IBM naudojimo sąlygos – su „SaaS“ susijusios pasiūlymo sąlygos

„IBM Watson Health Core“

Naudojimo sąlygas (NS) sudaro šios IBM naudojimo sąlygos – su „SaaS“ susijusios pasiūlymo sąlygos („Su „SaaS“ susijusios pasiūlymo sąlygos“) ir dokumentas „IBM naudojimo sąlygos – bendrosios sąlygos“ („Bendrosios sąlygos“), pasiekiamos šiuo URL: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Atsiradus prieštaravimams, su „SaaS“ susijusios pasiūlymo sąlygos laikomos viršesnėmis už Bendrąsias sąlygas. Klientas sutinka su šiomis NS, jeigu užsako, pasiekia ar naudoja „IBM SaaS“.

NS nustato IBM tarptautinės „Passport Advantage“ sutarties, IBM tarptautinės „Passport Advantage Express“ sutarties arba IBM tarptautinės pasirinktų „IBM SaaS“ pasiūlymų sutarties sąlygos, kiek jos taikomos, („Sutartis“) ir kartu su NS sudaro visą sutartį.

1. „IBM SaaS“

„IBM SaaS“ parduodama pagal vieną iš šių mokesčių apskaičiavimo metrikų, kaip nurodyta Operacijų dokumente:

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

2. Mokesčio apskaičiavimas

„IBM SaaS“ parduodama pagal vieną iš toliau nurodytų mokesčių apskaičiavimo schemų, pateiktų Operacijų dokumente:

a. **Prieiga** – tai matavimo vienetas, kuriuo remiantis galima įgyti „IBM SaaS“. Prieiga – tai teisės naudoti „IBM SaaS“. Klientas turi gauti atskirą Prieigos teisę, kad galėtų „IBM SaaS“ naudoti matavimo laikotarpiu, nurodytu Kliento Teisių suteikimo dokumente (TSD) arba Sandorio dokumente.

b. **Individas** – tai matavimo vienetas, kuriuo remiantis galima įgyti „IBM SaaS“. Individas yra vienas dalykas arba žmogus. Reikia įsigyti teises, kurių pakaktų kiekvienam „IBM SaaS“ apdorojamam arba valdomam Individui padengti matavimo laikotarpiu, nurodytu Kliento TSD arba Operacijų dokumente.

   Šiame „IBM SaaS“ Individas yra asmuo, įrenginys arba taikomoji programa mobiliesiems, kurios duomenis tvarko „IBM SaaS“.

c. **Egzempliorius** yra matavimo vienetas, kuriuo remiantis galima gauti „IBM SaaS“. Egzempliorius yra prieiga prie konkrečios „IBM SaaS“ konfigūracijos. Reikia įsigyti pakankamas teises, skirtas kiekvienam „IBM SaaS“ Egzemplioriui pasiekti ir naudoti matavimo laikotarpiu, nurodytu Kliento Operacijų dokumente.

3. Mokesčiai ir sąskaitų išrašymas

Už „IBM SaaS“ mokėtina suma nurodyta Operacijų dokumente.

3.1 Daliniai mėnesio mokesčiai

Dalinis mėnesio mokestis, kaip nurodyta Operacijų dokumente, gali būti nustatomas proporcingai.

3.2 Mokesčiai už perviršį

Jei Kliento faktinis naudojimas matavimo laikotarpiu viršys TSD nurodytas teises, Klientui bus išrašyta sąskaita už perviršį, nustatytą pagal Sandorio dokumentą.

4. Terminas ir atnaujinimo galimybės

„IBM SaaS“ naudojimo terminas prasideda nuo dienos, kai IBM praneša Klientui, kad jis turi prieigą prie pilotinės „IBM SaaS“ Bandymo operacinės aplinkos, kaip aprašyta Užsakymo dokumente. Individualių teisių prenumeratos laikotarpis prasideda, kai IBM praneša Klientui, kad suteikė prieigą prie Gamybos operacinės aplinkos. Užsakymo dokumente bus nurodyta, ar „IBM SaaS“ bus atnaujinama automatiškai, naudojama nepertraukiamai ar nutraukiama laikotarpio pabaigoje.

Atnaujinant automatiškai, jei Klientas nepateikia prašymo neatnaujinti raštu mažiausiai prieš 90 dienų iki termino galiojimo pabaigos datos, „IBM SaaS“ automatiškai atnaujinama TSD nurodytam laikotarpiui.

Naudojant nuolat, „IBM SaaS“ bus nuolat pasiekiama skaičiuojant mėnesiais, kol Klientas prieš 90 dienų raštu pateiks pranešimą apie nutraukimą. Praėjus šiam 90 dienų laikotarpiui, „IBM SaaS“ bus pasiekiama iki kalendorinio mėnesio pabaigos.

5. Techninis palaikymas

IBM pateiks „IBM Software as a Service Support Handbook“ (IBM Programinės įrangos kaip paslaugos palaikymo vadovą), kuriame nurodyta techninio palaikymo centro kontaktinė informacija, techninės priežiūros laikais ir kita informacija ir procesai. Techninio palaikymo kontaktinę ir kitą informaciją apie palaikymo operacijas galima rasti apsilankius „IBM SaaS“ palaikymo vadove: https://support.ibmcloud.com.

„IBM SaaS“ techninis palaikymas ir paprastos konfigūravimo užklausos teikiamos elektroniniu būdu. Techninis palaikymas siūlomas su „IBM SaaS“ ir kaip atskiras pasiūlymas neteikiamas.

Pranešant apie problemą, į jokius dokumentus ar informaciją negalima įtraukti jokios Asmeninės informacijos (AI), įskaitant Saugomą informaciją apie sveikatos būklę (PHI) ir slaptą asmeninę informaciją (SAI).

6. Apibrėžtys

Taikomi įstatymai – tai įstatymai, statutai arba įstatyminės normos, taisyklės, nuostatos, direktyvos, teismo nurodymai, potvarkiai arba kiti reikalavimai, kuriuos išleido vyriausybinė institucija ar kiti visuotinai pripažinti pramonės standartai, taikomi vykdant šias Naudojimo sąlygas.

API – tai taikomosios programos sąsaja, kuri yra programų, protokolų ir įrankių rinkinys, skirtas programinės įrangos kūrimui. API nurodo, kaip turi sąveikauti programinės įrangos komponentai ir API, naudojamos programuojant grafinės vartotojo sąsajos (GUI) komponentus.

Įgaliotasis administratorius – yra bet kuris Kliento darbuotojas, patvirtintas Kliento rangovas, asmuo arba grupė, atsakingi už tvarkingą ir patikimą platformos veikimo priežiūrą. Įsipareigojimai gali apimti konfigūraciją, palaikymą ir vartotojo bei paskyros tvarkymą. Be to, administratorius gali būti klinikinis tyrėjas, atsakingas už tyrimo nustatymą „Watson Health“ sistemoje.

Įgaliotasis individas – bet kuris įgaliotasis asmuo, taikomoji programa mobiliesiems arba įrenginys, kuriems buvo suteiktos prieigos teisės siųsti duomenis į „Watson Health Core“. Tai gali būti Klientas arba tyrimo dalyviai, klientai arba Kliento pacientai.

Klientui taikomi duomenų apsaugos įstatymai – tai duomenų apsaugos įstatymai, taikomi Kliento įsipareigojimų vykdymui pagal šią Šalių Sutartį, Susijusius dokumentus ir taikomus Paslaugų aprašus, Užsakymo dokumentus ir Darbo aprašus tarp Šalių.

Kliento duomenys – tai bet kokia Kliento arba Klientui skirtų duomenų įvestis „IBM SaaS“, kai įvedami Kliento duomenys, duomenis įveda Kliento klientas ar trečioji šalis arba duomenys įvedami jų vardu, ir įskaitant visus trečiosios šalies sveikatos priežiūros įrenginio duomenis.

Duomenų apsaugos įstatymai – tai visi Taikomi įstatymai, susiję su duomenų apsauga, privatumu arba sauga.

Duomenų subjektas – tai identifikuotas arba identifikuojamas asmuo, su kuriuo susiję Asmens duomenys.

Priskirtasis duomenų centras – tai duomenų centras (-ai), Operacijų dokumente nurodyti kaip pirminis ir avarinio atkūrimo duomenų centrai, kuriuose veikia Kliento „IBM SaaS“ egzempliorius, jei taikoma.

Sveikatos duomenys – tai visi duomenys arba informacija, įskaitant atvaizdus, kurie yra su sveikatos būkle susijusi Asmeninė informacija.

Tinka sveikatos duomenims – „IBM SaaS“ atveju reiškia, kad „IBM SaaS“ laikosi taikomų „Sveikatos duomenų susijusių jurisdikcijų“ („In-Scope Jurisdictions for Health Data“) saugos ir privatumo standartų, įstatymų ir taisyklių, įskaitant HIPAA realizavimo taisyklių (pakeistų HITECH aktu) 164 dalies, A ir C antrinėse dalyse išdėstytas diegimo specifikacijas ir kitus su Sveikatos duomenimis susijusius Taikomus įstatymus, bet tai nereiškia, kad IBM veikia kaip Verslo partneris arba Duomenų valdytojas.

HIPAA – tai 1996 m. Sveikatos draudimo portatyvumo ir atskaitomybės aktas („Health Insurance Portability and Accountability Act“) su pataisymais, įskaitant 2009 m. Amerikos atgaivinimo ir naujų investicijų akto („American Recovery and Reinvestment Act“) Sveikatos priežiūros informacijos

technologijos, skirtos ekonomikai ir klinikinei sveikatos priežiūrai aktą („Health Information Technology for Economic & Clinical Health Act“) (HITECH Aktas“), konkrečias JAV Sveikatos ir paslaugų departamento paskelbtas HIPAA 45 C.F.R. 160 ir 164 dalyse taisykles ir pagal HITECH Aktą paskelbtas konkrečias taisykles.

IBM taikomi duomenų apsaugos įstatymai – tai duomenų apsaugos įstatymai, taikomi IBM įsipareigojimų vykdymui pagal šią Šalių Sutartį, Susiję dokumentai ir taikomi Paslaugų aprašai, Užsakymo dokumentai ir Darbo aprašai.

IBM personalas – tai (a) IBM, jos Filialai ir subrangovai bei visų anksčiau nurodytų subjektų darbuotojai ir (b) visi trečiosios šalies tiekėjai; kiekvienu atveju IBM vardu teikiantys paslaugas pagal Sutarties sąlygas ir atitinkamus Susijusius dokumentus arba kitaip IBM įgalioti pasiekti Kliento Asmeninius duomenis.

Aprėpties šalys – tai 28 Europos Sąjungos šalys narės ir Šveicarija bei šalys, kurias IBM gali kartais įtraukti į šį sąrašą.

Asmeniniai duomenys arba **Asmeninė informacija** – tai bet kokia medijos arba bet kokio formato informacija, įskaitant elektroninius ir popierinius įrašus, susijusius su identifikuotu arba identifikuojamu individu. „Identifikuojamas individas“ yra tas, kurį galima konkrečiai tiesiogiai arba netiesiogiai identifikuoti pagal nuorodą į identifikavimo numerį arba pagal vieną ar daugiau veiksnių, būdingų jo / jos fizinei, fiziologinei, psichinei, ekonominei, kultūrinei arba socialinei tapatybei.

Apdorojimas ir jo variantai, pvz., **tvarkymas** (didžiosiomis arba mažosiomis raidėmis) – bet kokia su duomenimis automatiškai arba neautomatiškai atliekama operacija arba operacijų rinkinys, pvz., rinkimas, registravimas, organizavimas, laikymas, pritaikymas arba keitimas, išgavimas, konsultavimas, naudojimas, atskleidimas perduodant, platinant ar kitaip padarant pasiekiama, derinimas arba sujungimas, blokavimas, ištrynimas arba sunaikinimas.

Apdoroti duomenys – tai bet kokie duomenys, konfidenciali arba savininko informacija arba medžiaga, įskaitant Sveikatos duomenis ir Asmeninius duomenis, kuriuos pagal Sutarties sąlygas, Susijusį dokumentą ir (arba) Paslaugos aprašą, Užsakymo dokumentą ir (arba) Darbų aprašą, apdoroja IBM.

Saugos incidentas – reikšmė nurodyta toliau SBCA.

7. Paskyros tvarkymas

„IBM SaaS“ gali pasiekti tik Kliento įgaliotieji vartotojai („**Įgaliotieji administratoriai**“ arba „**Įgaliotieji individai**). Klientas valdys paskyras, kurias turės teisę pasiekti „IBM SaaS“, kuriose gali būti įgaliotųjų taikomųjų programų, Kliento personalo, Kliento trečiosios šalies paslaugų teikėjų ir rangovų, iš yra išskirtinai atsakingas už (i) visų įgaliotųjų vartotojų kontrolę, įskaitant, be apribojimų, visų įgaliotųjų vartotojų tapatybės patvirtinimą, ir (ii) užtikrinimą, kad „IBM SaaS“ pasiektų tik įgaliotieji vartotojai.

Įgaliotiesiems individams, kurie yra Kliento klientai, pacientai arba tyrimo dalyviai, gali būti suteikta prieiga išskirtinai duomenų įkėlimo į „IBM SaaS“ tikslu ir tokiu atveju tokie Įgaliotieji individai neturės jokios kitos prieigos prie „IBM SaaS“.

8. Privatumas

8.1 Bendrieji reikalavimai

Šalių susitarimo atžvilgiu, Klientas yra vienintelis visų Kliento Asmeninių duomenų valdytojas ir Klientas paskiria IBM duomenų tvarkytoju. Pagal Taikomus duomenų apsaugos įstatymus Klientas turi teisę instruktuoti IBM, kaip IBM turėtų apdoroti Kliento Asmeninius duomenis.

Kiek tai bus susiję su IBM apdorojamais Kliento Asmeniniais duomenimis, IBM:

a. laikysis visų IBM Taikomų duomenų apsaugos įstatymų ir

b. nemaišys Kliento Asmeninių duomenų su duomenimis iš kitų šaltinių, išskyrus:

- kai tai būtina teikiant „IBM SaaS“ ir tuo atveju jokiais kitais tikslais, jei Klientas aiškiai nenurodo daryti kitaip, arba
- pagal šias Naudojimo sąlygas ir SBCA priedo sąlygas.

Kai tai bus susiję su IBM apdorojamais Kliento Asmeniniais duomenimis, Klientas:

a. laikysis visų Klientui Taikomų duomenų apsaugos įstatymų;

b. bus atsakingas už visus Kliento ryšius su Kliento Filialais, pacientais ir vartotojais, Duomenų subjektais ir (arba) kitomis Kliento trečiosiomis šalimis;

c. sudarys su savo tvarkytojais visas duomenų apdorojimo sutartis, reikalingas IBM, kaip duomenų tvarkytojui, ir jos antriniams tvarkytojams visiems Kliento Asmeniniams duomenims apdoroti, ir

d. veiks kaip vienas IBM skirtas kontaktas ir bus išimtinai atsakingas už vidinį koordinavimą bei Kliento Filialų, kurie yra kiti IBM tvarkytojai, instrukcijų arba užklausų peržiūrą. IBM bus atleista nuo savo įsipareigojimo informuoti arba įspėti bet kurį Kliento Filialą, kuris yra tvarkytojas, kai tokia informacija arba įspėjimas bus pateikti Klientui. IBM turi teisę atsisakyti atmesti bet kokias bet kurio Kliento Filialo, kuris yra tvarkytojas, bet ne Klientas, tiesiogiai pateiktas instrukcijas.

Nė vienos šalies nereikalaujama veikti pažeidžiant šiai šaliai Taikomus duomenų apsaugos įstatymus.

8.2 Kliento duomenų teisės

Klientas pareiškia ir garantuoja, kad (a) jam priklauso duomenys, kuriuos jis įves „IBM SaaS“, arba (b) jis gavo ir yra atsakingas už išlaikymą visų būtinų teisių, leidimų, sutikimų ir įgaliojimų, kad IBM būtų suteikta teisė pasiekti, naudoti ir atskleisti Kliento duomenis, laikantis toliau šiose Naudojimo sąlygose arba Sutartyje nurodytų sąlygų, arba veikti kitaip, kai tai būtina IBM norint teikti „IBM SaaS“. Be to, Klientas pareiškia ir garantuoja, kad Kliento duomenys bus (a) susiję tik su JAV gyvenančiais asmenimis ir bus įvedami tik JAV duomenų centre esančiame „IBM SaaS“ arba (b) susiję su vienoje ar keliose Aprėpties šalyes gyvenančiais asmenimis ir tokiu atveju bus įvedami į „IBM SaaS“ Priskirtajame (-siuose) duomenų centre (-uose).

8.3 Duomenų paslaugos ir įsipareigojimai

a. Klientas sutinka, kad jis analizuos Kliento duomenis arba pateiks prašymą IBM atlikti jų analizę tiek, kiek tai susiję su Kliento „sveikatos priežiūros operacijomis“ arba „tyrimu“, kaip HIPAA apibrėžtos šios sąvokos ir (arba) panašios sąvokos kituose Taikomuose duomenų apsaugos įstatymuose, ir Klientas naudos Kliento duomenis arba nurodys IBM naudoti Kliento duomenis tik laikantis visų taikomų reikalavimų (pvz., Institucinės priežiūros komisijos nustatymų arba atsisakymo, kai reikalaujama) pagal šiuos ir bet kuriuos kitus Klientui Taikomus duomenų apsaugos įstatymus.

b. Klientas išskirtinai atsakingas už visų registracijų, sutikimų, įgaliojimų ir leidimų gavimą, kaip to reikalauja Klientui Taikomi įstatymai kiekvienoje Aprėpties šalyje, įskaitant, be apribojimų, HIPAA ir kitus taikomus duomenų privatumo ir apsaugos įstatymus, taisykles ir nuostatas, kad Kliento duomenys būtų įvesti į „IBM SaaS“ ir naudojami bei atskleidžiami, kaip numatyta šiose Naudojimo sąlygose ir Sutartyje, kurią sudarė Klientas ir IBM bei IBM leidžiami subrangovai. IBM neįsipareigoja prižiūrėti, ar tokios registracijos, sutikimai, įgaliojimai ir leidimai yra gauti arba reikalingi.

c. Klientas išskirtinai atsakingas už užtikrinimą, kad visi „IBM SaaS“ įvesti Kliento duomenys būtų susiję tik su JAV arba atitinkamoje Aprėpties šalyje gyvenančiais asmenimis.

d. IBM turės palaikymo centrus, kurių personalas išmanys HIPAA ir kitus IBM Taikomus duomenų apsaugos įstatymus, susijusius su duomenimis iš Aprėpties šalių.

8.4 Saugos priemonės ir saugos incidentai

a. IBM realizuos, palaikys ir laikysis techninių ir organizacinių priemonių (įskaitant organizacinius procesus ir procedūras bei įskaitant bet kokius konkrečius saugos įsipareigojimus, nustatytus arba nurodytus šiose Naudojimo sąlygose ir SBCA, skirtus apsaugoti Kliento Asmeninius duomenis nuo neteisėto naudojimo ir prieigos, netyčinio praradimo, sugadinimo, modifikavimo, sunaikinimo, vagystės arba neteisėto atskleidimo.

b. Jeigu IBM sužino apie Saugos incidentą (kaip apibrėžta SBCA), susijusį su Kliento Apdorojamais duomenimis, IBM informuos Klientą, kaip numatyta SBCA ir IBM Taikomuose duomenų apsaugos įstatymuose, ir tokiame pranešime bus įtraukta informacija apie visą žinomą poveikį Klientui arba Duomenų subjektams (jei yra), paveiktiems tokio Saugos incidento, ir IBM atliktus arba siūlomus atlikti taisymo veiksmus.

8.5 Užklausų ir skundų gavimas

IBM nedelsdama ir kiek leidžia IBM Taikomi duomenų apsaugos įstatymai, praneš Klientui raštu ne vėliau nei per penkias (5) darbo dienas po „IBM Watson Health“ duomenų privatumo pareigūno gauto užklausimo, pranešimo ar skundo, kurį IBM gavo dėl Kliento Asmeninių duomenų iš:

a. bet kurio Duomenų subjekto, susijusio su Asmeniniais duomenimis apie tokį IBM apdorojamą Duomenų subjektą. Klientas atsakys į tokias Duomenų subjektų užklausas ir IBM laikysis pagrįstų Kliento instrukcijų, padėdama Klientui atsakyti į tokias užklausas. Jei reikalauja IBM Taikomi įstatymai, IBM į tokias užklausas gali atsakyti tiesiogiai, jeigu IBM iš anksto praneša Klientui apie

tokį atsakymą ir pagrįstai suderina su Klientu tokio atsakymo formą ir turinį, kai leidžia IBM Taikomi įstatymai ar tai įmanoma kitu būdu;

b. bet kokios teisinės arba reguliavimo institucijos dėl IBM atliekamo Kliento Asmeninių duomenų apdorojimo, su sąlyga, kad IBM gali atsakyti į tokias iš vyriausybinių institucijų gautas užklausas (šaukimus į teismą ar panašius teisinius dokumentus) dėl kurių IBM privalo atskleisti informaciją, arba kai to dėl kitų priežasčių reikalauja Taikomi duomenų apsaugos įstatymai, jeigu IBM iš anksto praneša Klientui apie tokį atskleidimą ir pagrįstai suderina su Klientu tokio atsakymo formą ir turinį, kai tai leidžia įstatymai ar tai įmanoma kitu būdu.

8.6 Kliento asmeninių duomenų apdorojimas

IBM atskleis Kliento Asmeninius duomenis tik IBM personalui, kuriam jie gali būti reikalingi teikiant Paslaugas.

IBM vykdys visus pagrįstus Kliento prašymus IBM pakeisti, pataisyti, panaikinti arba blokuoti Kliento Asmeninius duomenis, laikantis Taikomų įstatymų.

Gavę kurios nors Šalies prašymą, IBM, Klientas arba jų Filialai sudarys pagal įstatymus reikalaujamas Kliento Asmeninių duomenų apsaugos standartines sutartis. Šalys sutinka (ir pasirūpins, kad sutiktų atitinkami Filialai), kad tarp Šalių atsiradus pretenzijoms tokioms sutartims bus taikomi šioje Sutartyje nurodyti atsakomybės apribojimai ir išimtys. Šalys bendradarbiaus sutardamos laikytis (arba pasirūpindamos, kad sutartų Šalių Filialai) ir laikydamosis vėliau abipusiu susitarimu nustatytų sąlygų arba sudarytų sutarčiu, jei to reikalautų Taikomi duomenų apsaugos įstatymai.

8.7 Kliento Asmeninių duomenų grąžinimas

Pasibaigus Sutarties galiojimo laikui arba ją nutraukus, IBM ir visas IBM Personalas nustos naudoti arba apdoroti bet kokią Kliento Nuosavybės teise pagrįstą informaciją, bet kokius Kliento Asmeninius duomenis ir Klientui pasirinkus arba paprašius:

a. nedelsiant grąžins tokiu formatu ir tokioje laikmenoje, kokiais Klientas pagrįstai paprašys, visą Kliento Nuosavybės teise pagrįstą informaciją ir Kliento Asmeninius duomenis, kuriuos IBM laiko elektroniniu būdu, ir gavę Kliento patvirtinimą apie gavimą, ištrins, sunaikins ar kitaip visam laikui padarys neperskaitomą arba neiššifruojamą Kliento Nuosavybės teise pagrįstą informaciją ir Kliento Asmeninius duomenis, įskaitant jų kopijas ir atsargines kopijas. IBM gali taikyti mokestį už laikmeną ir tam tikrus Kliento prašymu atliktus veiksmus (pvz., Kliento Nuosavybės teise pagrįstos informacijos ir Kliento Asmeninių duomenų pateikimą konkrečiu formatu arba Kliento Nuosavybės teise pagrįstos informacijos ir Kliento Asmeninių duomenų sunaikinimą konkrečiu būdu); ir

b. tiesiogiai ištrins, sunaikins arba kitaip visam laikui padarys neperskaitomą arba neiššifruojamą Kliento Nuosavybės teise pagrįstą informaciją ir Kliento Asmeninius duomenis, įskaitant jų kopijas ir atsargines kopijas.

8.8 Verslo partnerių sutartis

HIPAA atitinkančia ir reikalaujama aprėptimi IBM ir Klientas sudarys Verslo partnerių sutartį (VPS), kuri apibrėš IBM, kaip Kliento Verslo partnerio, įsipareigojimus teikiant „IBM SaaS“. Neapribojant aiškių IBM įsipareigojimų pagal Sutartį ir VPS, jei taikoma, Klientas pripažįsta ir sutinka, kad yra atsakingas už Taikomų įstatymų ir licencijavimo reikalavimų, kurie taikomi Kliento naudojimui ir kitoms veikloms, kai tai susiję (įskaitant Įgaliotųjų vartotojų naudojimą arba kitas veiklas) su „IBM SaaS“, taikymo sąlygų nustatymą ir jų laikymąsi.

8.9 Europos Sąjungos duomenų apdorojimo priedas

Jeigu Klientas nurodo IBM apdoroti Europos Sąjungos Asmeninius duomenis, IBM ir Klientas sudarys Duomenų apdorojimo priedą, į kurį įtrauks atitinkamus ES modelio teisinių dokumentų sąlygas, pašalindami nebūtinas sąlygas.

9. „IBM SaaS“ pasiūlymo papildomos sąlygos

9.1 Sauga

Šiai „IBM SaaS“ taikomi „IBM SaaS“ duomenų saugos ir privatumo principai, kurie pateikti http://www.ibm.com/cloud/data-security, ir papildomos sąlygos, nustatytos toliau ir šių Naudojimo sąlygų Saugos ir verslo tęstinumo priede. Jokie IBM duomenų saugos ir privatumo principų pakeitimai nesumažins „IBM SaaS“ saugos.

„IBM Watson Health Core“ realizuoja ISO 27001 sistema pagrįstas saugos politikas, standartus ir procesus, kurie aprašyti toliau šiame Saugos apraše. Kartu su saugos galimybėmis sprendime realizuota:

a. Saugios operacinės zonos

„IBM Watson Health Core“ realizuota nuodugni apsaugos strategija, naudojanti kelias saugos zonas, skirtas debesų kompiuterijos integravimo taškams tvarkyti, pvz., duomenims gauti ir pasirinktinėms taikomosioms programoms kurti.

b. Šifravimas

Visi tinklais ir laikmenomis perduodami Kliento duomenys yra šifruojami. Visi į arba iš „IBM Watson Health Core“ perduodami duomenys yra šifruojami. Šifravimo kodą tvarko bendrai naudojama paslauga. Klientas yra atsakingas už visus „IBM Watson Health Service“ ir Kliento tarpinio serverio tinklo ryšius ir kokybę.

c. Saugos įvykių kontrolė

IBM naudoja savo saugos informacijos platformos galimybes valdydama saugos informaciją ir įvykius, valdydama žurnalą, tirdama incidentus, aptikdama grėsmes ir valdydama pažeidžiamumą.

d. Tapatybės valdymas

- „Watson Health Core“ palaiko didelių pacientų ir vartotojų populiacijų atvirojo kodo standartų tapatybės patvirtinimo, naudojant „OpenID Connect“, teikėjus.
- Vartotojų populiacijose, kuriose tapatybės patvirtinimo teikėjas yra IBM, autentifikavimui tvarkyti „Watson Health Core“ naudoja atitinkamas katalogų paslaugas ir tapatybės valdymo galimybes.

e. Sudėtingas autentifikavimas ir vaidmenimis pagrįsta prieiga

- „Watson Health Core“ palaiko autentifikavimą SAML, kurį kaip mechanizmą gali naudoti Klientai integruodami savo „Single Sign On“ (vienkartinis prisijungimas – SSO) arba katalogų paslaugas.
- Jei reikia, „Watson Health Core“ naudoja prieigos valdymo sprendimą ir susijusius komponentus saugos politikoms tvarkyti.
- „Watson Health Core“ palaiko programine įranga pagrįstą dviejų dalių autentifikavimą.
- „Watson Health Core“ užtikrina bazinę vaidmenimis pagrįstos prieigos kontrolę, kaip reikalaujama; „Watson Health Core“ palaiko tyrimo konfigūravimą, vartotojo profilius, vaidmenis ir vartotojų grupes, naudojant programos taikomojo programavimo sąsajas (API arba APIs), kurios įgalina vaidmenimis pagrįstą prieigą.

9.2 Slapukai

Klientas žino ir sutinka, kad „IBM SaaS“ naudojimo ir palaikymo tikslais, naudodama sekimo ir kitas technologijas, IBM gali iš Kliento (jūsų darbuotojų ir rangovų) rinkti su „IBM SaaS“ naudojimu susijusią asmens informaciją. IBM renka naudojimo statistinius duomenis ir informaciją apie „IBM SaaS“ efektyvumą, kad galėtų gerinti vartotojų patirtį ir (arba) glaudžiau bendradarbiauti su Klientu. Klientas patvirtina, kad gaus arba jau yra gavęs sutikimą leisti IBM tvarkyti surinktą asmens informaciją anksčiau nurodytais tikslais, laikantis taikomos teisės, IBM, kitose IBM įmonėse ir jų subrangovų vietose, kur IBM ir mūsų subrangovai vykdo veiklą. IBM vykdys Kliento darbuotojų ir rangovų pageidavimus pasiekti, naujinti, taisyti arba panaikinti jų surinktą asmens informaciją.

9.3 Išvestinės naudojimosi vietos

Kai taikoma, mokesčiai yra pagrįsti vieta (-omis), kurią (-ias) Klientas nurodo kaip „IBM SaaS“ naudojimo vietą. IBM taikys mokesčius remdamasi pateikiant „IBM SaaS“ užsakymą kaip pagrindinę naudojimo vietą nurodytą įmonės adresą, nebent Klientas pateiks IBM papildomos informacijos. Klientas yra atsakingas už tokios informacijos atnaujinimą ir IBM informavimą apie visus pakeitimus.

9.4 Nuolatinis teikimas

Klientas turi teisę naudoti sprendimo galimybes ir patobulinimus, kuriuos IBM diegia nuolat teikiamame debesų kompiuterijos modelyje.

9.5 Atsarginis kopijavimas ir atkūrimas

„IBM Watson Health Core“ pateikia naujausią žinomą geros būklės Kliento duomenų atsarginę kopiją gamybos aplinkoje (įskaitant „Data Lake“ ir „Data Reservoir“ saugyklas), skirtą atkūrimo paslaugai sistemos trikties atveju.

9.6 Geras pasiekiamumas

„IBM Watson Health Core“ komponentai gamybos aplinkoje realizuojami taikant gero pasiekiamumo konfigūracijas, įtraukus į sankaupą perteklumo duomenų bazių serverius, skirtus užtikrinti darbo krūvio paskirstymą ir eliminuoti vieną trikčių tašką.

9.7 Avarinis atkūrimas

IBM avarinio atkūrimo metodas apima kelis duomenų centrus skirtingose geografinėse vietose, kad būtų užtikrinti toliau nurodyti verslo tęstinumo Gamybos aplinkoje:

- DAL – per 36 valandas po avarijos paskelbimo
- DAT – ne daugiau nei 24 valandų Kliento turinio praradimas

9.8 Matavimo įrankiai

„IBM SaaS“ naudoja sintetinį stebėjimo sprendimą, skirtą stebėti, matuoti ir pranešti apie pasiekiamumą arba prastovas, atsižvelgiant į paslaugos lygio įsipareigojimus. Šis sprendimas modeliuoja ir stebi vartotojo atsaką ir patirtį visuotiniu lygmeniu – tiek statinį pasiekiamumą, tiek operacijas.

Be to, „IBM SaaS“ naudojama tarptautinė stebėjimo sistema, skirta viso sprendimo metrikoms, įvykiams ir įspėjimams.

9.9 Viešumas

Klientas sutinka, kad viešojoje ar rinkodaros informacijoje IBM gali Klientą viešai vadinti „IBM SaaS“ prenumeratoriumi.

A priedas

1. „IBM Watson Health Core“

„IBM Watson Health Core“ – tai „Sveikatos duomenims pritaikyta“ platforma kaip paslauga („platform as a service“ – PaaS), kūrimo platforma ir operacinė posistemė, kuriose laikoma, tvarkoma ir apdorojama Saugoma informacija apie sveikatos būklę (PHI), kaip apibrėžia HIPAA, ir kiti Sveikatos duomenys, esantys IBM priklausančiuose arba valdomuose duomenų centruose, pagal IBM Taikomus duomenų apsaugos įstatymus. Klientas privalo įsigyti tinkamas teises „IBM Watson Health Core“ ir „IBM Watson Health Core Access“, kad būtų įgalintos toliau aprašytos funkcijos ir galimybės.

1.1 „Watson Health Core“ operacinės aplinkos

„Watson Health Core“ teisės apima tris Tinkamas sveikatos duomenims debesų kompiuterijos operacines aplinkas, kuriose Klientas gali apdoroti Sveikatos duomenis:

- Bandymo aplinka

  Suteikia izoliuotą aplinką, kurioje Klientai gali kurti ir tikrinti taikomąsias programas, sukurtas naudojant „IBM SaaS“. Bandomojoje aplinkoje realizuotos visos HIPAA saugos priemonės, išskyrus Avarinio atkūrimo, gero pasiekiamumo ir sistemos įrašų atsarginės kopijos priemonės.

- Gamybos aplinka

  Suteikia visą aplinką, kurioje Klientai gali diegti Sveikatos duomenų darbo krūvius. Gamybos aplinka yra gero pasiekiamumo, subalansuoto krūvio aplinka, kuri gali būti perjungta į Avarinio atkūrimo vietą.

- Avarinis atkūrimas

  Suteikia tikslią dubliuotą Gamybos aplinkos kopiją. Yra atskiroje duomenų centro vietoje.

1.2 Taikomosios programos kūrimas

„IBM Watson Health Core“ galima kurti taikomąją programą ir saugiai rinkti duomenis iš Kliento įrenginių arba Kliento įgaliotųjų vartotojų įrenginių. API suteikia programos sąsajas ir dokumentaciją, kurią Kliento įgaliotieji vartotojai, įskaitant Kliento trečiosios šalies paslaugos teikėjus, gali naudoti kurdami taikomąsias programas ir keisdamiesi duomenimis su „IBM SaaS“. Klientui arba jo kūrėjams naudojant API, jie privalo laikytis API kūrėjo reikalavimų.

- REST API

  „Watson Health Core“ suteikia seriją REST API ir paslaugų, skirtų „Watson Health Core“ platformai. API galimybės apima, neapsiribojant, prieigos prie duomenų saugyklų mechanizmus, duomenų tvarkymo paslaugą, vartotojų valdymą ir audito žurnalus.

- „Apple HealthKit“ ir „Apple ResearchKit“

  „Watson Health Core“ palaiko integravimą su „Apple ResearchKit“ API sistema, skirta tyrimams, atliekamiems naudojant „iOS“, ir su „Apple HealthKit“, skirta sveikatingumo duomenų fiksavimui.

1.3 Duomenų valdymas

- Sutikimų tvarkymas

  „Watson Health Core“ suteikia sistemą, skirtą pacientų arba tyrimo dalyvių duodamiems sutikimamsfiksuoti, kurioje galima saugiai laikyti sutikimų įrašus atskirai nuo duomenų apkrovos, kai asmuo įtraukiamas naudojant Kliento taikomąją programą, kurioje įjungta sutikimo funkcija.

- Duomenų maskavimas

  „Watson Health Core“ suteikia glaimybę atskirti vardų identifikatorius nuo struktūrizuotų duomenų apkrovų. „Watson Health Core“ gauna duomenis debesyje per programos API. API leidžia atskirti paciento arba asmens vardo identifikatorius nuo kitų duomenų apkrovų, kad būtų galima laikyti atskiroje šifruotoje duomenų saugykloje. Duomenų apkrovai priskiriamas anoniminis atpažinimo ženklas, kurį vėliau galima naudoti atsekant kilmę.

1.4 Sveikatos duomenų paslaugos

„Watson Health Core“ renka, laiko, sinchronizuoja duomenis, įskaitant struktūrizuotus ir nestruktūrizuotus išorinius Sveikatos duomenis ir kitą Asmeninę informaciją.

- Duomenų įdėjimas

  „Watson Health Core“ suteikia galimybę įdėti duomenis iš paciento taikomųjų programų arba įrenginių, naudojant programos API. „Watson Health Core“ kiekvienam Kliento Įgaliotajam individui suteikia teisę kiekvienais sutarties galiojimo metais įkelti į „Health Core“ ne daugiau nei 25 MB duomenų. Paslauga suteikia ne daugiau nei 10 įkėlimų Individui per dieną.

- Operacinė „Data Lake“

  Neapdoroti Kliento arba paciento duomenys „Watson Health Core“ laikomi pradine forma, kol bus panaudoti analizei ir modeliavimui.

- Gavimas, transformavimas, įkėlimas („Extract Transform Load“ – ETL)

  Duomenys transformuojami į normalizuotą formatą operacinėje posistemėje. Pramonės standartais pagrįsta „Enterprise Service Bus“, skirta sveikatos priežiūros įstaigoms, leidžia integruoti įvairiose Kliento taikomosiose programose ir protokoluose.

- Data Reservoir

  Sutvarkyti duomenys perkeliami į „Data Reservoir“. „Watson Health Core“ naudojami „IBM Unified Data Model for Healthcare“ aspektai normalizuoja verslo ir techninius sveikatos duomenis, skirtus naudoti analizei.

- Pagrindinis asmenų indeksas

  „Watson Health“ suteikia „Master Data Management“ įrankius, padedančius sujungti duomenis iš kelių šaltinių ir sukurti Ilgalaikį asmens įrašą (LPR).

2. Pasirenkamos funkcijos

2.1 „IBM Watson Health Core Terminology Service“

Ši papildoma paslauga palengvina duomenų integravimą iš esmės skirtingose sveikatos sistemose ir jų operacinį suderinamumą, užtikrindama nuoseklų klinikinės terminijos vartojimą visose „Watson Health Cloud“ taikomosiose programose. Ši paslauga suteikia funkcinę platformą visoms užduotims, kurios apima terminiją, kodų sistemas ir struktūrizuotą turinį, pvz.:

- naujų kodų sistemų kūrimą;
- tarptautinių kodų sistemų vertimą ir
- vietinių kodų sąrašų ir tarptautinių standartų susiejimą.

B priedas

IBM užtikrina toliau nurodytus „IBM SaaS“ pasiekiamumo paslaugos lygio sutarties (PLS) įsipareigojimus, kaip nurodyta TSD. PLS neteikia garantijų. PLS yra pasiekiama Klientui ir yra skirta naudoti tik gamybos aplinkose.

1. Pasiekiamumo kreditai

Pasiekiamumo permokų grąžinimas taikomas tik Individų teisių prenumeratos mokesčiams.

Sužinojęs, kad įvykis paveikė „IBM SaaS“ pasiekiamumą, Klientas turi per 24 valandas IBM techninio palaikymo centre užregistruoti 1 sudėtingumo lygio palaikymo kortelę. Klientas turi, kiek gali, padėti IBM diagnozuoti problemą ir ją išspręsti.

Palaikymo kortelės pretenzija dėl PLS sąlygų nesilaikymo turi būti pateikta per tris darbo dienas nuo sutartinio mėnesio pabaigos. Kompensacija už pagrįstą PLS pretenziją bus suteikta kaip kreditas būsimoje „IBM SaaS“ sąskaitoje faktūroje, atsižvelgiant į laikotarpį, per kurį „IBM SaaS“ gamybos sistema buvo nepasiekiama („Prastova“). Prastova skaičiuojama nuo tada, kai Klientas praneša apie įvykį, iki tada, kai „IBM SaaS“ atstatoma. Ji neapima laiko, susijusio su paslaugos teikimo nutraukimu dėl suplanuotos arba informuotos techninės priežiūros, dėl nuo IBM nepriklausančių priežasčių, problemų, susijusių su Kliento ar trečiosios šalies turiniu, technologijomis, dizainu ar instrukcijomis, nepalaikomų sistemų konfigūracijų ir platformų ar kitų Kliento klaidų arba Kliento sukeltų saugos problemų ar Kliento saugos tikrinimo. IBM taikys aukščiausią galimą kompensaciją, pagrįstą kiekvieno sutartinio mėnesio „IBM SaaS“ kaupiamuoju pasiekiamumu, kaip nurodyta toliau esančioje lentelėje. Bendra kompensacijos suma, atsižvelgiant į bet kurį sutartinį mėnesį, negali neviršyti 20 procentų vienos dvyliktosios (1/12) metinio mokesčio už „IBM SaaS“ dalies.

2. Paslaugų lygiai

„IBM SaaS“ pasiekiamumas per sutartinį mėnesį

Pasiekiamumas per sutartinį mėnesį	**Kompensacija (% mėnesio Individualios prenumeratos mokestis* sutartinį mėnesį, dėl kurio pareikšta pretenzija)**
<99,95 %	10 %
<99,0 %	20 %

* Jei „IBM SaaS“ buvo įsigyta iš IBM verslo partnerio, mėnesio prenumeratos mokestis bus apskaičiuojamas, atsižvelgiant į tuo metu galiojančiame kainoraštyje nurodytą „IBM SaaS“ kainą, kuri galioja pretenzijoje nurodytą sutartinį mėnesį, pritaikant 50 % nuolaidą. IBM suteiks nuolaidą Klientui tiesiogiai.

Pasiekiamumas, išreikštas procentine išraiška, apskaičiuojamas iš bendro minučių skaičiaus sutartinį mėnesį atėmus bendrą Prastovų minučių skaičių sutartinį mėnesį, gautą rezultatą padalijus iš bendro minučių skaičiaus sutartinį mėnesį.

Pavyzdžiui, sutartinį mėnesį iš viso buvo 108 Prastovos min.

Iš viso sutartinių mėnesį, kurį sudarė 30 dienų, buvo 43 200 min. - 108 min. Prastovų = 43 092 minutės _____ Iš viso 43 200 minučių	= 10 % Pasiekiamumo kredito už 99.75 % pasiekiamumo per sutartinį mėnesį

3. Išimtys

Ši PLS netaikoma:

- Be serverio stebėjimo, PLS netaikoma laikomiems virtualiesiems įrenginiams, palaikantiems pasirinktines arba Kliento taikomąsias programas.
- Jei Klientas pažeidė bet kokius esminius esamos sutarties įsipareigojimus.

C priedas

Šiame Saugos ir verslo tęstinumo priede („Security and Business Continuity Appendix“ – SBCA) nustatyti tam tikri IBM reikalavimai ir įsipareigojimai teikiant „IBM SaaS“ Klientui. Šiame priede nustatyti reikalavimai ir įsipareigojimai papildo „IBM SaaS“ duomenų saugos principų apraše nustatytus reikalavimus ir įsipareigojimus, kurie pasiekiami http://www.ibm.com/cloud/data-security. Didžiąja raide rašomų čia neapibrėžtų sąvokų reikšmės nurodytos Sutartyje arba Naudojimo sąlygose.

1. Informacijos saugos programa

IBM taiko vidaus saugos politikas, standartus ir procesus, kurie pagrįsti ISO 27001 sistema ir kontrolės sritimis. Kartu su IBM įmonės saugos organizacijos valdymu, reguliariai atliekami šių politikų, standartų ir procesų vidiniai auditai.

IBM palaiko organizacinių, operacinių, administravimo, fizinių ir techninių saugos priemonių, reguliuojančių Kliento turinio, kuris atitinka bent šio SBCA reikalavimus, apdorojimą, laikymą ir perdavimą, informacijos saugos programą.

Kliento prašymu IBM pasidalins su Klientu informacija apie „IBM Watson Health“ informacijos saugos programą, kad Klientas galėtų pagrįstai nustatyti jos nuolatinį tinkamumą, atitikimą ir efektyvumą. „IBM Watson Health“ informacijos saugos programa retkarčiai bus naujinama, kad atitiktų naujausias visuotinai priimtas pramonės praktikas ir IBM Taikomus įstatymus.

2. Prieigos valdikliai

IBM atskleis Kliento turinį tik savo darbuotojams, subrangovams arba trečiajai šaliai, kurie turės pagrįstų verslo poreikių pasiekti tokį Kliento turinį, kad padėtų IBM vykdyti savo įsipareigojimus Klientui ar kitiems asmenims, jei to reikia teikiant „IBM SaaS“ atitinkamai pagal Taikomus įstatymus, Sutarties arba Susieto dokumento sąlygas. Jeigu IBM yra Kliento Verslo partneris, IBM ir Klientas atskleis Asmeninę sveikatos informaciją tik laikydamiesi taikomų Šalių Verslo partnerio sutarties sąlygų.

IBM turi oficialų, vidinį vartotojo prieigos valdymo procesą, pagal kurį vartotojo prieigos oficialiai prašoma, ji patvirtinama patikrinus tapatybę ir suteikiama, atsižvelgiant į poreikį žinoti, taikant mažiausios privilegijos koncepciją. Prieiga prie Kliento turinio suteikiama tik aktyviems vartotojams ir aktyvioms vartotojų paskyroms. IBM turi aktyvių vartotojų paskyrų periodinio vidinio prieigos pakartotinio patvirtinimo oficialų procesą.

IBM naudoja saugius vartotojo autentifikavimo protokolus, įskaitant unikalių identifikatorių ir sudėtingų slaptažodžių priskyrimą aktyvių vartotojų paskyroms sistemose, kurios naudojamos teikiant paslaugas Klientui pagal IBM įmonės saugos standartus ir politikas:

a. Slaptažodžiai negali būti teikėjo pateikti numatytieji slaptažodžiai ir turi būti laikomi tokioje vietoje ir (arba) tokiu formatu, kuris nekeltų grėsmės duomenų, kurie juos naudojant saugomi, saugai.

b. Slaptažodžių rodymas ir spausdinimas turi būti užmaskuoti, glaudinti ar kitaip paslėpti, kad neįgaliotos šalys negalėtų stebėti ar vėliau jų atkurti. Slaptažodžių negalima registruoti arba fiksuoti įvedamų. Vartotojo slaptažodžių negalima laikyti paprastojo teksto formatu.

c. Bet kurios „IBM SaaS“ technologijos slaptažodžiai naudojami siekiant sumažinti riziką, susijusią su žinomais slaptažodžio ilgio pažeidžiamumais, ir turi būti dokumentuoti.

d. Kai dėl operacinių priežasčių reikia naudoti vidinius, konfidencialius, bendrinamus funkcinius ID, IBM tvarko bendrinamus, funkcinius ir (arba) Sistemos ID, dėl kurių, norint palaikyti individualią atskaitomybę, reikia registruoti slaptažodžius.

Visose sistemose ir taikomosiose programose, kuriose laikomas Kliento turinys, nustatomas neveiklumo skirtasis laikas.

Jei reikia, gavus Kliento prašymą ir IBM oficialiai patvirtinus, sukuriama nuotolinė prieiga prie IBM tinklo, sistemų ir taikomųjų programų, kuriose laikomas Kliento turinys, ir visi tokie ryšiai turi būti apsaugoti naudojant sudėtingus autentifikavimo ir šifravimo protokolus. Nuotolinės prieigos veikla turi būti užregistruota ir stebima.

Kiek to reikia teikiant „IBM SaaS“, IBM nuotoliniu būdu pasiekti bet kurią sistemą Kliento vidiniuose tinkluose, visos tokios nuotolinės prieigos bus atliekamos išskirtinai naudojant kliento saugios nuotolinės prieigos sistemas ir protokolus bei naudojant prieigos kredencialus, kuriuos Klientas pateikia IBM. Nuotolinė prieiga prie Kliento tinklo turi būti nustatoma tik gavus IBM prašymą ir Kliento patvirtinimą bei pagal tuo metu galiojančias Kliento politikas, kurios IBM bus pateiktos iš anksto. IBM naudojant Kliento vidaus tinklus bus taikomos Kliento IT naudojimo ir saugos politikos, kurios IBM bus pateiktos iš anksto.

IBM atskiria saugos administravimo, prieigos peržiūros ir saugos pažeidimų tyrimų pareigas.

Klientui būdingo Kliento turinio laikymas, išteklių nuoma ir apdorojimas yra logiškai atskirti nuo kitų IBM aptarnaujamų klientų. Tais atvejais, kai bendrai naudojamas laikymo, išteklių nuomos arba apdorojimo sritis autorizuos Klientas, IBM taikys procedūras ir saugos priemones, atitinkančias šioje SBCA išdėstytus reikalavimus, skirtus apsaugoti nuo neteisėto tokio Kliento turinio atskleidimo.

IBM realizuoja švaraus stalo / tuščio ekrano politikas, siekdama užtikrinti, kad Kliento turinys niekuomet nebūtų paliktas be priežiūros viešoje vietoje.

3. Perdavimas ir šifravimas

IBM imsis atitinkamų atsargumo priemonių perduodant Kliento turinį (faksu, el. paštu, kurjeriu ir t. t.), siekdama užtikrinti, kad naudojama teisinga gavėjo kontaktinė informacija, ir iš anksto susitardama su numatomu gavėju, kad apsaugotų tokios informacijos gavimą.

IBM naudoja ir nurodys naudoti IBM Personalui atitinkamų formų šifravimą ar kitas saugias technologijas visuomet, kai tai susiję su Kliento turinio apdorojimu, įskaitant, kai tai susiję su Kliento turinio perkėlimu, perdavimu, nuotoline prieiga arba saugykla (įskaitant atsarginės kopijos saugyklą). Pavyzdžiui, IBM, naudodama atitinkamą pramonės standarto šifravimą, šifruos visus įrašus ir failus, kuriuose yra Kliento turinio:

a. laikomo IBM nešiojamuosiuose kompiuteriuose, nešiojamuosiuose įrenginiuose arba nešiojamojoje elektroninėje medijoje, įskaitant atsarginių kopijų juostas, kurios perkeliamos į išorinę saugyklą;

b. laikomo arba transportuojamo IBM už Kliento arba IBM fiziškai apsaugotų biurų ir infrastruktūros ribų, išskyrus spausdintinius popierinius dokumentus;

c. IBM perkeliant viešuosiuose tinkluose;

d. iš IBM sistemų perduodant Klientui;

e. IBM perduodant belaidžiu būdu; ir

f. IBM laikomo serveriuose ir duomenų bazėse.

4. Tinklo sauga

IBM naudoja pagrįstai naujas sistemos saugos programinės įrangos, pvz., užkardų, tarpinių serverių, žiniatinklio taikomųjų programų užkardų ir sąsajų, versijas. Į tokią programinę įrangą turi būti įtraukta apsauga nuo kenkėjiškų programų ir pagrįstai naujos pataisos bei virusų apibrėžimai. Pagal įmonės standartus antivirusinė programinė įranga turi būti įdiegta darbo stotyse, serveriuose ir susijusiuose galiniuose taškuose, kur techniškai įmanoma, ir programinė įranga tvarkoma pagal įmonės politiką, taikant vidaus valdymo sprendimus.

IBM stebi „IBM SaaS“, kad kuo anksčiau aptiktų ir identifikuotų saugos incidentus. IBM naudos aptikimo įrankius, kurie atitinka bent pramonės standartą, ir taikys prevencijos, stebėjimo ir reagavimo procesus taip, kad identifikuotų tiek vidaus, tiek išorės pažeidžiamumus ir rizikas, dėl kurių gali įvykti Kliento turinio arba informacijos sistemų, kurios naudojamos Kliento paslaugų teikimų, neteisėtas atskleidimas, netinkamas naudojimas, pakeitimas arba sunaikinimas.

IBM prenumeruoja pažeidžiamumo informacijos paslaugas arba informacijos saugos konsultacijas ir kitus susijusius šaltinius, teikiančius naujausią informaciją apie sistemų pažeidžiamumus. IBM reguliariai atlieka savo tinklo pažeidžiamumo įvertinimą ir taisymus.

IBM stebi „IBM SaaS“, kad aptiktų, identifikuotų, sulaikytų ir išspręstų Saugos incidentus.

IBM patvirtina tinklo saugos infrastruktūros, kurioje pasiekiama „IBM SaaS“, pasiekiamumą, vientisumą ir efektyvumą, taikydama IBM leidimų tvarkymo procesus.

5. Incidentų valdymas ir pranešimai

„IBM Watson Health“ komanda dirba kartu su IBM reagavimo į kibernetinės saugos incidentus komanda, kuri tvarko saugos incidentų, susijusių su IBM pasiūlymais, gavimą, tyrimą ir vidinį koordinavimą, ir

realizuoja prevencinius veiksmus, būtinus siekiant sumažinti su programine įrangą susijusių saugos problemų skaičių. „Saugos incidentas“ – tai sėkminga neteisėta prieiga, naudojimas, atskleidimas, modifikavimas ar sąveika su sistemos operacijomis arba duomenimis informacijos sistemoje, kurią IBM naudoja „IBM SaaS“ teikimui. Aptikus Saugos incidentą (įprastinio nuskaitymo metu, gavus pavojaus signalą, slenkstinį įvykį ir pan.), IBM pateiks informaciją ir praneš Klientui:

a. apie visus patvirtintus Saugos incidentus, susijusius su Kliento turiniu, kai tik tai bus įmanoma, bet ne vėliau nei per 2 darbo dienas po tokio Saugos incidento tyrimo ir patvirtinimo;

b. iš karto gavus prieigos arba informacijos užklausą apie bet kokį Kliento turinį iš vyriausybinės institucijos (įskaitant duomenų apsaugos agentūras arba teisėsaugos institucijas), jei to nedraudžia įstatymai arba atitinkamas nurodymas; ir

c. išskyrus, kaip leidžiama šios SBCA skyriuje „Prieigos valdikliai“, prieš atskleidžiant, perduodant Kliento turinį arba suteikiant prieigą prie jo trečiajai šaliai.

6. Prisijungimas

IBM, atsižvelgdama į IBM politikas, praktikas ir visuotinai priimtas pramonės praktikas, atlieka pagrįstą sistemų stebėjimą dėl neteisėto Kliento Apdorojamų duomenų naudojimo arba prieigos prie jų. Faktiniai prisijungimo pažeidimai arba jų mėginimai ir prieigos pažeidimai bus registruojami.

IBM laiko visų prieigos užklausų įrašus ir prieigos veiklų žurnalus visų sistemų, kuriose laikomi, pasiekiami, apdorojami ir perduodami Kliento ir Sveikatos duomenys tiek, kiek to reikalauja HIPAA ir kiti IBM Taikomi duomenų apsaugos įstatymai.

Į žurnalus ir ataskaitas įtraukta tokia minimali informacija: (i) visi tiek sėkmingi, tiek nesėkmingi prisiregistravimo bandymai, įskaitant pagrįstą identifikavimo informaciją; (ii) visi sistemos ir tinklo konfigūracijos keitimai, įskaitant taikomųjų programų diegimus, vartotojų tvarkymo keitimus ir prieigos prie failų teisių modifikavimus; (iii) tiek sėkmingi, tiek nesėkmingi prieigos prie išteklių bandymai, įskaitant bandymus pasiekti failus, bendrai naudojamus tinklo objektus, žurnalą ar kitus išteklius; ir (iv) duomenų atsisiuntimai, įskaitant turinio duomenų tipą ir atsisiuntimui naudotą prieigos protokolą.

7. Programinės įrangos kūrimas ir keitimų tvarkymas

IBM taiko saugaus taikomųjų programų kūrimo ir kodavimo praktikų, kurios apsaugo gamybos taikomųjų programų vientisumą ir susijusio šaltinio kodą nuo neteisėtų ir nepatikrintų modifikavimų.

IBM taiko keitimų valdymo procesą, kuris apima (a) keitimų registravimą ir oficialų patvirtinimą bei gražinimo procedūras; ir (b) atitinkamą tokių keitimų tikrinimą, įskaitant, kai reikia, vartotojo sutikimą tikrinti bei saugos patikrą.

IBM palaiko pataisų tvarkymo procesą, kuris apima pataisų tikrinimą prieš diegiant visose sistemose, kurios naudojamos saugant Kliento turinį, prieigai prie jo ir perdavimui arba naudojamos tiekiant paslaugas, įskaitant „IBM SaaS“, Klientui.

IBM reikalauja, kad sistemos administratoriai laikytų visą, tikslią ir naujausią informaciją, susijusią su konfigūracija visų informacijos sistemų, naudojamų saugant, pasiekiant ir perduodant Kliento turinį.

8. Fizinė ir aplinkos sauga

„IBM Watson Health Core“ platforma įdiegta „IBM SoftLayer“ duomenų infrastruktūroje. „IBM SoftLayer“ palaiko fizinę ir aplinkos saugą, prieigos kontrolę, valdymo priemones ir procesus, kurie apsaugo Kliento duomenis nuo žmonių, aplinkos ir techninių pažeidimų arba poveikio.

Bendroji prieiga prie infrastruktūrų, kuriose laikoma „IBM SaaS“, kontroliuojama naudojant kortelių prieigos sistemą. Visose vietose sumontuotos uždaro tinklo televizijos sistemos („Closed circuit television“ – CCTV) kameros, kurias stebi apsaugos darbuotojai. Pasirinktos įėjimo durys prijungtos prie signalizacijos, kurią stebi apsaugos darbuotojai.

Prieiga prie kontroliuojamų zonų apribota naudojant prieigą kortelėmis ir (arba) papildomą biometrinį patvirtinimą. Visi asmenys, neturintys leidimo patekti į kontroliuojamas zonas, privalo užsiregistruoti ir būti lydimi asmens, turinčio leidimą patekti į kontroliuojamą zoną. Visi kontroliuojamos zonos avariniai išėjimai prijungti prie garsinės signalizacijos, kurią stebi apsaugos darbuotojai. Periodiškai atliekamas signalizacijos veikimas dokumentuojamas, o dokumentai saugomi. Patekimo į kontroliuojamas zonas teisės kas ketvirtį tvirtinamos visiškai iš naujo. Patekimas į kontroliuojamas zonas panaikinamas nutraukus darbo sutartį.

Infrastruktūros yra apsaugotos nuo aplinkos veiksnių, pvz., ugnies, vandens ir karščio, naudojant gaisrines signalizacijas, gesintuvus, dūmų signalizatorius ir ugnies gesinimo slopinimo ir gesinimo sistema. Infrastruktūros yra apsaugotos nuo maitinimo nutraukimų ar trikčių, naudojant nepertraukiamo maitinimo šaltinių („Uninterruptible Power Supply“ – UPS) sistemas ir atsarginius generatorius, kurie reguliariai prižiūrimi ir tikrinami.

„IBM SoftLayer“ atitikties informaciją ir ataskaitas galima rasti šiuo adresu: http://www.softlayer.com/compliance.

9. Verslo operacijų tęstinumas

IBM turi verslo tęstinumo ir avarinio atkūrimo planus, kurie užtikrina paslaugos lygio palaikymą pagal šioje Sutartyje numatytus įsipareigojimus. Tokie verslo tęstinumo ir avarinio atkūrimo planai bus periodiškai atnaujinami ir tikrinami (bent kartą per metus). IBM realizuos visus pagrįstus verslo tęstinumo ir avarinio atkūrimo planų keitimus, būtinus siekiant išlaikyti atitiktį su visuotinai priimtoms pramonės praktikoms, kiekvienu atveju nepagrįstai neliečiant Kliento naudojamos „IBM SaaS“ arba gamybos aplinkos.

Įvykus nelaimei, dėl kurios „IBM SaaS“ taptų nepasiekiama Klientui, IBM nedelsdama praneš Klientui ir pradės vykdyti verslo tęstinumo ir (arba) avarinio atkūrimo planą. Pranešus apie nelaimę, „IBM SaaS“ verslo tęstinumo tikslas yra atkurti Kliento prieigą prie „IBM SaaS“ taip: prastovos atveju Duomenų atkūrimo laikas (DAL), per kurį reikia atkurti „IBM Watson Health“ gamybos aplinką, yra 36 valandos nuo nelaimės paskelbimo. Duomenų atkūrimo taškas (DAT) yra ne daugiau nei 24 valandos nuo Kliento turinio praradimo gamybos aplinkoje. Konkrečių „Watson Health“ sprendimų verslo tęstinumo tikslai gali skirtis.

IBM avarinio atkūrimo sprendimas apima kelis duomenų centrus nutolusiose viena nuo kitos geografinėse srityse.

Visuose „IBM SoftLayer“ duomenų centruose naudojamos kelios maitinimo linijos, skaidulinės jungtys, paskirtieji generatoriai ir atsarginiai akumuliatoriai. Jie pagaminti naudojant geriausią pramonės šakos aparatūrą ir įrangą, užtikrinant aukščiausią našumo, patikimumo ir operacinio suderinamumo lygį. Tikrinamas visų duomenų centruose naudojamų duomenų centro komponentų, pvz., užtikrinančių perteklinius n+1 galios ir aušinimo išteklius, stabilumas.

10. Laikymasis

IBM saugos praktikos pagrįstos ISO 27001-27002. Šios praktikos suteikia kontrolės struktūras, skirtas, neapsiribojant, Rizikos analizei, Fizinei saugai, Avariniam planavimui, Tyrimams, Informacijos apsaugai, Mokymui, Duomenų apsaugai ir Operacijoms.

IBM peržiūri, ar su sauga ir privatumu susijusios veiklos atitinka IBM saugos praktikas.

IBM laikosi IBM Taikomų duomenų apsaugos įstatymų Aprėpties jurisdikcijose.

Tinkamai tvarkyti Kliento konfidencialią informaciją reikalauja ir IBM Verslo elgesio nuostatos, kurias kasmet turi peržiūrėti visi darbuotojai (ir patvirtinti, kad peržiūrėjo).

11. Įvairios kitos sąlygos

IBM užtikrins, kad jos sutartys su visais subrangovais ir (arba) trečiosiomis šalimis, susijusiomis su „IBM SaaS“ teikimu, nustatytų sąlygas, kurios ne mažiau nei šios SBCA apsaugotų Kliento turinį, ir turėtų atitinkamą Susietą dokumentą, kuriuos tokių sąlygų taikymo paslaugoms aprėptimi vykdytų šie subrangovai ir (arba) trečiosios šalys.