IBM Felhasználási Feltételek – SaaS Ajánlatra Vonatkozó Feltételek

IBM Watson Health Core

A Felhasználási Feltételeket („Felhasználási Feltételek”) a jelen IBM Felhasználási Feltételek – SaaS (Szoftver, mint Szolgáltatás) Ajánlatra Vonatkozó Feltételek („SaaS Ajánlatra Vonatkozó Feltételek”) és az IBM Felhasználási Feltételek – Általános Feltételek („Általános Feltételek”) című dokumentum alkotja, amely a következő URL-címen érhető el: http://www.ibm.com/software/sla/sladb.nsf/sla/tou-gen-terms/.

Abban az esetben, ha ellentmondás merül fel, a SaaS Ajánlatra Vonatkozó Feltételek irányadóak az Általános Feltételekkel szemben. Az IBM SaaS megrendelésével, elérésével vagy használatával az Ügyfél elfogadja a Felhasználási Feltételeket.

A jelen Felhasználási Feltételekre az IBM Nemzetközi Passport Advantage Megállapodás, az IBM Nemzetközi Passport Advantage Express Megállapodás vagy az IBM Nemzetközi Megállapodás Kijelölt IBM SaaS Ajánlatokhoz („Megállapodás”) feltételei irányadóak, és a Felhasználási Feltételekkel (ToU) együtt ezek alkotják a teljes megállapodást.

1. IBM SaaS - Szoftver, mint Szolgáltatás

A következő IBM SaaS Ajánlatokra az alábbi SaaS Egyedi Ajánlatokra vonatkozó Feltételek alkalmazandóak:

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

2. Díjakkal kapcsolatos mérőszámok

Az IBM SaaS értékesítése a következő díjszabási egységek egyike szerint történik, a Tranzakciós Dokumentumban meghatározottak szerint:

a. A **Hozzáférés** olyan mértékegység, amely alapján az IBM SaaS megvásárolható. A Hozzáférés az IBM SaaS használatára vonatkozó jogosultságokat jelenti. Az Ügyfélnek egyszeri Hozzáférési jogosultságot kell beszereznie az IBM SaaS az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során történő használatához.

b. Az **Egyén** olyan mértékegység, amely alapján az IBM SaaS megvásárolható. Az Egyén egy tárgy vagy emberi lény lehet. Megfelelő jogosultságokat kell beszerezni annak érdekében, hogy biztosítani lehessen az Ügyfél Felhasználási Engedélyében (PoE) vagy Tranzakciós Dokumentumában meghatározott mérési időszakban az IBM SaaS által feldolgozott vagy kezelt összes Egyént.

   A jelen IBM SaaS esetén Egyénnek számít az a személy, eszköz vagy mobilalkalmazás, amelynek adatait az IBM SaaS kezeli.

c. **Példány** – olyan mértékegység, amely alapján az IBM SaaS megvásárolható. A Példány hozzáférést biztosít az IBM SaaS egy megadott konfigurációjához. Megfelelő jogosultságokat kell beszerezni az IBM SaaS minden egyes Példányához, amely az Ügyfél Felhasználási Engedélyében (PoE) vagy a Tranzakciós Dokumentumban meghatározott mérési időszak során hozzáférhető és használható.

3. Díjak és számlázás

Az IBM SaaS termékért fizetendő összeg a Tranzakciós Dokumentumban van meghatározva.

3.1 Részleges Havi Díjak

Amennyiben a Tranzakciós Dokumentum így rendelkezik, részleges havi díj alkalmazandó.

3.2 Többlethasználat díjak

Ha az Ügyfél tényleges IBM SaaS használata a mérési időszak alatt meghaladja a Felhasználási Engedélyben meghatározott jogosultságot, az Ügyfélnek a Tranzakciós Dokumentumban meghatározottak szerint többlethasználati díjat kell fizetnie a kiállított számla alapján.

4. Előfizetési időszak és Megújítási lehetőségek

Az IBM SaaS előfizetési időszaka azon a napon kezdődik, amikor az IBM értesíti az Ügyfelet, hogy hozzáférést kapott az IBM SaaS Próba működési környezetéhez, a Megrendelési Dokumentumban foglaltaknak megfelelően. Az Egyén jogosultságokhoz tartozó előfizetési időszak akkor kezdődik, amikor az IBM értesíti az Ügyfelet, hogy hozzáférést kapott a Termelési működési környezethez. A Megrendelési Dokumentum határozza meg, hogy az IBM SaaS automatikusan megújul, folyamatos használat alapján folytatódik vagy megszűnik az előfizetési időszak végén.

Az automatikus megújulás esetében, amennyiben az Ügyfél nem kéri írásban a megújítás felfüggesztését az előfizetési időszak lejárati dátuma előtt legalább 90 nappal, az IBM SaaS automatikusan megújul a Felhasználási Engedélyben meghatározott időszakra.

Folyamatos használat esetén az IBM SaaS folyamatosan, hónapról hónapra elérhető, amíg az Ügyfél nem kéri 90 nappal korábban írásos értesítés formájában a megszüntetést. Az IBM SaaS a 90 napos időszak lejárta után a naptári hónap végéig elérhető marad.

5. Technikai Támogatás

Az IBM rendelkezésre bocsátja az IBM Szolgáltatásként kínált szoftver Támogatási kézikönyvet, amely a technikai támogatás kapcsolattartási adatait, a karbantartási időpontokat, illetve egyéb információkat és folyamatokat tartalmaz. A technikai támogatás kapcsolattartási adatai és a támogatási tevékenységekkel kapcsolatos egyéb információk az IBM SaaS Támogatási kézikönyvben érhetők el a https://support.ibmcloud.com címen.

Az IBM SaaS technikai támogatása és az egyszerű konfigurációs kérések biztosítása elektronikus igénylés útján történik. A Technikai Támogatás az IBM SaaS termék részét képezi, és önálló ajánlatként nem érhető el.

A bejelentett problémákról szóló dokumentációban vagy információk között nem szerepelhet semmilyen személyes adat (PI), beleértve a védett egészségügyi adatokat (PHI) és a bizalmas személyes adatokat (SPI).

6. Meghatározások

Vonatkozó jogszabályok – a jelen Felhasználási Feltételek teljesítésére vonatkozó, kormányzati hatóság által kiadott törvényeket, határozatokat, jogszabályokat, szabályokat, rendeleteket, irányelveket és egyéb előírásokat vagy az általánosan elfogadott iparági szabványokat jelentik.

API – alkalmazásprogramozási felület, amely rutinok, protokollok és eszközök készlete szoftveralkalmazások létrehozásához. Az API határozza meg a szoftverösszetevők interakcióját, illetve az API-k használatával történik a grafikus felhasználói felület (GUI) összetevőinek programozása.

Jogosult Adminisztrátor – az Ügyfél bármely alkalmazottja, jóváhagyott alvállalkozója, az Ügyfélhez tartozó személy vagy csoport, aki a platform fenntartásának és megbízható működésének felügyeletéért felelős. A kötelezettségek a konfigurálást, támogatást, továbbá a felhasználók és a fiókok kezelését foglalhatják magukban. Az adminisztrátor olyan klinikai vizsgáló is lehet, aki egy tanulmánynak a Watson Health rendszerben történő beállításáért felelős.

Jogosult Egyén – bármely hitelesített személy, mobilalkalmazás vagy eszköz, amely hozzáférést kapott adatoknak a Watson Health Core rendszerbe való küldéséhez szükséges hozzáférési jogokhoz. Ilyen személy lehet az Ügyfél, illetve a tanulmányok résztvevői, ügyfelek vagy az Ügyfél betegei.

Ügyfélre Vonatkozó Adatvédelmi Jogszabályok – azon Adatvédelmi Jogszabályok, amelyek az Ügyfélnek a Megállapodásban, a Kapcsolódó Dokumentumokban, illetve a vonatkozó Szolgáltatásleírásokban, Megrendelési Dokumentumokban és a Felek közötti Munkaleírásokban foglalt kötelezettségeinek a teljesítésére vonatkoznak.

Ügyféladatok – minden az Ügyfél által vagy számára az IBM SaaS rendszerbe bevitt adat, függetlenül attól, hogy az adat az Ügyfél saját adata vagy az Ügyfél egy ügyfele vagy bármely harmadik fél által vagy nevében megadott adat, beleértve a harmadik felek egészségügyi eszközeiből származó adatokat.

Adatvédelmi Jogszabályok – bármely, az adatvédelemmel és adatbiztonsággal kapcsolatos Vonatkozó Jogszabály.

Adatalany – azonosított vagy azonosítható személy, akihez Személyes Adatok tartoznak.

Kijelölt Adatközpont – az Ügyfél IBM SaaS példányát futtató azon adatközpont(ok), amely(ek)et elsődleges és katasztrófa utáni helyreállítási adatközpontnak határoztak meg a Tranzakciós Dokumentumban, amennyiben van ilyen.

Egészségügyi Adatok – bármely olyan adat vagy információ (képeket is beleértve), amelyek egészségügyi állapothoz kapcsolódó Személyes Adatnak minősülnek.

Egészségügyi Adatok Átvitelére Alkalmas – az IBM SaaS vonatkozásában az IBM SaaS azon képességét jelenti, miszerint megfelel az illetékes joghatóságok Egészségügyi Adatok kezelésére vonatkozó biztonsági és adatvédelmi szabványainak, jogszabályainak és rendeleteinek, beleértve a HIPAA-t végrehajtó rendeletek 164. szakaszának A és C alrészeiben foglalt megvalósítási specifikációkat (a HITECH törvény általi módosításoknak megfelelően), valamint az Egészségügyi Adatok tekintetében hatályok egyéb Vonatkozó Jogszabályokat, ez azonban nem jelenti azt, hogy az IBM Üzlettársként vagy Adatkezelőként jár el.

HIPAA – az Egyesült Államok 1996-ban született, az egészségbiztosítás hordozhatóságáról és elszámoltathatóságáról szóló, módosított törvénye (Health Insurance Portability and Accountability Act), beleértve a 2009-es, az amerikai gazdasági helyreállításról és az új befektetésekről szóló törvény (American Recovery and Reinvestment Act) gazdasági és egészségügyi információk egészségügyi informatikai támogatásának bevezetéséről szóló törvényét (Health Information Technology for Economic and Clinical Health Act) („HITECH törvény”), a HIPAA értelmében az Egyesült Államok Egyesült Államok minisztériuma által a 45 C.F.R. 160. és 164. szakaszában kihirdetett bizonyos rendeleteket, valamint a HITECH törvény értelmében kihirdetett bizonyos rendeleteket is.

IBM-re Vonatkozó Adatvédelmi Jogszabályok – azon Adatvédelmi Jogszabályok, amelyek az IBM vállalatnak a Megállapodásban, a Kapcsolódó Dokumentumokban, illetve a vonatkozó Szolgáltatásleírásokban, Megrendelési Dokumentumokban és a Felek közötti Munkaleírásokban foglalt kötelezettségeinek a teljesítésére vonatkoznak.

IBM Személyzete – (a) az IBM, annak Társvállalatai és alvállalkozói, valamint ezek alkalmazottai; és (b) harmadik félnek minősülő beszállítók, amelyek az IBM nevében teljesítenek szolgáltatásokat a Megállapodás és a vonatkozó Kapcsolódó Dokumentumok értelmében, vagy amelyeknek az IBM más módon engedélyezi az Ügyfél Személyes Adataihoz való hozzáférést.

Hatókörbe Tartozó Országok – az Európai Unió 28 tagállama és Svájc, valamint azok az országok, amelyeket az IBM időnként hozzáadhat ehhez a listához.

Személyes Adatok vagy **Személyes Információk** – bármilyen adathordozón vagy formátumban, beleértve az elektronikus és papíralapú feljegyzéseket, tárolt azon adatok, amelyek egy azonosított vagy azonosítható személyhez kapcsolódnak. Az „azonosítható személy” olyan személy, aki közvetlen vagy közvetett módon azonosítható, különösen egy azonosító számra vagy a személy fizikai, fiziológiai, mentális, gazdasági, kulturális vagy társadalmi önazonosságára vonatkozó egy vagy több tényezőre történő utalás révén.

Feldolgozás és annak változatai, például **feldolgoz** (kis- vagy nagybetűvel írva) – az adatokkal automatikus vagy nem automatikus módon végzett bármely művelet vagy műveletek összessége, például gyűjtés, rögzítés, rendszerezés, tárolás, átalakítás vagy megváltoztatás, visszakeresés, betekintés, felhasználás, közlés továbbítás útján, terjesztés vagy egyéb módon történő hozzáférhetővé tétel révén, összehangolás vagy összekapcsolás, zárolás, törlés, illetve megsemmisítés.

Feldolgozott Adat – bármilyen adat, bizalmas vagy védett információk vagy anyagok, beleértve az Egészségügyi Adatokat és a Személyes Adatokat, amelyet az IBM a Megállapodás, Kapcsolódó Dokumentum és/vagy Szolgáltatásleírás, Megrendelési Dokumentum és/vagy a Munkaleírás értelmében feldolgozott.

Biztonsági Incidens – az SBCA-ban foglaltaknak megfelelő jelentéssel bír.

7. Fiókkezelés

Az IBM SaaS kizárólag az Ügyfél jogosult felhasználói („**Jogosult Adminisztrátorok**” vagy „**Jogosult Egyének**”) számára érhető el. Az Ügyfél szabályozza az IBM SaaS elérésére jogosult fiókokat, amely magában foglalhatja a jogosult alkalmazásokat, az Ügyfél személyzetét, az Ügyfél harmadik félnek minősülő szolgáltatóit és alvállalkozóit, és kizárólag az Ügyfél felelős (i) a jogosult felhasználók szabályozásáért, korlátozás nélkül beleértve bármely jogosult felhasználó személyazonosságának az ellenőrzését; és (ii) annak biztosításáért, hogy kizárólag jogosult felhasználók férhessenek hozzá az IBM SaaS ajánlathoz.

A Jogosult Egyének, akik az Ügyfél ügyfelei, betegei vagy tanulmányának résztvevői, hozzáférést kaphatnak kizárólag adatoknak az IBM SaaS ajánlatba való feltöltésének céljából, mely esetben ezen Jogosult Egyének nem rendelkezhetnek más hozzáféréssel az IBM SaaS ajánlathoz.

8. Adatvédelem

8.1 Általános követelmények

A Felek között fennálló viszony tekintetében az Ügyfél az Ügyfél Személyes Adatainak kizárólagos kezelője, az Ügyfél adatfeldolgozónak bízza meg az IBM vállalatot. A Vonatkozó Adatvédelmi Jogszabályoknak megfelelően, az Ügyfél jogosult utasításokat adni az IBM vállalatnak az Ügyfél Személyes Adatainak az IBM általi feldolgozásával kapcsolatban.

Az Ügyfél Személyes Adatainak az IBM által történő feldolgozása közben az IBM:

a. megfelel az IBM-re Vonatkozó Adatvédelmi Jogszabályoknak; és

b. nem vegyíti az Ügyfél Személyes Adatait más forrásokból származó adatokkal, kivéve:

- amennyiben az IBM SaaS biztosítása szempontjából szükséges, illetve más célból nem, kivéve, ha az Ügyfél kifejezetten másként nem rendelkezett; vagy
- a jelen Felhasználási Feltételeknek és az SBCA Függeléknek megfelelően.

Az Ügyfél Személyes Adatainak az IBM által történő feldolgozása közben az Ügyfél:

a. megfelel az Ügyfélre Vonatkozó Adatvédelmi Jogszabályoknak;

b. felelősséget vállal az Ügyfél és az Ügyfél Társvállalatai, betegei, végfelhasználói, az Adatalanyok és/vagy az Ügyfél más, harmadik felei közötti kommunikációért;

c. adatfeldolgozási megállapodásokat köt az adatkezelőivel, akiknek engedélyezniük kell az IBM, mint adatfeldolgozó és az IBM alfeldolgozói számára az Ügyfél Személyes Adatainak a feldolgozását; és

d. az IBM egyedüli kapcsolattartójaként szolgál, valamint kizárólagos felelősséget vállal az Ügyfél Társvállalataitól – amelyek az IBM felé további adatkezelőként lépnek fel – származó utasítások és kérések belső koordinálásáért, áttekintéséért és elküldéséért. Az IBM nem köteles tájékoztatni és értesíteni az Ügyfél bármely, adatkezelőnek minősülő Társvállalatát, amennyiben az ilyen információt vagy értesítést biztosított az Ügyfél számára. Az IBM jogosult visszautasítani bármilyen utasítást, amelyet az Ügyfél olyan adatkezelőnek minősülő Társvállalatától kapott, amely nem az Ügyfél.

Egyik fél sem kötelezett az adott félre vonatkozó Adatvédelmi Jogszabályokat sértő módon eljárni.

8.2 Ügyféladatokkal kapcsolatos jogok

Az Ügyfél kijelenti és szavatolja, hogy (a) birtokolja az IBM SaaS ajánlatba bevinni kívánt adatokat, vagy (b) beszerzett minden olyan jogosultságot, engedélyt, hozzájárulást és jóváhagyást, és felelősséget vállal ezek fenntartásáért, amelyek szükségesek azon jogosultságok biztosításához az IBM számára, amelyek lehetővé teszik az Ügyféladatokhoz való hozzáférést és azok használatát és közzétételét a jelen Felhasználási Feltételekben vagy a Megállapodásban foglaltaknak megfelelően, vagy az IBM számára az IBM SaaS biztosításához szükséges más módon. Az Ügyfél továbbá kijelenti és szavatolja, hogy az Ügyféladatok kizárólag (a) az Amerikai Egyesült Államokban lakó egyénekhez kapcsolódnak, mely esetben kizárólag az Amerikai Egyesült Államokban található adatközpontban viszi be azokat az IBM SaaS ajánlatba, vagy (b) a Hatókörbe tartozó egy vagy több országban lakó egyénekhez kapcsolódnak, mely esetben kizárólag a Kijelölt Adatközpont(ok)ban viszi be azokat az IBM SaaS ajánlatba.

8.3 Adatokkal kapcsolatos szolgáltatások és kötelezettségek

a. Az Ügyfél beleegyezik, hogy kizárólag olyan elemzést végez vagy olyan elemzés elvégzését kéri az IBM vállalattól az Ügyféladatokon, amely az Ügyfél „egészségügyhöz kapcsolódó műveleteinek” vagy „kutatásainak” minősülő tevékenységekkel áll összefüggésben, amelyeket a HIPAA-ban foglaltak és/vagy egyéb Vonatkozó Adatvédelmi Jogszabályokban található hasonló fogalmak határoznak meg, illetve hogy az Ügyfél az Ügyféladatokat kizárólag minden vonatkozó követelménynek (például Intézményi Felülvizsgálati Testület döntése vagy joglemondás, ha szükséges) megfelelően használja fel vagy utasítja az IBM vállalatot azok felhasználására az Ügyfélre Vonatkozó jelen vagy más Adatvédelmi Jogszabályok értelmében.

b. Az Ügyfél kizárólagos felelőssége a Hatókörbe Tartozó Országokban hatályos Ügyfélre Vonatkozó Jogszabályok alapján szükséges bármilyen és minden regisztráció, hozzájárulás, jogosultság és engedély beszerzése, korlátozás nélkül beleértve a HIPAA-t és bármely más vonatkozó adatvédelmi és -biztonsági törvényt, szabályt és rendeletet, annak érdekében, hogy az Ügyfél, az IBM és az IBM jogosult alvállalkozói az Ügyféladatokat bevihessék az IBM SaaS ajánlatba, illetve felhasználhassák és közzétehessék azokat a jelen Felhasználási Feltételekben és a Megállapodásban foglaltak szerint. Az IBM nem felelős az ilyen regisztrációk, hozzájárulások, jogosultságok és engedélyek beszerzésének, illetve ezek szükségességének nyomon követéséért.

c. Az Ügyfél kizárólagos felelőssége annak biztosítása, hogy az IBM SaaS ajánlatba bevitt minden Ügyféladat kizárólag az Amerikai Egyesült Államokban vagy a Hatókörbe tartozó országokban tartózkodó egyénekre kapcsolódó adatokra korlátozódik.

d. Az IBM olyan támogatási központokat biztosít, amelyek személyzete képzésben részesült a HIPAA-ban és a Hatókörbe tartozó országokból származó adatokra hatályos egyéb IBM-re Vonatkozó Adatvédelmi Jogszabályokban foglaltak tekintetében.

8.4 Biztonsági Intézkedések és Biztonsági Incidensek

a. Az IBM technikai és szervezeti intézkedéseket (beleértve szervezeti folyamatokat és eljárásokat, valamint bármely, a jelen Felhasználási Feltételekben és a SBCA-ban meghatározott vagy hivatkozott különleges biztonsági kötelezettséget) valósít meg, tart fenn és követ az Ügyfél Személyes Adatainak jogosulatlan használattal vagy hozzáféréssel, véletlen adatvesztéssel, sérüléssel, módosítással, megsemmisüléssel, lopással vagy jogosulatlan közzététellel szembeni védelme érdekében.

b. Abban az esetben, amennyiben az IBM tudomást szerez az Ügyfél Feldolgozott Adatait érintő Biztonsági Incidensről (az SBCA-ban foglaltaknak megfelelően), az IBM tájékoztatja az Ügyfelet az SBCA-ban és az IBM-re Vonatkozó Adatvédelmi Jogszabályokban foglalt feltételeknek megfelelően, továbbá az ilyen értesítés információt biztosít bármely, az Ügyfelet vagy bármely Adatalanyt (ha van ilyen) érintő, ilyen Biztonsági Incidens által okozott ismert hatásról és az IBM által elvégzett vagy javasolt javító intézkedésről.

8.5 Érdeklődések és panaszok fogadása

Az IBM azonnal és, az IBM-re Vonatkozó Adatvédelmi Jogszabályok által megengedett mértékig, nem több mint öt (5) munkanapon belül írásban értesíti az Ügyfelet az IBM Watson Health adatvédelmi tisztségviselőjéhez beérkezett érdeklődésről, kommunikációról vagy panaszról, amelyet az IBM az Ügyfél Személyes Adataival kapcsolatban kap a következőktől:

a. bármely Adatalanytól az Adatalanyhoz kapcsolódó azon Személyes Adatokkal kapcsolatban, amelyeket az IBM dolgozott fel. Az Ügyfél kötelessége válaszolni az Adatalanyok ilyen kéréseire, és az IBM vállalja, hogy betartja az Ügyfél ésszerű utasításait, segítve az Ügyfél válaszát az ilyen kérésekre. Ha az IBM-re Vonatkozó Jogszabályok előírják, az IBM közvetlenül válaszolhat az ilyen kérésekre, amennyiben az IBM előzetesen tájékoztatja az Ügyfelet bármely ilyen jellegű válaszadásról, és ésszerű módon egyeztet az Ügyféllel az ilyen válasz formájával és tartalmával kapcsolatban, ha ezt az IBM-re Vonatkozó Jogszabályok ezt lehetővé teszik vagy más módon lehetséges;

b. bármely igazságügyi vagy szabályozó hatóságtól az Ügyfél bármely Személyes Adatának az IBM által történő Feldolgozásával kapcsolatban, amennyiben az IBM válaszolhat ilyen, kormányzati szervtől idézés vagy hasonló, az IBM által történő közzétételre kötelező, jogi dokumentum formájában kapott kérésekre, illetve ha a Vonatkozó Adatvédelmi Jogszabályokban más módon erre kötelezik, amennyiben az IBM előzetesen tájékoztatja az Ügyfelet bármely ilyen jellegű közzétételről, és ésszerű módon egyeztet az Ügyféllel az ilyen válasz formájával és tartalmával kapcsolatban, ha a jogszabályok ezt lehetővé teszik vagy más módon lehetséges.

8.6 Ügyfél Személyes Adatainak feldolgozása

Az IBM az IBM Személyzetéhez tartozó azon személyekre korlátozza az Ügyfél Személyes Adatainak közzétételét, akikre szükség lehet a Szolgáltatások biztosítása érdekében.

Az IBM megfelel az Ügyfél minden ésszerű kérésének, amely arra irányul, hogy az IBM módosítsa, javítsa, törölje vagy zárolja az Ügyfél Személyes Adatait a Vonatkozó Jogszabályoknak megfelelően.

Bármelyik Fél kérésére az IBM, az Ügyfél vagy Társvállalataik a jogszabályok által előírt szabványos megállapodásokat kötnek az Ügyfél Személyes Adatainak védelme érdekében. A Felek megegyeznek

(és megszerzik Társvállalataik beleegyezését is), hogy az ilyen megállapodásokra érvényesek a jelen Megállapodásban foglalt, a Felek közötti követelések tekintetében fennálló felelősségkorlátozások és -kizárások. A Felek együttműködnek további, közösen elfogadott feltételek vagy megállapodások megkötésében (vagy biztosítják, hogy a Felek Társvállalatai megkötik azokat) és betartásában, a Vonatkozó Adatvédelmi Jogszabályok esetleges előírásainak megfelelően.

8.7 Ügyfél Személyes Adatainak visszaküldése

A Megállapodás lejáratakor vagy megszűnésekor az IBM vállalja, hogy beszünteti az Ügyfél Védett Adatainak és az Ügyfél Személyes Adatainak további használatát vagy feldolgozását, és kötelezi erre az IBM Személyzetét is, továbbá az Ügyfél választásának és kérésének megfelelően:

a. azonnal visszajuttatja az Ügyfél számára az Ügyfél Védett adatait és az Ügyfél Személyes Adatait, amelyeket az IBM elektronikus formában tárol, az Ügyfél ésszerű kérésének megfelelő formátumban és adathordozón, valamint az Ügyfélnek az adatok átvételét igazoló visszajelzése után törli, megsemmisíti vagy más módon véglegesen olvashatatlanná és megfejthetetlenné teszi az Ügyfél Védett Adatait és az Ügyfél Személyes Adatait, beleértve azok másolatait és biztonsági másolatait is. Az IBM díjat számíthat fel az adathordozó, illetve az Ügyfél kérésére végrehajtott bizonyos tevékenységek után (például az Ügyfél Védett Adatainak és az Ügyfél Személyes Adatainak különleges formátumban történő átadása vagy Ügyfél Védett Adatainak és az Ügyfél Személyes Adatainak különleges módon történő megsemmisítése); és

b. közvetlenül törli, megsemmisíti vagy más módon véglegesen olvashatatlanná és megfejthetetlenné teszi az Ügyfél Védett Adatait és az Ügyfél Személyes Adatait, beleértve azok másolatait és biztonsági másolatait is.

8.8 Üzlettársakról Szóló Megállapodás

A HIPAA által előírt módon és megfelelő mértékben az IBM és az Ügyfél Üzlettársakról Szóló Megállapodást („BAA”) köt, amely szabályozza az IBM az Ügyfél Üzlettársaként fellépő kötelezettségeit az IBM SaaS biztosítása során. Az IBM a Megállapodásban és a BAA-ban foglalt, ha van ilyen, kifejezett kötelezettségeit nem korlátozva, az Ügyfél tudomásul veszi és elfogadja, hogy felelősséget vállal az alkalmazandó Vonatkozó Jogszabályok és licencelési követelmények meghatározásáért és azok betartásáért, amelyek az IBM SaaS Ügyfél általi használatára vagy az ahhoz kapcsolódó más tevékenységekre vonatkoznak (beleértve a Jogosult Felhasználók általi használatot és más tevékenységeket is).

8.9 Adatfeldolgozási kiegészítés az Európai Unió vonatkozásában

Amennyiben az Ügyfél az IBM vállalatot európai uniós Személyes Adatok feldolgozására utasítja, az IBM és az Ügyfél egy Adatfeldolgozási Kiegészítést is megköt, amelybe belefoglalja a megfelelő EU Mintazáradékokat, a választható záradékok kihagyásával.

9. Az IBM SaaS - Szoftver mint szolgáltatás ajánlat további feltételei

9.1 Biztonság

A jelen IBM SaaS az IBM SaaS ajánlatokra vonatkozó IBM adatbiztonsági és adatvédelmi irányelveket (http://www.ibm.com/cloud/data-security), valamint az alább és a jelen Felhasználási Feltételek Biztonságról és üzletmenet-folytonosságról szóló függelékében foglalt további feltételeket követi. Az IBM adatbiztonsági és adatvédelmi irányelveinek bármilyen módosítása nem csökkenti az IBM SaaS biztonságosságát.

Az IBM Watson Health Core biztonsági irányelveket, szabványokat és az ISO 27001-as keretrendszeren alapuló folyamatokat valósít meg, a Biztonsági leírásban tovább részletezett módon. A biztonsági képességek közül a megoldás a következőket valósítja meg:

a. Biztonságos Működési Zónák

   Az IBM Watson Health Core mélységi védelmi stratégiát valósít meg több biztonsági zóna használatával, a felhőalapú integrációs pontok, például az adatbevezetés és az egyéni alkalmazások fejlesztése kezeléséhez.

b. Titkosítás

   Minden Ügyféladatot tárolása és mozgatása titkosítva történik. Az IBM Watson Health Core rendszeren keresztül haladó adatok mindegyike titkosítva van. Egy megosztott szolgáltatás biztosítja a titkosítási kulcsok kezelését. Az Ügyfél vállal felelősséget az IBM Watson Health

Szolgáltatás és az Ügyfél proxykiszolgálója közötti hálózati kapcsolatért és a kapcsolat minőségéért.

c. Biztonsági események megfigyelése

Az IBM biztonsági-intelligencia platformját használja a biztonsági információk és események felügyeletéhez, a naplózás kezeléséhez, incidensvizsgálatokhoz, fenyegetésészleléshez és a biztonsági rések kezeléséhez.

d. Identitáskezelés

- A Watson Health Core nyílt szabványokon alapuló azonosságszolgáltatókat támogat a nagyméretű beteg- és felhasználói populációk kezelésére az OpenID Connect használatával.
- Azon felhasználói populációk esetén, ahol az IBM az azonosságszolgáltató, a Watson Health Core megfelelő címtárszolgáltatásokat és azonosságkezelési képességeket használ a hitelesítés kezelésére.

e. Erős hitelesítés és szerepköralapú hozzáférés

- A Watson Health Core az SAML-hitelesítést támogatja az Ügyfelek saját egyszeri bejelentkezési (SSO) eljárásának vagy címtárszolgáltatásainak integrálási mechanizmusaként.
- A Watson Health Core egy hozzáférés-kezelési megoldást és az ahhoz kapcsolódó összetevőket használja a biztonsági irányelvek kezeléséhez, amikor szükséges.
- A Watson Health Core szoftveralapú kétfaktoros hitelesítést támogat.
- A Watson Health Core alapvető, szerepköralapú hozzáférés-vezérlést biztosít, ha szükséges; a Watson Health Core támogatja a tanulmányoknak, felhasználói profiloknak, szerepköröknek és felhasználói csoportoknak a szerepköralapú hozzáférést lehetővé tevő alkalmazásprogramozási felületek („API” vagy „API-k”) használatával történő konfigurálását.

9.2 Sütik (Cookie)

Az Ügyfél tudatában van és elfogadja, hogy az IBM az IBM SaaS ajánlat normál működésének és támogatásának részeként nyomon követés és egyéb technológiák révén az IBM SaaS felhasználásához kapcsolódó személyes információkat gyűjthet az Ügyfélről (annak alkalmazottairól és alvállalkozóiról). Az IBM használati statisztikák és az IBM SaaS ajánlat hatékonyságával kapcsolatos információk begyűjtése érdekében végzi ezt a tevékenységet, amelynek célja a felhasználói élmény javítása és/vagy az interakcióknak az Ügyfél igényeihez való igazítása. Az Ügyfél ezúton megerősíti, hogy megszerzi vagy megszerezte a szükséges hozzájárulásokat annak engedélyezéséhez, hogy az IBM a fenti célokra feldolgozza a gyűjtött személyes információkat az IBM vállalaton belül, más IBM vállalatokban, valamint ezek alvállalkozói által a saját vagy alvállalkozói üzletmenetének részeként, a vonatkozó jogszabályoknak megfelelően. Az IBM teljesíti az Ügyfél alkalmazottaitól és alvállalkozóitól származó, a gyűjtött személyes információk elérésére, frissítésére, javítására vagy törlésére irányuló kéréseket.

9.3 Származtatott előnyökkel járó helyszínek

Adott esetben az Ügyfél által az IBM SaaS termék használatából származó haszon realizálásának helyeként megjelölt hely(ek) alapján kell adót fizetni. Az IBM a felsorolt üzleti címek alapján alkalmazza az adókat az IBM SaaS rendelésekor az elsődleges előnyben részesülő helyen, hacsak az Ügyfél külön információkat nem bocsát az IBM rendelkezésére. Az Ügyfél felelősséggel tartozik azért, hogy az erre vonatkozó információkat naprakészen tartsa, és tájékoztassa az IBM vállalatot az esetleges változtatásokról.

9.4 Folyamatos biztosítás

Az Ügyfél jogosult a megoldáshoz készült és az IBM által telepített képességek és fejlesztések egy felhőalapú, folyamatos biztosítást lehetővé tevő modell alapján történő fogadására.

9.5 Biztonsági mentés és visszaállítás

Az IBM Watson Health Core biztosítja az Ügyféladatok utolsó ismert kifogástalan állapotának biztonsági másolatát a termelési környezetben (beleértve a Data Lake és Data Reservoir adattárakat is) a szolgáltatás rendszerhiba esetén történő visszaállíthatása céljából.

9.6 Magas rendelkezésre állás

Az IBM Watson Health Core összetevőinek a termelési környezetben történő megvalósítása magas rendelkezésre állást biztosító konfigurációkban történik, redundancia céljából fürtözött adatbázis-kiszolgálókkal a munkaterhelés elosztása és az egyetlen ponton bekövetkező meghibásodások elkerülése érdekében.

9.7 Katasztrófa utáni helyreállítás

Az IBM katasztrófa utáni helyreállítási megközelítése több eltérő földrajzi helyen található adatközpontból áll a Termelési környezetére vonatkozó következő üzleti folytonossági célok megvalósítása érdekében:

- RTO – a katasztrófa bejelentésétől számított 36 órán belül
- RPO – legfeljebb 24 órányi elvesztett Ügyféltartalom

9.8 Mérési eszközök

Az IBM SaaS szintetikus megfigyelési megoldást használ a vállalt szolgáltatási szintek rendelkezésére állásának vagy kiesésének megfigyelésére, mérésére és jelentésére. Ez a megoldás globális szinten szimulálja és követi nyomon a felhasználói választ és élményt – a statikus rendelkezésre állás és a tranzakciók tekintetében egyaránt.

Az IBM SaaS egy belső megfigyelési megoldást is használ a mérőszámokra, eseményekre és riasztásokra vonatkozóan a teljes megoldás tekintetében.

9.9 Nyilvánosság

Az Ügyfél beleegyezik, hogy az IBM nyilvánosan hivatkozhat az Ügyfélre mint az IBM SaaS egy előfizetőjére a sajtóban vagy marketingkommunikációiban.

„A” Függelék

1. IBM Watson Health Core

Az IBM Watson Health Core az Egészségügyi Adatok Átvitelére Alkalmas platformszolgáltatás (PaaS), fejlesztési platform és működési alrendszer a HIPAA értelmében Védett Egészségügyi Adatoknak (PHI) minősülő adatok, illetve az egyéb Egészségügyi Adatok az IBM tulajdonában álló vagy az IBM által felügyelt adatközpontban történő tárolására, gondozására és feldolgozására az IBM-re Vonatkozó Adatvédelmi Jogszabályoknak megfelelően. Az Ügyfélnek megfelelő jogosultságokat kell beszereznie az IBM Watson Health Core és az IBM Watson Health Core Access szolgáltatáshoz az alább ismertetett képességek és funkciók engedélyezéséhez.

1.1 Watson Health Core működési környezetek

A Watson Health Core jogosultság három, az Egészségügyi Adatok Átvitelére Alkalmas felhőalapú működési környezetet fog át, amelyek lehetővé teszik az Ügyfél számára az Egészségügyi Adatok feldolgozását:

- Próba

  Egy védett környezetet biztosít, amelyben az Ügyfelek az IBM SaaS használatával készített alkalmazásokat fejleszthetnek és tesztelhetnek. A próbakörnyezet a HIPAA biztonsági szabályozások mindegyikének megfelel a katasztrófa utáni helyreállítást, a magas rendelkezésre állást és a rekordalapú rendszerek biztonsági mentését kivéve.

- Termelési környezet

  A teljes értékű környezetet biztosítja, amelyben az Ügyfelek Egészségügyi Adatokhoz kapcsolódó munkaterheléseket telepíthetnek. A termelési környezet egy magas rendelkezésre állású, terhelés-kiegyensúlyozott környezet, amely feladatátadást biztosít egy katasztrófa utáni helyreállítási helyszínre a meghibásodása esetén.

- Katasztrófa utáni helyreállítás

  Egy tükrözött replikát biztosít a Termelési környezetről, és külön elhelyezkedő adatközpontban található.

1.2 Alkalmazásfejlesztés

Az IBM Watson Health Core lehetővé teszi az alkalmazásfejlesztést és a biztonságos adatgyűjtést az Ügyfél eszközeiről vagy az Ügyfél engedélyezett felhasználóinak eszközeiről. Az API felületek programfelületeket és dokumentációt biztosítanak, amelyeket az Ügyfél jogosult felhasználói, beleértve az Ügyfél harmadik félnek minősülő szolgáltatóit, használhatnak alkalmazások fejlesztéséhez és az IBM SaaS ajánlattal folytatott adatcseréhez. Az API felületeknek az Ügyfél vagy annak fejlesztői általi használatára az API Fejlesztői Követelményeknek hatályosak.

- REST API felületek

  A Watson Health Core számos REST API felületet és szolgáltatást biztosít a Watson Health Core platformhoz. Az API képességek többek között az adattárak, az adatgondozási szolgáltatás, a felhasználókezelés és a felügyeleti naplók elérésére szolgáló mechanizmusokat foglalják magukban.

- Apple HealthKit és Apple ResearchKit

  A Watson Health Core támogatja az iOS-alapú kutatási tanulmányokhoz használható Apple ResearchKit API keretrendszerrel, illetve az egészségügyi adatok rögzítésére szolgáló Apple HealthKit szolgáltatással való integrációt.

1.3 Adatszabályozás

- Hozzájárulás-kezelés

  A Watson Health Core biztosítja a betegek vagy tanulmányok résztvevői által adott hozzájárulások rögzítésére szolgáló keretrendszert, és képes biztonságosan tárolni a hozzájárulások rekordját a hasznos adatoktól függetlenül, amikor a személy a hozzájárulások kezelésére alkalmas Ügyfélalkalmazáson keresztül regisztrál.

- Adatrejtés

  A Watson Health Core lehetővé teszi a névazonosítók elválasztását a strukturált hasznos adatoktól. A Watson Health Core a felhőben található adatokat program API felületeken keresztül fogadja. Az API felületek lehetővé teszik a betegek vagy személyek névazonosítóinak a hasznos adatok többi részéről való leválasztását, és egy különálló, titkosított adattárolóban való tárolását. A hasznos adatokhoz egy azonosításra alkalmatlan tokent rendel hozzá a rendszer, amely a későbbiekben eredetkövetésre használható.

1.4 Egészségügyi adatokkal kapcsolatos szolgáltatások

A Watson Health Core biztosítja a strukturált és nem strukturált adatok gyűjtését, tárolását és szinkronizálását, beleértve a külső Egészségügyi Adatokat és más Személyes Adatokat is.

- Adatbevitel

  A Watson Health Core lehetővé teszi a betegekhez kapcsolódó alkalmazásokból vagy eszközökből származó adatok bevitelét a program API felületeken keresztül. A Watson Health Core legfeljebb 25 MB adat feltöltését teszi lehetővé a Health Core szolgáltatásba az Ügyfél egyes Jogosult Egyénjei számára a szerződéses időszak minden évében. A szolgáltatás legfeljebb napi 10 feltöltést tesz lehetővé Egyénenként.

- Működéshez kapcsolódó Data Lake adattár

  A nyers Ügyfél- vagy betegadatok tárolása natív formában történik a Watson Health Core szolgáltatásban, amíg az adatokra szükség nem lesz elemzés és modellezés céljából.

- Kinyerés, átalakítás, betöltés (ETL)

  A működési alrendszer normalizált formátumba alakítja át az adatokat. Az egészségügyi létesítmények számára készült, iparági szabványokon alapuló Enterprise Service Bus lehetővé teszi a különböző Ügyfélalkalmazások és -protokollok közötti integrációt.

- Data Reservoir

  A gondozás befejezése után az adatok átkerülnek a Data Reservoir tárolóba. A Watson Health Core az IBM Unified Data Model for Healthcare bizonyos aspektusait használja az üzleti és technikai egészségügyi adatok normalizálására az elemzésekben történő felhasználás érdekében.

- Személyi törzsindex

  A Watson Health Core törzsadat-kezelési eszközöket biztosít a több forrásból származó adatok összesítése céljából, amelyekből összeállítható egy hosszanti személyi rekord (LPR).

2. Választható jellemzők (feature)

2.1 IBM Watson Health Core Terminology Service

Ez a bővítményként elérhető szolgáltatás adatintegrációt és együttműködést hoz létre az önálló egészségügyi rendszerek között, a klinikai terminológia egységes használatát biztosítva a Watson Health Cloud alkalmazások mindegyike között. Ez a szolgáltatás biztosítja a funkcionális platformot a terminológiával, kódrendszerekkel és strukturált tartalmakkal kapcsolatos feladatok mindegyike számára, például:

- új kódrendszerek létrehozása;
- nemzetközi kódrendszerek lefordítása; és
- helyi kódlisták és nemzetközi szabványok közötti megfeleltetés.

IBM Felhasználási Feltételek – Szolgáltatásszint-megállapodás (SLA)

"B" Függelék

Az IBM a következő rendelkezésre állási Szolgáltatásszint-szerződést („SLA”) biztosítja az IBM SaaS ajánlathoz a Felhasználási Engedélyben meghatározottak szerint. Az SLA nem jelent garanciális kötelezettségvállalást. Az SLA csak az Ügyfél számára érhető el, és csak a termelési célú környezetekben való használatra vonatkozik.

1. Rendelkezésre-állási Jóváírás

A rendelkezésre állási visszatérítések kizárólag az Egyén jogosultságokhoz tartozó előfizetési díjakra vonatkoznak.

Az Ügyfélnek naplóznia kell egy 1. súlyossági (kritikussági) szintű hibajegyet az IBM technikai támogatási ügyfélszolgálatánál legfeljebb 24 órával azt követően, hogy az az Ügyfél először észlelte az esemény az IBM SaaS igénybevételére gyakorolt hatását. Az Ügyfélnek ésszerű keretek között segítenie kell az IBM szakértőit az okok feltárásában és a probléma megoldásában.

Az SLA követelményeinek való meg nem feleléssel kapcsolatos hibajegyeket legfeljebb három munkanappal a Szerződéses Hónap utolsó napja után el kell küldeni. Egy érvényes SLA-alapú követelés teljesítése az IBM SaaS ajánlatért a jövőben fizetendő számla értékén érvényesíthető jóváírás formájában történik, amelynek összege attól az időtartamtól függ, amíg az IBM SaaS termelési célú rendszerfeldolgozása nem volt elérhető („Állásidő”). Az Állásidő az esemény az Ügyfél általi bejelentésétől az IBM SaaS helyreállításáig tart, és nem foglalja magában az ütemezett vagy bejelentett karbantartási célú leállások idejét; az IBM ellenőrzésén kívül eső okokat; az Ügyféltől vagy harmadik személytől származó tartalmakkal, technológiákkal, kialakításokkal és utasításokkal kapcsolatos problémákat; a nem támogatott rendszer-konfigurációkat és platformokat, vagy egyéb az Ügyfél által okozott hibákat; vagy az Ügyfél által okozott biztonsági incidenseket, illetve az Ügyfél általi biztonsági teszteket. Az IBM a lehető legnagyobb mértékű visszatérítést alkalmazza az egyes Szerződéses Hónapokban az IBM SaaS összesített rendelkezésre állásának megfelelően, az alábbi táblázat szerint. Az egy Szerződéses Hónapra kifizetett visszatérítések összértéke nem haladhatja meg az IBM SaaS ajánlatért fizetett éves díj egy tizenkettedének (1/12) 20 százalékát.

2. Szolgáltatási Szintek

Az IBM SaaS rendelkezésre állása egy Szerződéses Hónap során

Rendelkezésre állás egy Szerződéses Hónap során	**Visszatérítés (A követelés tárgyát képező szerződéses hónap Egyénre vonatkozó havi előfizetési díjának* adott %-a)**
<99,95%	10%
<99,0%	20%

*Ha az Ügyfél az IBM SaaS ajánlatot egy IBM Business Partnertől szerezte be, a havi előfizetési díj számítása az IBM SaaS ajánlat éppen érvényes listaárának 50%-a alapján lesz kiszámítva a Követelés által érintett Szerződéses Hónapra vonatkozóan. Az IBM a visszatérítést közvetlenül az Ügyfél számára teszi elérhetővé.

A rendelkezésre állás százalékos arányának számítása a következő módon történik: egy Szerződéses Hónap perceinek száma, mínusz az Állásidő perceinek száma egy Szerződéses Hónapban, osztva egy Szerződéses Hónap teljes szolgáltatási idejének mennyiségével.

Példa: összesen 108 perc Állásidő egy szerződéses hónap során

43 200 perc szolgáltatási idő egy 30 napos szerződött hónapban - 108 perc Állásidő = 43 092 perc _____ összesen 43 200 perc	= 10% Rendelkezésreállási Jóváírás 99,75%-os rendelkezésre állásért egy szerződéses hónap során

3. Kizárások

Az SLA nem vonatkozik a következőkre:

- A kiszolgálómegfigyeléstől eltekintve, az SLA nem vonatkozik az egyéni vagy az Ügyfélalkalmazások támogatásának céljával üzemeltetett virtuális gépekre.
- Ha az Ügyfél megszegte a jelen megállapodásban meghatározott bármely anyagi kötelezettségét.

C Függelék

A jelen Biztonságról és üzletmenet-folytonosságról szóló függelék („SBCA”) bizonyos követelményeket és kötelezettségeket fogalmaz meg az IBM számára az IBM SaaS szolgáltatásnak az Ügyfél számára történő biztosításával kapcsolatban. Az itt meghatározott követelmények és kötelezettségek kiegészítik az IBM SaaS adatbiztonsági elveinek leírásában meghatározottakat, amelyek itt érhetők el: http://www.ibm.com/cloud/data-security. A jelen dokumentumban nem definiált nagybetűs kifejezések jelentését a Megállapodás vagy Felhasználási Feltételek tartalmazzák.

1. Információbiztonsági program

Az IBM az ISO 27001-as keretrendszeren és az ellenőrzési területeken alapuló belső biztonsági irányelvekkel, szabványokkal és folyamatokkal rendelkezik. Az IBM vállalati biztonsági szervezete általi felügyelet mellett, ezek az irányelvek, szabványok és folyamatok rendszeresen képezik belső felülvizsgálatok tárgyát.

Az IBM szervezeti, üzemeltetési, adminisztratív, fizikai és technikai óvintézkedésekből álló információbiztonsági programot működtet, amely szabályozza az Ügyféltartalmaknak legalább a jelen SBCA követelményeinek megfelelő feldolgozását, tárolását és átvitelét.

Az IBM vállalja, hogy az Ügyfél kérésére megosztja az Ügyféllel az IBM Watson Health információbiztonsági programmal kapcsolatos információikat annak érdekében, hogy az Ügyfél ésszerű módon meghatározhassa annak változatlan megfelelőségét, elfogadhatóságát és hatékonyságát. Az IBM Watson Health információbiztonsági program időről időre frissítésen esik át, hogy naprakész maradjon az általánosan elfogadott ipari gyakorlatoknak és az IBM-re Vonatkozó Jogszabályoknak megfelelően.

2. Hozzáférés-felügyelet

Az IBM kizárólag alkalmazottai, alvállalkozói vagy olyan harmadik felek számára teszi közzé az Ügyféltartalmakat, amelyek jogszerű üzleti igénnyel rendelkeznek az ilyen Ügyféltartalmak elérésére vonatkozóan annak érdekében, hogy segíteni tudják az IBM vállalatot az Ügyfél vagy más személyek felé fennálló kötelezettségeinek a teljesítésében az IBM SaaS biztosítása céljából, a Vonatkozó Jogszabályokban, a Megállapodásban vagy egy Kapcsolódó Dokumentumban, ha van ilyen, foglaltaknak megfelelően. Abban az esetben, ha az IBM az Ügyfél egy Üzlettársa, az IBM és az Ügyfél kizárólag a Felek között érvényben lévő Üzlettársakról Szóló Megállapodásban foglaltaknak megfelelően tehetnek közzé Személyes Egészségügyi Adatokat.

Az IBM egy formális, a felhasználói hozzáférést kezelő belső folyamattal, amelynek keretében a felhasználói hozzáférés kérelmezése, majd jóváhagyása az azonosság igazolásakor formálisan történik, és a hozzáférést a tartalom ismeretének szükségessége alapján biztosítja a rendszer, érvényesítve ezzel a legkevesebb jogosultság elvét. Az Ügyféltartalmakhoz való hozzáférést a rendszer az aktív felhasználókra és az aktív felhasználói fiókokra korlátozza. Az IBM formális folyamattal rendelkezik az aktív felhasználói fiókok hozzáférésének rendszeres belső újraértékelésére.

Az IBM biztonságos felhasználó-hitelesítési protokollokat használ, beleértve egyedi azonosítók és erős jelszavak hozzárendelését az aktív felhasználói fiókokhoz azokon a rendszereken, amelyek használatával szolgáltatásokat biztosít az Ügyfélnek, az IBM vállalati biztonsági szabványait és irányelveit követve:

a. A jelszavak nem lehetnek forgalmazó által megadott alapértelmezett jelszavak és olyan helyszínen és/vagy formátumban kell azokat tárolni, amely nem veszélyezteti az általuk védett adatok biztonságát.

b. A jelszavak megjelenítését és nyomtatását el kell rejteni, eltakarni vagy más módon olvashatatlanná tenni, hogy jogosulatlan felek ne figyelhessék meg, illetve ne tudják visszafejteni azokat. A jelszavakat tilos naplózni vagy rögzíteni bevitelük közben. A felhasználói jelszavakat tilos nyílt szöveges formában tárolni.

c. Az IBM SaaS ajánlatot veszélyeztető egyes technológiák esetén úgy kell jelszót választani, hogy azzal mérsékelni lehessen az ismert jelszóhosszból fakadó biztonsági réseket, illetve dokumentálni kell azokat.

d. Ha belső, emelt jogosultságszintű, megosztott funkcionalitású azonosítók használata szükséges működtetési okokból, az IBM kezeli a jelszók kivételét igénylő megosztott, funkcionális és/vagy Rendszer-azonosítókat az egyéni elszámoltathatóság fenntartása érdekében.

Inaktivitásból eredő időtúllépések vannak érvényben az Ügyféltartalmakat tároló rendszerek és alkalmazások mindegyike esetén.

Ha szükséges, az Ügyfél kérésére és az IBM formális jóváhagyásával távoli kapcsolat létesíthető az IBM azon hálózatával, rendszereivel és alkalmazásaival, amelyek Ügyféltartalmakat tárolnak, és minden ilyen távoli kapcsolatot erős hitelesítési és titkosítási protokollok használatával kell biztonságossá tenni. A távoli hozzáférési tevékenységet naplózni és figyelni kell.

Az IBM SaaS biztosítása által kívánt mértékig, ha az IBM vállalatnak távolról hozzá kell férnie az Ügyfél belső hálózatában található rendszerhez, minden ilyen távoli hozzáférés kizárólag az Ügyfél biztonságos távoli hozzáférési rendszereinek és protokolljainak használatával történik, az Ügyfél által az IBM számára megadott hozzáférési hitelesítési adatok használatával. Az Ügyfél hálózatához való távoli hozzáférés kizárólag az IBM kérésére és az Ügyfél jóváhagyásával történhet, az Ügyfél akkor érvényben lévő irányelveinek megfelelően, amelyeket előre ismertet az IBM vállalattal. Az Ügyfél belső hálózatainak IBM általi használatára az Ügyfél informatikai használati feltételei és irányelvei érvényesek, amelyeket előre ismertet az IBM vállalattal.

Az IBM megvalósítja a felelősségek szétválasztását a biztonsági felügyelet, a hozzáférések felülvizsgálata és a biztonsági irányelvek megsértésének vizsgálata tekintetében.

Az Ügyfélhez kapcsolódó Ügyféltartalmak tárolása, üzemeltetése és feldolgozása logikai módon különül el az IBM által kiszolgált más ügyfelek tartalmaitól. Azokban az esetekben, amikor megosztott tárolási, üzemeltetési vagy feldolgozási munkaterületet engedélyez az Ügyfél, az IBM a jelen SBCA követelményeinek megfelelő eljárásokat és óvintézkedéseket foganatosít, amelyeket az ilyen Ügyféltartalmak jogosulatlan közzétételének megelőzésére terveztek.

Az IBM üres asztal/üres képernyő irányelvet valósít meg annak biztosítására, hogy az Ügyféltartalmak nem maradnak felügyelet nélkül semmilyen nyilvános helyen és semmikor.

3. Átvitel és titkosítás

Az IBM megfelelő óvintézkedéseket tesz az Ügyféltartalmak átvitele (fax, e-mail, futár stb.) közben annak biztosítására, hogy a megfelelő kapcsolattartási információt használja a címzett azonosítására, és előzetes intézkedéseket tesz a kívánt címzettel közösen az ilyen információk beszerzése céljából.

Az IBM és az IBM Személyzete mindig megfelelő formátumú titkosítást és más biztonsági technológiákat használ az Ügyféltartalmak feldolgozásával összefüggésben, beleértve az Ügyféltartalmakkal kapcsolatos kommunikációt, szállítást, távoli hozzáférést és tárolást (beleértve a biztonsági mentést). Az IBM vállalja például, hogy a megfelelő iparági szabványnak megfelelő titkosítás használatával titkosítja az Ügyféltartalmakat tartalmazó összes rekordot és fájlt:

a. amelyek az IBM laptopjain, hordozható eszközein és hordozható elektronikus adathordozóin találhatók, beleértve a biztonsági másolatokat tartalmazó szalagokat, miközben egy telephelyen kívüli tárolási létesítménybe szállítják azokat;

b. amelyeket az IBM az Ügyfél vagy az IBM fizikailag biztosított irodáin és létesítményein kívül tárol vagy oda szállít, kivéve a nyomtatott, papíralapú dokumentumokat;

c. az IBM általi, nyilvános hálózatok közötti átvitel közben;

d. az IBM rendszereiről az Ügyfél számára történő átvitel közben;

e. az IBM általi vezeték nélküli átvitel közben; és

f. az IBM által kiszolgálókon és adatbázisokban történő tárolása közben.

4. Hálózati biztonság

Az IBM a rendszerbiztonsági szoftverek, például tűzfalak, proxyk, webalkalmazás-tűzfalak és felületek ésszerűen naprakész változatait használja. Az ilyen szoftvereknek a rosszindulatú programok elleni védelemmel, valamint ésszerűen naprakész javításokkal és vírusdefiníciókkal is rendelkeznie kell. A vállalati szabványoknak megfelelően víruskereső szoftver telepítendő a munkaállomásokra, kiszolgálókra és a kapcsolódó végpontokra, ahol az technikailag megoldható, és a szoftver kezelése a vállalati irányelvekkel és a belső felügyeleti megoldásokkal összhangban zajlik.

Az IBM megfigyeli az IBM SaaS ajánlatot a biztonsági incidensek lehető leghamarabbi észlelése és azonosítása érdekében. Az IBM legalább az iparági szabványoknak megfelelő behatolásészlelési eszközöket, valamint megelőzési, megfigyelési és reagálási folyamatokat tart fenn olyan módon, hogy egyaránt képes legyen azonosítani azon belső és külső biztonsági réseket és kockázatokat, amelyek az Ügyféltartalmakkal vagy az Ügyfél számára szolgáltatások biztosításához használt információs rendszerekkel kapcsolatos jogosulatlan közzétételhez, visszaéléshez, módosításhoz, illetve ezek megsemmisítéséhez vezethetnek.

Az IBM a biztonsági résekhez kapcsolódó adatszerzési szolgáltatásokra, információbiztonsági tanácsadásra vagy más vonatkozó, a rendszerek sebezhetőségére vonatkozóan aktuális információt szolgáltató forrásokra fizet elő. Az IBM rendszeresen felméri a biztonsági réseket és elvégzi hálózatának hibaelhárítását.

Az IBM megfigyeli az IBM SaaS ajánlatot a Biztonsági Incidensek észlelése, azonosítása, elkülönítése és elhárítása érdekében.

Az IBM az IBM kiadáskezelési folyamatain keresztül ellenőrzi azon hálózati biztonsági infrastruktúra rendelkezésre állását, integritását és hatékonyságát, amelyen az IBM SaaS ajánlatot elérhetővé tette.

5. Incidensek kezelése és értesítések

Az IBM Watson Health csapatai együttműködnek az IBM Cybersecurity Incident Response Team csapatával. Ez a globális szinten működő csapat az IBM ajánlatokhoz kapcsolódó biztonsági incidensek fogadásával, kivizsgálásával és belső koordinálásával foglalkozik, a szoftverekhez kapcsolódó biztonsági problémák mérsékléséhez szükséges megelőző lépések megvalósítása érdekében. A „Biztonsági Incidens” azon információs rendszer rendszerműveleteihez vagy adataihoz való sikeres jogosulatlan hozzáférést, illetve azok használatát, közlését, módosítását vagy zavarását jelenti, mely rendszert az IBM az IBM SaaS biztosításához használja. Biztonsági Incidensek felfedezése esetén (rutinvizsgálatok, riasztások, küszöbértéket átlépő események stb. révén), az IBM tájékoztatja és értesíti az Ügyfelet:

a. bármely, az Ügyféltartalmakat érintő, igazolt Biztonsági Incidensről a lehető leghamarabbi időpontban, de legalább az adott Biztonsági Incidens kivizsgálását és megállapítását követő 2 munkanapon belül;

b. az Ügyféltartalmakat érintő, kormányzati tisztviselő (beleértve az adatvédelmi és rendvédelmi szerveket) által kért bármely hozzáférést vagy információ-szolgáltatást követően azonnal, amennyiben ezt nem tiltja jogszabály vagy vonatkozó határozat; és

c. a jelen SBCA Hozzáférés-felügyelet című szakaszában engedélyezettektől eltekintve, az Ügyféltartalmak egy harmadik fél általi vagy harmadik fél számára történő közlését, átvitelét vagy biztosítását megelőzően.

6. Naplózás

Az IBM az IBM irányelveinek és gyakorlatainak, valamint az általánosan elfogadott iparági gyakorlatoknak megfelelően ésszerűen megfigyeli a rendszereket az Ügyfél Feldolgozott Adatainak jogosulatlan használatának vagy az azokhoz való hozzáférésnek az észlelése érdekében. Naplózza a bejelentkezéshez és hozzáféréshez kapcsolódó tényleges vagy megkísérelt jogsértéseket.

Az IBM a HIPAA-ban és az egyéb, IBM-re Vonatkozó Adatvédelmi Jogszabályokban meghatározott ideig megőrzi a hozzáférésekkel kapcsolatos összes kérelmet, és naplózza a hozzáférési tevékenységeket minden olyan rendszer esetében, amely tárol, hozzáfér, feldolgoz és közvetít Ügyfél- és Egészségügyi Adatokat.

A naplók és jelentések legalább a következőket foglalják magukban: (i) minden bejelentkezési kísérlet, függetlenül annak sikerességétől vagy sikertelenségétől, beleértve az ésszerű azonosítóadatokat; (ii) a rendszer és a hálózat konfigurációjának minden módosítása, beleértve az alkalmazástelepítéseket, a felhasználókezelési módosításokat és a fájlelérési engedélyek módosításait; (iii) erőforrás-elérési kísérletek, függetlenül azok sikerességétől vagy sikertelenségétől, beleértve a fájlokhoz, hálózati megosztásokhoz, naplókhoz vagy más erőforrásokhoz való hozzáférési kísérleteket; és (iv) adatletöltések, beleértve az adatok tartalomtípusát és a letöltéshez használt hozzáférési protokollt.

7. Szoftveralkalmazás-fejlesztés és változáskezelés

Az IBM biztonságos alkalmazásfejlesztési és kódolási gyakorlatokat követ, amelyek megvédik a termelési alkalmazások és a kapcsolódó forráskódok integritását a jogosulatlan és ellenőrizetlen módosításokkal szemben.

Az IBM változáskezelési folyamatot követ, amely magában foglalja (a) a módosítások rögzítését és formális jóváhagyását, valamint a visszalépési eljárásokat, és (b) az ilyen módosítások megfelelő tesztelését, beleértve a felhasználói elfogadási tesztelést, ahol szükséges, továbbá a biztonsági tesztelést.

Az IBM egy javításkezelési folyamatot követ, amely magában foglalja a javítások tesztelését azok minden olyan rendszeren történő telepítése előtt, amelyek az Ügyféltartalmak tárolására, továbbítására, az azokhoz való hozzáférésre, illetve szolgáltatások, az IBM SaaS ajánlatot is beleértve, biztosítására használnak az Ügyfél számára.

Az IBM megköveteli, hogy az adminisztrátorok teljes, pontos és naprakész adatokkal rendelkezzenek az összes olyan információs rendszerrel kapcsolatban, amelyeket Ügyféltartalmak tárolására, továbbítására és az azokhoz való hozzáférésre használnak.

8. Fizikai biztonság és a környezet biztonsága

Az IBM Watson Health Core platform telepítése az IBM SoftLayer adatstruktúrára történik. Az IBM SoftLayer fizikai és környezeti biztonságot, hozzáférés-felügyeletet, illetve az Ügyféladatokat emberi, környezeti és technikai eredetű megsértéstől vagy hatásoktól védő vezérlőket és folyamatokat működtet.

Az IBM SaaS ajánlatot futtató létesítményekbe való általános belépést kártyás beléptetőrendszer szabályozza. Zárt láncú videorendszer (CCTV) van telepítve a telephelyeken, amelyet biztonsági személyzet felügyel. Bizonyos bejáratok riasztóval vannak ellátva, és biztonsági személyzet felügyeli ezeket a riasztókat.

A felügyelt területekhez való hozzáférést a kártyás és/vagy további biometrikus azonosítást igénylő beléptetőrendszer korlátozza. A felügyelt területekhez jogosult hozzáféréssel nem rendelkező személyeknek be kell jelentkezniük, és kizárólag a felügyelt területhez jóváhagyott hozzáféréssel rendelkező személy kíséretében léphetnek be a felügyelt területekre. Minden felügyelt terület vészkijárata hangalapú riasztóval van felszerelve, és biztonsági személyzet felügyeli ezeket a riasztókat. A riasztók működésének ellenőrzése rendszeresen történik, amiről megőrzendő dokumentáció készül. A felügyelt területekhez való hozzáférési engedélyeket negyedéves rendszerességgel teljes mértékben felülvizsgálják. A felügyelt területekre való belépési engedélyt a munkaviszony megszűnésével visszavonják.

A létesítmények olyan környezeti tényezőkkel szembeni védelmét, mint a tűz, víz és hő, tűzriasztók, tűzoltó készülékek, füstjelzők és tűzoltó rendszerek biztosítják. A létesítmények áramkimaradásokkal és áramszünetekkel szembeni védelmét szünetmentes tápegységek (UPS) és tartalék generátorok biztosítják, amelyeket rendszeresen karbantartanak és ellenőriznek.

Az IBM SoftLayer szolgáltatáshoz kapcsolódó megfelelőségi információk és jelentések a következő helyen érhetők el: http://www.softlayer.com/compliance.

9. Üzletmenet-folytonosság

Az IBM üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervekkel rendelkezik, amelyeket úgy alakítottak ki, hogy a Megállapodásban foglalt kötelezettségeinek megfelelő szintű szolgáltatást tartsanak fenn. Az ilyen üzletmenet-folytonossági és katasztrófa utáni helyreállítási terveket rendszeresen frissítik és ellenőrzik (legalább évente egyszer). Az IBM megvalósít minden olyan ésszerű változtatást az üzletmenet-folytonossági és katasztrófa utáni helyreállítási tervekben, amely az általánosan elfogadott iparági gyakorlatoknak való megfeleléshez szükséges, minden esetben arra törekedve, hogy elkerülje az Ügyfél által használt IBM SaaS vagy termelési környezet működésének ésszerűtlen megzavarását.

Olyan katasztrófa bekövetkezése esetén, amely miatt az IBM SaaS elérhetetlenné válik az Ügyfél számára, az IBM azonnal értesíti az Ügyfelet, és életbe lépteti az üzletmenet-folytonossági és/vagy katasztrófa utáni helyreállítási tervet. Katasztrófa bejelentése esetén az IBM SaaS üzletmenet-folytonossági célkitűzése az Ügyfélnek az IBM SaaS rendszerhez való hozzáférésének visszaállítása a következő módon: áramkimaradás esetén a Helyreállítási Célidőtartam (RTO) az IBM Watson Health termelési környezetének helyreállítása a katasztrófa bejelentését követő 36 órán belül. Az Adatvesztési Tűrés (RPO) legfeljebb 24 órányi elvesztett Ügyféltartalom a termelési környezetben. Az egyes Watson Health megoldások üzletmenet-folytonossági célkitűzései eltérőek lehetnek.

Az IBM katasztrófa utáni helyreállítási megközelítése több eltérő földrajzi helyen található adatközpontból áll.

Minden IBM SoftLayer adatközpont több áramforrást, száloptikai kapcsolatot, dedikált generátort és tartalék akkumulátort használ. Ezek iparágvezető hardverekből és berendezésekből állnak, biztosítva

ezzel a lehető legmagasabb szintű teljesítményt, megbízhatóságot és együttműködési képességet. Minden n+1 redundáns áramforrást és hűtést tartalmazó adatközpont-összetevőt például ellenőriznek az adatközponton belüli stabilitás megőrzése érdekében.

10. Megfelelőség

Az IBM biztonsági gyakorlatai az ISO 27001-27002 szabványon alapulnak. Ezen gyakorlatok szabályozási szerkezetet biztosítanak, többek között, a kockázatelemzés, fizikai biztonság, vészhelyzeti tervezés, vizsgálatok, információvédelem, oktatás, adatvédelem és működtetés számára.

Az IBM folyamatosan ellenőrzi, hogy a biztonsággal és az adatvédelemmel kapcsolatos tevékenységek megfelelnek-e az IBM biztonsági gyakorlatainak.

Az IBM megfelel az IBM-re Vonatkozó Adatvédelmi Jogszabályoknak a Hatókörbe Tartozó Joghatóságok területén.

Az Ügyfél bizalmas adatainak kezelését az IBM üzleti magatartási irányelvei is megkövetelik, amelyeket minden alkalmazottnak át kell tekintenie (és igazolni azok áttekintését) éves rendszerességgel.

11. Egyéb

Az IBM biztosítja, hogy az alvállalkozóival és/vagy az IBM SaaS szolgáltatás biztosítása során közreműködő harmadik felekkel kötött megállapodásainak feltételei legalább olyan mértékben védik az Ügyféltartalmakat, mint a jelen SBCA és bármely vonatkozó Kapcsolódó Dokumentum, az ilyen alvállalkozók és/vagy harmadik felek által elvégzendő szolgáltatásokra alkalmazható mértékig.