoznanega posameznika ali posameznika, ki ga je mogoče prepoznati, na katerega se nanašajo osebni podatki.

Podano podatkovno središče pomeni eno ali več podatkovnih središč, ki so v transakcijskem dokumentu določena kot primarna podatkovna središča in podatkovna središča za obnovitev po hudi napaki, v katerih se izvaja naročnikov primerek ponudbe IBM SaaS, če je to ustrezno.

Zdravstveni podatki pomenijo vsi podatki ali informacije, vključno s slikami, ki veljajo za z zdravjem povezane osebne podatke.

Primeren za zdravstvene podatke v povezavi s ponudbo IBM SaaS pomeni zmožnost ponudbe IBM SaaS za izpolnjevanje veljavnih standardov glede varnosti in zasebnosti, zakonodaje ter predpisov v zadevnih sodnih pristojnostih za zdravstvene podatke, vključno z izvedbenimi specifikacijami iz dela 164, poddelov A in C, uredb o izvajanju Zakona o prenosljivosti in odgovornosti zdravstvenega zavarovanja –

HIPAA (kot ga spreminja zakon HITECH Act) in drugo veljavno zakonodajo o zdravstvenih podatkih, vendar ne pomeni, da IBM deluje kot poslovni sodelavec ali upravljavec podatkov.

HIPAA pomeni ameriški Zakon o prenosljivosti in odgovornosti zdravstvenega zavarovanja iz leta 1996, kot je bil spremenjen, med drugim z Zakonom o zdravstveni informacijski tehnologiji za ekonomsko in klinično zdravje ("HITECH") iz leta 2009, nekaterimi predpisi, razglašenimi na podlagi zakona HIPAA s strani Ministrstva Združenih držav za zdravje in človeške vire v razdelku 45 Zakonika zveznih predpisov (45 C.F.R.), v delih 160 in 164 ter nekaterih predpisih, razglašenih v skladu z zakonom HITECH.

Za IBM zadevna zakonodaja o podatkih pomeni zakonodajo o podatkih, ki zadeva izvajanje IBM-ovih obveznosti po tej pogodbi, povezanih dokumentih ter ustreznih opisih storitev, naročilnicah in dogovorih o obsegu del med pogodbenima strankama.

IBM-ovo osebje pomeni (a) IBM, njegove povezane družbe in njegove podizvajalce ter zaposlene iz vseh treh kategorij; in (b) vse zunanje dobavitelje; ki izvajajo storitve v imenu IBM-a v skladu s pogodbo in ustreznimi povezanimi dokumenti ali ki jim IBM drugače omogoči dostop do naročnikovih osebnih podatkov.

Zadevne države pomeni 28 držav članic Evropske unije in Švico ter države, ki jih lahko IBM občasno doda na ta seznam.

Osebni podatki ali **osebne informacije** pomeni podatke v kateremkoli mediju ali obliki zapisa, vključno z elektronskimi in papirnimi zapisi, ki se nanašajo na prepoznanega posameznika ali posameznika, ki ga je mogoče prepoznati, pri čemer je "posameznik, ki ga je mogoče prepoznati" nekdo, ki ga je mogoče neposredno ali posredno prepoznati, predvsem na podlagi identifikacijske številke oziroma enega ali več dejavnikov, značilnih za njegovo fizično, fiziološko, duševno, ekonomsko, kulturno ali družbeno identiteto.

Obdelati in izpeljanke iz te besede, na primer **obdelovanje** pomeni vsak postopek ali nabor postopkov, ki se samodejno ali ročno izvede na podatkih, na primer zbiranje, beleženje, organiziranje, shranjevanje, prilagajanje ali spreminjanje, pridobivanje, ogledovanje, uporaba, razkrivanje s prenosom, razširjanje ali drugi načini dajanja na voljo, poravnavanje ali kombiniranje, blokiranje, brisanje ali uničenje.

Obdelani podatki pomeni vse podatke, zaupne ali lastniške informacije ali gradiva, vključno z zdravstvenimi in osebnimi podatki, ki jih obdeluje IBM v skladu s pogodbo, povezanim dokumentom in/ali opisom storitev, naročilnico in/ali dogovorom o obsegu del.

Varnostni dogodek je opredeljen v dodatku o varnosti in poslovni kontinuiteti.

7. Upravljanje računa

Ponudba IBM SaaS je dostopna samo naročnikovim pooblaščenim uporabnikom ("**pooblaščeni skrbniki**" ali "**pooblaščeni posamezniki**"). Naročnik bo nadzoroval račune, pooblaščene za dostop do ponudbe IBM SaaS, ki lahko vključujejo pooblaščene aplikacije, naročnikovo osebje, naročnikove zunanje ponudnike in izvajalce ter nosi izključno odgovornost za (i) nadzorovanje vseh pooblaščenih uporabnikov, med drugim preverjanje pristnosti identitete vseh pooblaščenih uporabnikov; ter (ii) zagotavljanje, da do ponudbe IBM SaaS dostopajo le pooblaščeni uporabniki.

Pooblaščeni uporabniki, ki so naročnikove stranke, pacienti ali udeleženci študije, imajo lahko dostop le za namene nalaganja podatkov v ponudbo IBM SaaS, pri čemer ti pooblaščeni posamezniki ne bodo imeli nobenega drugega dostopa do ponudbe IBM SaaS.

8. Zasebnost

8.1 Splošne zahteve

Izmed pogodbenih strank je naročnik izključni upravljavec vseh naročnikovih osebnih podatkov, hkrati pa naročnik določa IBM kot obdelovalca podatkov. V skladu z veljavno zakonodajo o podatkih ima naročnik pravico, da IBM-u posreduje navodila za obdelavo naročnikovih osebnih podatkov s strani IBM-a.

IBM bo v okviru obsega, v katerem obdeluje naročnikove osebne podatke:

a. spoštoval vso za IBM zadevno zakonodajo o podatkih; in

b. ne bo mešal naročnikovih osebnih podatkov s podatki iz drugih virov, razen:

- za potrebe zagotavljanja ponudbe IBM SaaS, vendar za noben drug namen, če mu naročnik izrecno ne da drugačnih navodil; ali
- v skladu z določili teh pogojev uporabe in dodatka o varnosti in poslovni kontinuiteti.

Naročnik bo v okviru obsega, v katerem IBM obdeluje naročnikove osebne podatke:

a. spoštoval vso za naročnika zadevno zakonodajo o podatkih;

b. odgovoren za vso komunikacijo med naročnikom in naročnikovimi povezanimi družbami, pacienti, končnimi uporabniki, posamezniki, na katere se nanašajo podatki, in/ali ostalimi naročnikovimi tretjimi osebami;

c. podpisal pogodbe o obdelovanju podatkov s svojimi upravljavci, ki morajo potrditi IBM kot obdelovalca podatkov in njegovim podobdelovalcem dovoliti obdelovanje vseh naročnikovih osebnih podatkov; in

d. deloval kot edini kontakt za IBM ter nosil izključno odgovornost za interno koordiniranje, pregledovanje in predložitev navodil ali zahtev naročnikovih povezanih družb, ki so drugi upravljavci kot IBM. IBM ne bo dolžan informirati ali obvestiti nobene naročnikove povezane družbe, ki deluje kot upravljavec, če bo o tem predhodno informiral ali obvestil naročnika. IBM lahko zavrne vsakršna navodila, ki jih neposredno posreduje katerakoli naročnikova povezana družba, ki deluje kot upravljavec, vendar ni naročnik.

Od nobene pogodbene stranke se ne bo zahtevalo, da deluje v nasprotju z zakonodajo o podatkih, ki jo zadeva.

8.2 Naročnikove pravice nad podatki

Naročnik izjavlja in jamči, da (a) je lastnik podatkov, ki jih bo vnesel v ponudbo IBM SaaS, ali (b) je pridobil in bo ohranjal vse potrebne pravice, dovoljenja, soglasja in pooblastila, da bo IBM-u podelil pravico do uporabe in razkritja naročnikovih podatkov ter dostop do njih v skladu z določili v teh pogojih uporabe ali pogodbi ali kot je drugače potrebno za IBM-ovo zagotavljanje ponudbe IBM SaaS. Naročnik poleg tega izjavlja in jamči, da se bodo naročnikovi podatki nanašali izključno na (a) posameznike s prebivališčem v Združenih državah, pri čemer se bodo vnašali v ponudbo IBM SaaS v podatkovnem središču v Združenih državah, ali (b) posameznike s prebivališčem v eni ali več zadevnih državah, pri čemer se bodo vnašali v ponudbo IBM SaaS v podanih podatkovnih središčih.

8.3 Podatkovne storitve in dolžnosti

a. Naročnik soglaša, da bo izvajal analitiko naročnikovih podatkov, oziroma to zahteval od IBM-a, v povezavi z dejavnostmi, ki štejejo za naročnikove "zdravstvene operacije" ali "raziskovanje", kot sta izraza definirana v zakonu HIPAA in/ali podobnih določilih druge veljavne zakonodaje o podatkih, ter da bo naročnik uporabljal naročnikove podatke, oziroma enako zahteval od IBM-a, v skladu z vsemi relevantnimi zahtevami (npr. ugotovitvami ali odpovedmi ameriškega Institucionalnega nadzornega odbora – IRB) po tej in vsakršni drugi za naročnika zadevni zakonodaji o podatkih.

b. Naročnik nosi izključno odgovornost, da pridobi vse morebitne registracije, soglasja, pooblastila in dovoljenja, ki so zahtevana po zakonodaji, ki zadeva naročnika, v vseh zadevnih državah, med drugim vključno z zakonom HIPAA in vsakršno drugo veljavno zakonodajo, pravilih in predpisih o zasebnosti in varnosti podatkov, da bodo naročnikovi podatki tako s strani naročnika kot tudi IBM-a in IBM-ovih odobrenih podizvajalcev vneseni v ponudbo IBM SaaS ter uporabljani in razkriti v skladu s temi pogoji uporabe in pogodbe. IBM ne bo dolžan spremljati, kdaj so take registracije, soglasja, pooblastila in dovoljenja prejeta ali zahtevana.

c. Naročnik nosi izključno odgovornost, da zagotovi, da so vsi naročnikovi podatki, vneseni v ponudbo IBM SaaS, omejeni na podatke o posameznikih s prebivališčem v Združenih državah ali ustrezni zadevni državi.

d. IBM bo zagotavljal centre za podporo z osebjem, ki bo seznanjeno z zakonom HIPAA in drugo za IBM zadevno zakonodajo o podatkih, za podatke iz zadevnih držav.

8.4 Varnostni ukrepi in varnostni dogodki

a. IBM bo uvedel, vzdrževal in spoštoval tehnične in organizacijske ukrepe (vključno z organizacijskimi procesi in postopki ter morebitnimi posebnimi varnostnimi obveznostmi, ki jih določajo ali navajajo te pogoji uporabe in dodatek o varnosti in poslovni kontinuiteti za varovanje naročnikovih osebnih podatkov pred nepooblaščeno uporabo ali dostopom, nenamerno izgubo, poškodbo, spremembo, uničenjem, krajo ali nepooblaščenim razkritjem.

b. Če IBM izve za varnostni dogodek (kot je opredeljen v dodatku o varnostni in poslovni kontinuiteti), povezan z naročnikovimi obdelanimi podatki, bo IBM o tem obvestil naročnika v skladu z določili dodatka o varnosti in poslovni kontinuiteti ter za IBM zadevno zakonodajo o podatkih, to obvestilo bo vključevalo informacije o vseh znanih vplivih na naročnika ali morebitne posameznike, na katere se nanašajo podatki, vpletenih v tak varnostni dogodek, ter izvedene ali predlagane popravne ukrepe s strani IBM-a.

8.5 Prejem poizvedb in pritožb

IBM bo naročnika pisno obvestil nemudoma, vendar, kadar to dovoljuje za IBM zadevna zakonodaja o podatkih, najpozneje v petih (5) delovnih dneh po tem, ko vodja za zasebnost podatkov za IBM Watson Health prejme poizvedbo, vprašanje ali pritožbo, ki jo je prejel IBM v zvezi z naročnikovimi osebnimi podatki od:

a. kateregakoli posameznika, na katerega se nanašajo osebni podatki, ki jih obdeluje IBM. Naročnik se bo odzval na vsako tako zahtevo posameznikov, na katere se nanašajo podatki, IBM pa bo spoštoval naročnikova razumna navodila za pomoč naročniku pri odzivanju na take zahteve. Če tako zahteva za IBM zadevna zakonodaja, se bo IBM neposredno odzval na take zahteve, pod pogojem, da IBM vnaprej obvesti naročnika o takih odzivih in se razumno usklajuje z naročnikom glede oblike in vsebine takega odziva, če je to dovoljeno po za IBM zadevni zakonodaji ali drugače mogoče;

b. kateregakoli sodnega ali regulatornega organa, v zvezi z IBM-ovim obdelovanjem vsakršnih naročnikovih osebnih podatkov, pod pogojem, da se IBM lahko odzove na take zahteve, ki jih prejme od vladnih agencij, s sodnim pozivom ali podobnim pravnim dokumentom, ki od IBM-a zahteva razkritje, ali kot drugače zahteva veljavna zakonodaji o podatkih, pod pogojem, da IBM naročnika vnaprej obvesti o takem razkritju in se z njim razumno usklajuje glede oblike in vsebine takega odziva, če je to dovoljeno po zakonodaji ali drugače mogoče.

8.6 Obdelovanje naročnikovih osebnih podatkov

IBM bo razkril naročnikove osebne podatke le tistemu IBM-ovemu osebju, ki bo IBM-u pomagalo pri zagotavljanju storitev.

IBM bo izpolnil vsako naročnikovo razumno zahtevo za dopolnitev, popravek, izbris ali blokado naročnikovih osebnih podatkov v skladu z veljavno zakonodajo.

Na zahtevo katerekoli od pogodbenih strank bodo IBM, naročnik ali njune povezane družbe sklenili standardne pogodbe, ki jih predpisuje zakonodaja za varovanje naročnikovih osebnih podatkov. Stranki soglašata (in zagotavljata, da soglašajo tudi njune povezane družbe), da bodo za zahtevke med pogodbenima strankama v takih dodatnih pogodbah veljale omejitve in zavrnitve odgovornosti iz te pogodbe. Pogodbeni stranki bosta sodelovali pri sklepanju in spoštovanju nadaljnjih sporazumno dogovorjenih določil ali pogodb (ali zagotavljanju, da taka določila ali pogodbe sklenejo njune povezane družbe), kot je morda zahtevano po veljavni zakonodaji o podatkih.

8.7 Vrnitev naročnikovih osebnih podatkov

Ob izteku ali prenehanju pogodbe bo IBM in IBM-ovo osebje nehalo uporabljati ali obdelovati vsakršne naročnikove lastniške informacije in vsakršne naročnikove osebne podatke ter IBM bo na naročnikovo izbiro in zahtevo:

a. v obliki zapisa in mediju za shranjevanje, ki ga lahko naročnik razumno zahteva, nemudoma vrnil vse naročnikove lastniške informacije in naročnikove osebne podatke, ki jih IBM elektronsko shranjuje, ter po naročnikovi potrditvi prejema izbrisal ali uničil naročnikove lastniške informacije in naročnikove osebne podatke, vključno s kopijami in varnostnimi kopijami, oziroma jih drugače trajno spremenil tako, da jih ne bo mogoče prebrati ali dešifrirati. IBM lahko zaračuna stroške medijev za shranjevanje in nekaterih dejavnosti, ki jih izvede na naročnikovo zahtevo (na primer zagotovitev naročnikovih lastniških informacij in naročnikovih osebnih podatkov v posebni obliki zapisa ali uničenje naročnikovih lastniških informacij in naročnikovih osebnih podatkov na poseben način); in

b. neposredno uničil ali drugače trajno spremenil naročnikove lastniške informacije in naročnikove osebne podatke, vključno s kopijami in varnostnimi kopijami, tako da jih ne bo mogoče prebrati ali dešifrirati.

8.8 Pogodba o poslovnem sodelovanju

Kot je ustrezno in zahtevano po zakonu HIPAA, bosta IBM in naročnik sklenila pogodbo o poslovnem sodelovanju ("BAA"), ki bo urejala obveznosti IBM-a kot naročnikovega poslovnega sodelavca pri zagotavljanju ponudbe IBM SaaS. Brez omejevanja IBM-ovih izrecnih obveznosti po tej pogodbi in, če je ustrezno, po pogodbi o poslovnem sodelovanju naročnik soglaša in potrjuje, da je dolžan ugotoviti veljavnost in zagotavljati skladnost z vso veljavno zakonodajo in licenčnimi zahtevami, ki veljajo za naročnikovo uporabo ali druge dejavnosti v zvezi s ponudbo IBM SaaS (vključno z uporabo ali drugimi dejavnostmi pooblaščenih uporabnikov).

8.9 Dodatek o obdelovanju podatkov iz Evropske unije

Če naročnik IBM-u naroči obdelovanje osebnih podatkov iz Evropske unije, bosta IBM in naročnik sklenila Dodatek o obdelovanju podatkov, če je ustrezno, vključno s standardnimi klavzulami EU ter z odstranjenimi izbirnimi klavzulami.

9. Dodatni pogoji ponudbe IBM SaaS

9.1 Varnost

Ta ponudba IBM SaaS je skladna z IBM-ovimi načeli glede varnosti podatkov in zasebnosti za IBM-ovo programsko opremo kot storitev, ki so na voljo na spletnem mestu http://www.ibm.com/cloud/data-security, dodatnimi spodaj navedenimi določili ter dodatkom o varnosti in poslovni kontinuiteti k tem pogojem uporabe. Morebitne spremembe IBM-ovih načel glede zaščite podatkov in zasebnosti ne bodo zmanjšale stopnje varnosti za ponudbo IBM SaaS.

IBM Watson Health Core uporablja varnostne pravilnike, standarde in procese, ki temeljijo na standardu ISO 27001, kot je podrobneje opisano v opisu varnosti. Rešitev uporablja naslednje od varnostnih zmožnosti:

a. Varna operacijska območja

   IBM Watson Health Core uporablja celovito obrambno strategijo na več varnostnih območjih za upravljanje integracijskih točk v oblaku, kot je nalaganje podatkov in razvijanje aplikacij po meri.

b. Šifriranje

   Vsi naročnikovi podatki so šifrirani v mirovanju in v gibanju. Vsi podatki, ki se prenašajo v storitev IBM Watson Health Core in iz nje, so šifrirani. Storitev v skupni rabi zagotavlja upravljanje šifrirnih ključev. Naročnik je odgovoren za celotno omrežno povezljivost in kakovost med storitvijo IBM Watson Health Service in pooblaščenim naročnikovim strežnikom.

c. Varnostno nadziranje dogodkov

   IBM uporablja svojo platformo za obveščanje o varnosti za upravljanje varnostnih informacij in dogodkov, upravljanje dnevnikov, forenziko dogodkov, zaznavanje groženj ter upravljanje ranljivosti.

d. Upravljanje identitet

   - Watson Health Core podpira ponudnike identitet z odprtimi standardi za obsežne populacije pacientov in uporabnikov, ki uporabljajo OpenID Connect.
   - Za populacije uporabnikov, katerih ponudnik identitet je IBM, Watson Health Core za preverjanje pristnosti uporablja ustrezne imeniške storitve in zmožnosti upravljanja identitet.

e. Strogo preverjanje pristnosti in dostop na podlagi vlog

   - Watson Health Core podpira preverjanje pristnosti prek mehanizma SAML, ki naročnikom omogoča integracijo njihove enotne prijave (SSO) ali imeniških storitev.
   - Watson Health Core za upravljanje varnostnih pravilnikov po potrebi uporablja rešitev za upravljanje dostopa in povezane komponente.
   - Watson Health Core podpira dvostopenjsko preverjanje pristnosti na podlagi programske opreme.
   - Watson Health Core po potrebi zagotavlja nadzor dostopa na podlagi vlog; Watson Health Core podpira konfiguriranje študij, uporabniških profilov, vlog in uporabniških skupin prek aplikacijskih programerskih vmesnikov ("API" ali "API-ji"), ki omogočajo dostop na podlagi vlog.

9.2 Piškotki

Naročnik se zaveda in soglaša, da lahko IBM kot del običajnega delovanja in podpore za ponudbo IBM SaaS prek sledenja in drugih tehnologij zbira naročnikove osebne podatke (naročnikovih zaposlenih in pogodbenikov) v zvezi z uporabo ponudbe IBM SaaS. IBM s tem pridobiva statistiko o uporabi in podatke o učinkovitosti ponudbe IBM SaaS z namenom izboljšanja uporabniške izkušnje in/ali prilagajanja interakcije z naročnikom. Naročnik potrjuje, da je/bo pridobil soglasje, ki IBM-u dovoljuje obdelavo zbranih osebnih podatkov za navedeni namen v skladu z veljavno zakonodajo znotraj IBM-a, drugih IBM-ovih družb in njihovih podizvajalcev ne glede na to, kje IBM in njegovi podizvajalci poslujejo. IBM bo upošteval zahteve naročnikovih zaposlenih in pogodbenikov za dostop, posodobitev, spremembo ali izbris njihovih zbranih osebnih podatkov.

9.3 Izpeljane lokacije prejemanja storitev

Kadar je to ustrezno, davki temeljijo na eni ali več lokacijah, ki jih naročnik navede kot lokacije prejemanja storitev iz ponudbe IBM SaaS. IBM obračuna davke na podlagi poslovnega naslova, ki ga je naročnik navedel pri naročilu ponudbe IBM SaaS kot primarno lokacijo uporabe storitev, razen če naročnik IBM-u posreduje dodatne podatke o tem. Naročnik je dolžan posodabljati take podatke in IBM-u sporočiti morebitne spremembe.

9.4 Neprekinjena dobava

Naročnik je upravičen do zmožnosti in izboljšav rešitve, ki jih IBM namesti v model za neprekinjeno dobavo v oblaku.

9.5 Varnostno kopiranje in obnovitev

IBM Watson Health Core zagotavlja varnostno kopiranje naročnikovih podatkov v produkcijskem okolju (vključno s podatkovnimi jezeri (Data Lake) in podatkovnimi zbiralniki (Data Reservoir)) v zadnje znano ustrezno stanje za namene obnovitve storitve v primeru sistemske napake.

9.6 Visoka razpoložljivost

Komponente storitve IBM Watson Health Core v produkcijskem okolju so uvedene v visoko razpoložljivih konfiguracijah, z gručenjem strežnikov baz podatkov zaradi redundance z namenom distribuiranja delovnih obremenitev in odpravljenja kritičnih točk odpovedi.

9.7 Obnovitev po hudi napaki

IBM-ov pristop do obnovitve po hudi napaki zajema več podatkovnih središč na različnih geografskih območjih za doseganje ciljne poslovne kontinuitete za svoje produkcijsko okolje, kot sledi:

- Ciljni čas obnovitve (RTO) – v 36 urah po razglasitvi hude napake
- Ciljna točka obnovitve (RPO) – največ 24 ur izgube naročnikove vsebine

9.8 Meritvena orodja

Ponudba IBM SaaS uporablja sintetično nadzorno rešitev za nadzorovanje, merjenje in poročanje o razpoložljivosti ali izpadih glede na zagotovljene ravni storitev. Ta rešitev simulira in spremlja uporabniške odzive in izkušnje na globalni ravni – tako za statično razpoložljivost kot za transakcije.

Ponudba IBM SaaS uporablja tudi notranji nadzorni sistem za metrike, dogodke in opozorila v celotni rešitvi.

9.9 Publiciteta

Naročnik soglaša, da lahko IBM naročnika v oglaševalskih ali tržnih komunikacijah javno imenuje kot naročnika na ponudbo IBM SaaS.

Dodatek A

1. IBM Watson Health Core

IBM Watson Health Core je platforma kot storitev (PaaS), primerna za zdravstvene podatke, razvojna platforma in operacijski podsistem za shranjevanje, organiziranje ter obdelovanje zaščitenih zdravstvenih podatkov, kot so opredeljeni po zakonu HIPAA, in drugih zdravstvenih podatkov v skladu z za IBM zadevno zakonodajo o podatkih v podatkovnih središčih, ki so v lasti IBM-a ali jih upravlja IBM. Naročnik mora pridobiti ustrezna pooblastila za IBM Watson Health Core in IBM Watson Health Core Access, če želi omogočiti spodaj opisane funkcije in zmožnosti.

1.1 Operacijska okolja Watson Health Core

Pooblastilo za Watson Health Core združuje tri operacijska okolja v oblaku, primerna za zdravstvene podatke, ki naročniku omogočajo obdelovanje zdravstvenih podatkov:

- Pilotno okolje

  Zagotavlja preizkusno okolje, v katerem lahko naročniki razvijajo in preizkušajo aplikacije, ki jih zgradijo prek ponudbe IBM SaaS. Pilotno okolje uporablja vse varnostne kontrolnike iz Zakona o prenosu zdravstvenih podatkov in odgovornosti (HIPAA), razen obnovitve po hudi napaki, visoke razpoložljivosti in varnostnega kopiranja evidenčnih sistemov.

- Produkcijsko okolje

  Zagotavlja celovito okolje, v katerem lahko naročniki namestijo delovne obremenitve zdravstvenih podatkov. Produkcijsko okolje je visoko razpoložljivo okolje z uravnoteženimi obremenitvami in lahko ob izpadu preklopi na lokacijo za obnovitev po hudi napaki.

- Obnovitev po hudi napaki

  Zagotavlja zrcalno repliko produkcijskega okolja; nahaja se na ločeni lokaciji podatkovnega središča.

1.2 Razvoj aplikacij

IBM Watson Health Core omogoča razvijanje aplikacij in varno zbiranje podatkov iz naročnikovih naprav ali naprav naročnikovih pooblaščenih uporabnikov. API-ji zagotavljajo programske vmesnike in dokumentacijo, kar lahko naročnikovi pooblaščeni uporabniki, vključno z naročnikovimi zunanjimi ponudniki storitev, uporabljajo za razvijanje aplikacij in izmenjevanje podatkov prek ponudbe IBM SaaS. Naročnik in njegovi razvijalci morajo uporabljati API-je v skladu z zahtevami razvijalcev API-jev.

- API-ji REST

  Watson Health Core zagotavlja niz API-jev in storitev REST za platformo Watson Health Core. Zmožnosti API-jev med drugim vključujejo mehanizme za dostop do podatkovnih repozitorijev, storitve za upravljanje podatkov, upravljanje uporabnikov in dnevnike nadzora.

- Apple HealthKit in Apple ResearchKit

  Watson Health Core podpira integracijo z ogrodjem za API-je Apple ResearchKit za raziskovalne študije v sistemu iOS in z Apple HealthKit za zajem podatkov o splošnem počutju.

1.3 Vodenje podatkov

- Upravljanje soglasij

  Watson Health Core zagotavlja ogrodje za zajem soglasij pacientov ali udeležencev študij in lahko varno shrani evidenco soglasij, razen podatkovnih obremenitev, kadar se posameznik prijavi prek naročnikove aplikacije, ki omogoča soglasja.

- Maskiranje podatkov

  Watson Health Core zagotavlja zmožnost ločevanja imenskih identifikatorjev od strukturiranih podatkovnih obremenitev. Watson Health Core prejema podatke v oblaku prek programskih API-jev. API-ji omogočajo ločevanje imenskih identifikatorjev pacientov ali posameznikov od ostalih podatkovnih obremenitev, ki se shranjujejo v ločeni šifrirani shrambi podatkov. Podatkovni obremenitvi je dodeljen anonimiziran žeton, ki ga je mogoče pozneje uporabiti za spremljanje izvora.

1.4 Storitve za zdravstvene podatke

Watson Health Core zagotavlja zbiranje, shranjevanje ter sinhroniziranje strukturiranih in nestrukturiranih podatkov, vključno z zunanjimi zdravstvenimi podatki in drugimi osebnimi podatki.

- Vnašanje podatkov

  Watson Health Core zagotavlja zmožnost vnašanja podatkov iz aplikacij ali naprav pacientov prek programskih API-jev. Watson Health Core vsakega od naročnikovih pooblaščenih posameznikov pooblašča za nalaganje do 25 MB podatkov v storitev Health Core v vsakem letu pogodbenega obdobja. Storitev omogoča do 10 nalaganj na posameznika na dan.

- Operacijsko "podatkovno jezero"

  Neobdelani podatki naročnikov ali pacientov se shranjujejo v storitvi Watson Health Core v izvorni obliki, dokler se ne uporabijo za analitiko in modeliranje.

- Ekstrahiraj, pretvori, naloži (Extract Transform Load – ETL)

  Podatki so pretvorjeni v normalizirano obliko zapisa znotraj operacijskega podsistema. Arhitekturni model Enterprise Service Bus za zdravstvo, ki temelji na panožnim standardih, omogoča integracijo v različnih naročnikovih aplikacijah in protokolih.

- Zbiralnik podatkov

  Ko se podatki organizirajo, so premaknjeni v zbiralnik podatkov. Watson Health Core uporablja dele storitve IBM Unified Data Model for Healthcare za normalizacijo poslovnih in tehničnih zdravstvenih podatkov, namenjenih uporabi v analitiki.

- Matični indeks oseb

  Watson Health zagotavlja orodja za upravljanje matičnih podatkov za namene konsolidiranja podatkov iz različnih virov, iz katerih se ustvari longitudinalni zapis o osebi (LPR).

2. Izbirne funkcije

2.1 IBM Watson Health Core Terminology Service

Ta dodatna storitev omogoča integracijo podatkov in skupno uporabnost med različnimi zdravstvenimi sistemi, kar zagotavlja dosledno uporabo klinične terminologije v vseh aplikacijah Watson Health Cloud. Ta storitev zagotavlja funkcionalno platformo za vsa opravila, ki vključujejo terminologijo, kodne sisteme in strukturirano vsebino, na primer:

- ustvarjanje novih kodnih sistemov;
- prevajanje mednarodnih kodnih sistemov; in
- preslikave med lokalnimi kodnimi seznami in mednarodnimi standardi.

Dodatek B

IBM za ponudbo IBM SaaS zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost ("SLA"), kot je navedeno v dokazilu o upravičenosti. Pogodba o ravni storitev ne zagotavlja jamstva. Pogodba o ravni storitev je na voljo samo naročniku in velja samo za uporabo v produkcijskih okoljih.

1. Dobropisi za razpoložljivost

Rabati za razpoložljivost veljajo le za naročnino za pooblastila za posameznike.

Naročnik mora pri IBM-ovi službi za tehnično podporo vložiti prijavo za podporo ravni resnosti 1, in sicer v 24 urah od trenutka, ko naročnik ugotovi, da je dogodek vplival na razpoložljivost ponudbe IBM SaaS. Naročnik mora razumno pomagati IBM-u pri kakršnemkoli diagnosticiranju in razreševanju težav.

Naročnik mora predložiti zahtevek za podporo zaradi neizpolnjevanja pogodbe o ravni storitev v treh delovnih dneh po koncu pogodbenega meseca. Nadomestilo za upravičen zahtevek na podlagi pogodbe o ravni storitev (SLA) bo priznano kot dobropis pri naslednjem računu za ponudbo IBM SaaS na podlagi obdobja, v katerem obdelovanje produkcijskega sistema za ponudbo IBM SaaS ni na voljo ("nerazpoložljivost"). Nerazpoložljivost se meri od trenutka, ko je naročnik poročal o dogodku, do trenutka, ko je bilo obnovljeno delovanje ponudbe IBM SaaS, ter ne vključuje časa, ki je povezan z izpadom zaradi načrtovanega ali napovedanega vzdrževanja; zaradi vzrokov, ki so zunaj IBM-ovega nadzora; zaradi težav z vsebino, tehnologijo, zasnovo ali navodili naročnika ali tretje osebe; zaradi nepodprtih sistemskih konfiguracij in platform ali zaradi drugih napak naročnika; ali zaradi varnostnega dogodka, ki ga je povzročil naročnik ali naročnikovo preizkušanje varnosti. IBM bo uporabil najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti ponudbe IBM SaaS v vsakem pogodbenem mesecu, kot je prikazano v spodnji tabeli. Celotno nadomestilo za posamezni pogodbeni mesec ne sme presegati 20 odstotkov ene dvanajstine (1/12) letnega zneska za ponudbo IBM SaaS.

2. Ravni storitve

Razpoložljivost ponudbe IBM SaaS v pogodbenem mesecu

Razpoložljivost v pogodbenem mesecu	**Nadomestilo (odstotek mesečne naročnine za posameznika* za pogodbeni mesec, na katerega se nanaša zahtevek)**
< 99,95 %	10 %
< 99,0 %	20 %

* Če je naročnik ponudbo IBM SaaS pridobil od IBM-ovega poslovnega partnerja, se mesečna naročnina obračuna na podlagi takrat veljavne cene za ponudbo IBM SaaS, ki velja za pogodbeni mesec, na katerega se nanaša zahtevek, pri čemer bo upoštevan 50-odstotni popust. IBM bo rabat omogočil neposredno naročniku.

Razpoložljivost, izražena v odstotkih, se izračuna kot: (a) skupno število minut v pogodbenem mesecu, zmanjšano za (b) skupno število minut nerazpoložljivosti v pogodbenem mesecu, deljeno s (c) skupnim številom minut v pogodbenem mesecu.

Primer: skupaj 108 minut nerazpoložljivosti v pogodbenem mesecu

Skupaj 43.200 minut v 30-dnevnem pogodbenem mesecu - 108 minut nerazpoložljivosti = 43.092 minut _____ Skupaj 43.200 minut	= 10-odstotni dobropis za razpoložljivost za 99,75-odstotno razpoložljivost v pogodbenem mesecu

3. Izjeme

Ta pogodba o ravni storitev ne velja za naslednje:

- Z izjemo nadzorovanja strežnikov ta pogodba o ravni storitev ne velja za gostujoče navidezne naprave za podporo aplikacij po meri ali naročnikovih aplikacij.
- Če je naročnik kršil katerokoli bistveno obveznost po trenutnih obveznostih iz pogodbe.

Dodatek C

Ta dodatek o varnosti in poslovni kontinuiteti ("SBCA") določa nekatere IBM-ove zahteve in obveznosti pri zagotavljanju ponudbe IBM SaaS naročniku. Zahteve in obveznosti, navedene v nadaljnjem besedilu, veljajo poleg tistih, ki so navedene v opisu načel za varnost podatkov za IBM SaaS, ki so na voljo na spletnem mestu http://www.ibm.com/cloud/data-security. Izrazi, ki niso opredeljeni v nadaljnjem besedilu, so opredeljeni v pogodbi ali pogojih uporabe.

1. Program za varnost podatkov

IBM ima interne varnostne pravilnike, standarde in postopke, ki temeljijo na standardu ISO 27001, ter nadzorna območja. Te pravilnike, standarde in postopke upravlja IBM-ova organizacija za poslovno varnost, poleg tega pa jih redno preverjajo notranji revizorji.

IBM vzdržuje program za varnost podatkov z operacijskimi, administrativnimi, fizičnimi in tehničnimi varnostnimi mehanizmi, ki urejajo obdelovanje, shranjevanje in prenos naročnikove vsebine ter morajo biti skladni vsaj z zahtevami tega dodatka o varnosti in poslovni kontinuiteti.

IBM bo na naročnikovo zahtevo naročniku posredoval informacije o programu za varnost podatkov IBM Watson Health, da bo lahko naročnik razumno ugotovil, ali je še naprej ustrezen, primeren in učinkovit. Program za varnost podatkov IBM Watson Health bo občasno posodobljen z upoštevanjem sodobnih splošno priznanih panožnih praks in za IBM zadevne zakonodaje.

2. Nadzor dostopa

IBM bo naročnikovo vsebino razkril le svojim zaposlenim, podizvajalcem ali tretjim osebam, ki imajo legitimno poslovno potrebo za dostop do naročnikove vsebine z namenom sodelovanja z IBM-om pri izpolnjevanju njegovih obveznosti do naročnika ali drugih oseb, kot je zahtevano, za zagotavljanje ponudbe IBM SaaS v skladu z veljavno zakonodajo, pogodbo ali povezanim dokumentom, kot je ustrezno. Če je IBM naročnikov poslovni sodelavec, bosta IBM in naročnik razkrila osebne zdravstvene podatke le skladno z določili veljavne pogodbe o poslovnem sodelovanju, sklenjene med pogodbenima strankama.

IBM ima formalen interni postopek za upravljanje uporabniškega dostopa, znotraj katerega je treba uporabniški dostop formalno zahtevati, odobriti po preverjanju pristnosti identitete in podeliti na podlagi potrebe po seznanjenju, za kar se uporablja načelo najmanjšega privilegija. Dostop do naročnikove vsebine bo omejen in omogočen le aktivnim uporabnikom in aktivnim uporabniškim računom. IBM ima formalen postopek za redno ponovno preverjanje internega dostopa aktivnih uporabniških računov.

IBM uporablja varne protokole za preverjanje pristnosti uporabnikov, med drugim dodeljevanje enoličnih identifikatorjev in močna gesla za aktivne uporabniške račune v sistemih, ki se uporabljajo za zagotavljanje storitev naročniku v skladu z IBM-ovimi poslovnimi varnostnimi standardi in praksami:

a. Gesla ne bodo že s strani dobaviteljev zagotovljena privzeta gesla ter bodo shranjena na lokaciji in/ali v obliki zapisa, ki ne ogroža varnosti podatkov, ki jih ščitijo.

b. Prikazovanje in tiskanje gesel mora biti maskirano, preprečeno ali drugače zakrito, da jih nepooblaščene osebe ne morejo videti ali pozneje pridobiti. Gesla se pri vnašanju ne smejo beležiti ali zajemati. Uporabniška gesla ne smejo biti shranjena kot navadno besedilo.

c. Gesla za vsako od tehnologij, ki sestavljajo ponudbo IBM SaaS, so izbrana tako, da zmanjšajo tveganja, povezana z znanimi ranljivostmi zaradi dolžine gesel, ter morajo biti dokumentirana.

d. Kadar je zaradi operacijskih razlogov potrebna uporaba internih, privilegiranih, funkcionalnih ID-jev v skupni rabi, IBM upravlja ID-je v skupni rabi, funkcionalne ID-je in/ali sistemske ID-je, ki zahtevajo odjavo gesel za ohranjanje individualne odgovornosti.

Za vse sisteme in aplikacije, v katerih je shranjena naročnikova vsebina, so vzpostavljene časovne omejitve nedejavnosti.

Po potrebi bo na naročnikovo zahtevo in po IBM-ovi formalni odobritvi vzpostavljen oddaljeni dostop do IBM-ovega omrežja, sistemov in aplikacij, v katerih je shranjena naročnikova vsebina, vse take oddaljene povezave pa bodo zavarovane s strogimi protokoli za preverjanje pristnosti in šifriranje. Dejavnost oddaljenega dostopa bo beležena in nadzorovana.

Če mora za zagotavljanje ponudbe IBM SaaS IBM oddaljeno dostopati do kateregakoli sistema znotraj naročnikovih internih omrežij, bo oddaljeni dostop izveden le prek naročnikovih varnih sistemov in protokolov za oddaljeni dostop ter poverilnic za dostop, ki jih naročnik zagotovi IBM-u. Oddaljeni dostop do naročnikovega omrežja bo izveden le na IBM-ovo zahtevo in po naročnikovi odobritvi ter v skladu s takrat veljavnimi naročnikovimi pravilniki, ki bodo predhodno zagotovljeni IBM-u. IBM-ova uporaba naročnikovih internih omrežij bo skladna z naročnikovimi pravilniki za uporabo IT in varnostnimi pravilniki, ki bodo predhodno zagotovljeni IBM-u.

IBM ima vzpostavljeno razmejitev dolžnosti za upravljanje varnosti, pregledovanje dostopa in raziskovanje varnostnih kršitev.

Shranjevanje, gostovanje in obdelovanje naročnikove vsebine, lastne naročniku, se izvaja ločeno kot za druge naročnike, katerim IBM zagotavlja storitve. Če naročnik odobri skupno rabo delovnih območij za shranjevanje, gostovanje ali obdelovanje, bo IBM vzpostavil postopke in varnostne mehanizme, skladne z zahtevami iz tega dodatka o varnosti in poslovni kontinuiteti, ki so namenjeni preprečevanju nepooblaščenega razkrivanja naročnikove vsebine.

IBM ima vzpostavljeno pravilo čiste mize/praznega zaslona, da naročnikovi podatki nikoli niso nenadzorovani v nobenem javnem prostoru.

3. Prenos in šifriranje

IBM bo izvajal ustrezne varnostne ukrepe pri prenašanju naročnikove vsebine (prek faksa, e-pošte, kurirske službe itd.) in se prepričal, da bodo uporabljeni pravi prejemnikovi kontaktni podatki, ter se z bodočim prejemnikom o tem vnaprej dogovoril, s čimer bo zagotovil varen prejem takih podatkov.

IBM in njegovo osebje vedno uporablja ustrezne oblike šifriranja ali druge varnostne tehnologije v povezavi z obdelovanjem naročnikove vsebine, kar vključuje vsakršen prenos, posredovanje, oddaljeni dostop do ali shranjevanje (vključno s shranjevanjem varnostnih kopij) naročnikove vsebine. IBM bo na primer z ustreznim panožno standardnim šifriranjem šifriral vse zapise in datoteke z naročnikovo vsebino, ki:

a. so shranjeni v IBM-ovih prenosnih računalnikih, prenosnih napravah ali prenosnih elektronskih medijih, vključno s trakovi za varnostne kopije med prenosom v objekt za shranjevanje na drugi lokaciji;

b. so shranjeni ali preneseni s strani IBM-a zunaj naročnikovih ali IBM-ovih fizično zavarovanih poslovnih stavb in objektov, kar ne vključuje dokumentov v papirni obliki;

c. jih IBM prenaša prek javnih omrežij;

d. se prenašajo iz IBM-ovih sistemov k naročniku;

e. jih IBM brezžično prenaša; in

f. jih IBM hrani v strežnikih in bazah podatkov.

4. Varnost omrežja

IBM uporablja razumno posodobljene različice programske opreme za varnost sistemov, kot so požarni zidovi, proxyji, požarni zidovi za spletne aplikacije in vmesniki. Ta programska oprema mora vsebovati zaščito pred zlonamerno programsko opremo ter razumno posodobljene popravke in definicije virusov. V skladu s poslovnimi standardi mora biti protivirusna programska oprema nameščena v delovnih postajah, strežnikih in povezanih končnih točkah, kjer je to s tehničnega vidika mogoče, programsko opremo pa se v skladu s pravili korporacije upravlja z internimi rešitvami za upravljanje.

IBM nadzoruje ponudbo IBM SaaS, da čim prej zazna in prepozna varnostne dogodke. IBM bo ohranjal vsaj s panožnimi standardi skladna orodja za zaznavanje vdorov ter postopke za preprečevanje, nadzorovanje in odzivanje, zasnovane za zaznavanje tako notranjih kot zunanjih ranljivosti in tveganj, zaradi katerih bi lahko prišlo do nepooblaščenega razkritja, zlorabe, spremembe ali uničenja naročnikove vsebine ali informacijskih sistemov, ki se uporabljajo za zagotavljanje storitev naročniku.

IBM uporablja storitve obveščanja o ranljivostih ali svetovalce za varnost podatkov in druge relevantne vire, ki zagotavljajo aktualne informacije o ranljivostih sistema. IBM redno preverja ranljivosti in popravlja svoje omrežje.

IBM nadzoruje ponudbo IBM SaaS, da zaznava, prepoznava, omejuje in razrešuje varnostne dogodke.

IBM preverja razpoložljivost, celovitost in učinkovitost varnostne infrastrukture omrežja, v katerem se zagotavlja ponudba IBM SaaS, z IBM-ovimi postopki za upravljanje izdaj.

5. Upravljanje dogodkov in obvestila o dogodkih

Ekipe za IBM Watson Health sodelujejo z IBM-ovo ekipo za odzivanje na dogodke spletne varnosti, globalno ekipo, ki upravlja prejemanje, raziskovanje in interno koordiniranje varnostnih dogodkov, povezanih z IBM-ovimi ponudbami, z namenom uvajanja preventivnih ukrepov za zmanjšanje varnostnih težav s programsko opremo. "Varnostni dogodek" je uspešno nepooblaščeno dostopanje do, uporaba, razkritje, spreminjanje ali oviranje sistemskih operacij ali podatkov v informacijskem sistemu, ki ga IBM uporablja za zagotavljanje ponudbe IBM SaaS. Če se odkrije varnostni dogodek (z rutinskim pregledom, opozorili, mejnimi dogodki itd.), bo IBM informiral in obvestil naročnika:

a. o vseh potrjenih varnostnih dogodkih, ki zadevajo naročnikovo vsebino, takoj, ko je to mogoče, in najpozneje v 2 delovnih dneh po preiskavi in potrditvi varnostnega dogodka;

b. nemudoma po vsakršni zahtevi za dostop do naročnikove vsebine ali informacij o njej s strani kateregakoli vladnega uslužbenca (vključno s katerokoli agencijo za varovanje podatkov ali organom pregona), razen če mu to prepoveduje zakonodaja ali relevantna odredba; in

c. razen, kot je dovoljeno v razdelku z naslovom "Nadzor dostopa" v tem dodatku o varnosti in poslovni kontinuiteti, pred vsakršnim razkritjem ali prenosom naročnikove vsebine tretji osebi oziroma dostopom do nje s strani tretje osebe.

6. Beleženje

IBM v skladu z IBM-ovimi pravilniki in praksami ter splošno sprejetimi panožnimi praksami izvaja razumen nadzor nad sistemi za ugotavljanje nepooblaščene uporabe ali dostopa do naročnikovih obdelanih podatkov. Dejanske ali neuspele nedovoljene prijave ali nedovoljeni dostopi bodo zabeleženi.

IBM vodi evidenco vseh zahtev za dostop in dnevnikov dejavnosti dostopa za vse sisteme, v katerih se shranjuje, dostopa do, obdeluje ali prenaša naročnikove in zdravstvene podatke tako dolgo, kot je zahtevano po zakonu HIPAA in drugi za IBM zadevni zakonodaji o podatkih.

Dnevniki in poročila vsebujejo vsaj: (i) vse uspešne ali neuspešne poskuse prijav, vključno z razumnimi identifikacijskimi podatki; (ii) vse spremembe konfiguracije sistemov in omrežij, vključno z namestitvami aplikacij, spremembami glede upravljanja uporabnikov in spremembami glede dovoljenj za dostop do datotek; (iii) uspešne ali neuspešne poskuse dostopa do virov, vključno s poskusi dostopa do katerekoli datoteke, omrežnega pogona, dnevnika ali drugih virov ; in (iv) prenose podatkov, vključno z vrsto vsebine podatkov in protokolom za dostop, uporabljenim za prenos.

7. Razvijanje strojne opreme in upravljanje sprememb

IBM spoštuje prakse za varno razvijanje aplikacij in kodiranje, ki varujejo celovitost produkcijskih aplikacij in povezane izvorne kode pred nepooblaščenimi in nepreizkušenimi spremembami.

IBM uporablja postopek za upravljanje sprememb, ki vključuje (a) beleženje in formalno odobravanje sprememb ter postopke za umik; ter (b) ustrezno preizkušanje teh sprememb, vključno s preizkušanjem sprejemanja s strani uporabnikov, če je ustrezno, in varnostno preizkušanje.

IBM uporablja postopek za upravljanje popravkov, ki vključuje preizkušanje popravkov pred namestitvijo v vse sisteme, ki se uporabljajo za shranjevanje, dostopanje do in prenašanje naročnikove vsebine ali zagotavljanje storitev naročniku, vključno s ponudbo IBM SaaS.

IBM zahteva, da skrbniki sistemov hranijo popolne, točne in posodobljene informacije o konfiguraciji vseh informacijskih sistemov, ki se uporabljajo za shranjevanje in prenašanje naročnikove vsebine ter dostopanje do nje.

8. Fizična in okoljska varnost

Platforma IBM Watson Health Core je nameščena v podatkovni infrastrukturi IBM SoftLayer. IBM SoftLayer uporablja fizično in okoljsko varovanje, nadzor dostopa, kontrolnike ter postopke za varovanje naročnikovih podatkov pred človeškim, okoljskim in tehničnim vdorom ali vplivom.

Splošni dostop do objektov, v katerih gostuje ponudba IBM SaaS, je nadzorovan prek sistema za dostop s kartico. V objektih so povsod nameščene televizijske kamere zaprtega kroga (CCTV), ki jih spremlja varnostno osebje. Izbrana dostopna vrata so varovana z alarmnimi sistemi, ki jih nadzoruje varnostno osebje.

Dostop do nadzorovanih območij je omejen z uporabo kartic za dostop in/ali dodatnega biometričnega preverjanja pristnosti. Vsi posamezniki brez pooblaščenega dostopa do nadzorovanih območij se morajo vpisati v evidenco, nato pa jih spremlja posameznik z odobrenim dostopom do nadzorovanih območij. Vsi

zasilni izhodi na nadzorovanih območjih so varovani z zvočnimi alarmnimi sistemi, ki jih nadzoruje varnostno osebje. Izvaja in dokumentira se redno preverjanje delovanja alarmnih sistemov, o čemer se hranijo tudi zapisi. Pravice za dostop do nadzorovanih območij se v celoti ponovno preverjajo štirikrat letno. Pravica za dostop do nadzorovanih območij se odvzame ob prenehanju delovnega razmerja.

Objekti so zaščiteni pred okoljskimi dejavniki, kot so ogenj, voda in vročina, s požarnimi alarmi, gasilnimi aparati, dimnimi alarmi ter sistemi za dušenje in gašenje požarov. Objekti so zaščiteni pred motnjami ali izpadi napajanja s sistemi in rezervnimi generatorji za neprekinjeno napajanje (UPS), ki se jih redno vzdržuje in preizkuša.

Informacije in poročila o skladnosti za IBM SoftLayer so na voljo na spletnem mestu: http://www.softlayer.com/compliance.

9. Kontinuiteta poslovnih operacij

IBM ima načrte za poslovno kontinuiteto in obnovitev po hudi napaki, ki so namenjeni ohranjanju ravni storitev v skladu z obveznostmi po tej pogodbi. Načrti za poslovno kontinuiteto in obnovitev po hudi napaki se bodo redno posodabljali in preizkušali (vsaj enkrat na leto). IBM bo v načrte za poslovno kontinuiteto in obnovitev po hudi napaki uvedel vse razumne spremembe, potrebne za ohranjanje skladnosti s splošno sprejetimi panožnimi praksami, v vsakem primeru pa ne da bi nerazumno oviral ponudbo IBM SaaS ali produkcijsko okolje, ki ju uporablja naročnik.

V primeru hude napake, zaradi katere ponudba IBM SaaS naročniku ni na voljo, bo IBM nemudoma obvestil naročnika ter aktiviral načrt za poslovno kontinuiteto in/ali obnovitev po hudi napaki. Ob razglasitvi hude napake ciljna poslovna kontinuiteta ponudbe IBM SaaS zajema ponovno vzpostavitev naročnikovega dostopa do ponudbe IBM SaaS, kot sledi: v primeru izpada je ciljni čas obnovitve (RTO) za ponovno vzpostavitev produkcijskega okolja IBM Watson Health največ 36 ur po razglasitvi hude napake. Ciljna točka obnovitve (RPO) je največ 24 ur izgube naročnikove vsebine znotraj produkcijskega okolja. Ciljna poslovna kontinuiteta za posamezne rešitve Watson Health se lahko razlikuje.

IBM-ov pristop do obnovitve po hudi napaki zajema več podatkovnih središč na različnih geografskih območjih.

Vsa podatkovna središča IBM SoftLayer imajo več virov napajanja, vlakenskih povezav, namenskih generatorjev in rezervnih baterij. Zgrajena so iz vodilne strojne in druge opreme v panogi, kar zagotavlja najvišjo raven zmogljivosti, zanesljivosti in skupne uporabnosti. Vse komponente podatkovnih središč, ki vključujejo na primer redundantne vire napajanja in ohlajanja n+1, se preverjajo, da se zagotavlja stabilnost znotraj podatkovnih središč.

10. Skladnost

IBM-ove varnostne prakse temeljijo na standardu ISO 27001-27002. Te prakse zagotavljajo nadzorne strukture za analizo tveganj, fizično varnost, načrtovanje za izredno stanje, preiskave, zaščito informacij, izobraževanje, zaščito podatkov, operacije itd.

IBM preverja skladnost dejavnosti, povezanih z varnostjo in zasebnostjo, z IBM-ovimi varnostnimi pravilniki.

IBM spoštuje za IBM zadevno zakonodajo o podatkih, v zadevnih sodnih pristojnostih.

Ustrezno ravnanje z naročnikovimi zaupnimi podatki je zahtevano tudi po IBM-ovih smernicah poslovnega vedenja, s katerimi se morajo vsako leto seznaniti vsi zaposleni (in potrditi njihov pregled).

11. Razno

IBM bo zagotovil, da vse njegove pogodbe s podizvajalci in/ali tretjimi osebami, vpletenimi v zagotavljanje ponudbe IBM SaaS, vsebujejo določila, ki v vsaj enaki meri ščitijo naročnikovo vsebino kot določila iz tega dodatka o varnosti in poslovni kontinuiteti ter morebitnega ustreznega povezanega dokumenta, v takem obsegu, kot ta določila veljajo za storitve, ki jih bodo ti podizvajalci in/ali tretje osebe izvajali.