ADATVÉDELMI SZABÁLYZAT

Haraszti Hedvig egészségügyi szolgáltató

Nyilvántartási szám: 50362741

Adószám: 67526381-1-33

Székhely: 2600-Vác, Lovarda tér 16.

Hatályos 2018. május 25-től

Tartalom

1. Bevezetés

Jelen dokumentum a **Haraszti Hedvig** (továbbiakban Szolgáltató) adatvédelmi szabályzata (a továbbiakban AVSZ) az Európai Parlament és a Tanács (EU) 2016/679 rendeletében és a kapcsolódó jogszabályokban – különös tekintettel az 1997. évi CLIV. törvényre az egészségügyről, valamint az 1997. évi XLVII. törvényre az egészségügyi és a hozzájuk kapcsolódó személyes adatok védelméről – meghatározottak szerint.

1.1 A dokumentum célja

Az AVSZ célja a személyes adatok kezelése és védelme követelményrendszerének és környezetének meghatározása. A szabályzat rögzíti az adatkezelés folyamatát, a biztonsági intézkedéseket, azok dokumentálásának és ellenőrzésének feladatait és ezek végrehajtásának idejét, valamint az ehhez szükséges egyes szerepköröket.

1.2 A dokumentum szervezeti hatálya

Az AVSZ kiterjed a Szolgáltató információkezeléssel- és feldolgozással kapcsolatos összes folyamatára és tevékenységére és a tulajdonában vagy használatában lévő elektronikus információs rendszerekben előforduló adatokra.

1.3 A dokumentum tárgyi hatálya

Jelen dokumentum tárgyi hatálya kiterjed Szolgáltató rendelőiben, telephelyein és fióktelepein található összes üzemelő, használatban lévő vagy a jövőben bevezetett, alkalmazott informatikai eszközre, rendszerre, a teljes, digitálisan és papíron tárolt egészségügyi dokumentációra, valamint a digitális- és papíralapú archívumokra és az azok tárolására szolgáló helyiségekre.

1.4 A dokumentum személyi hatálya

Az elfogadott AVSZ vonatkozik:

- A **Szolgáltató** valamennyi alkalmazottjára,
- A **Szolgáltató** összes közreműködő munkatársára,
- A **Szolgáltató** szerződéses, vagy más módon kapcsolatba kerülő természetes vagy jogi személyekre, gazdasági társaságokra a velük kötött megállapodás révén.

Az AVSZ személyi hatálya kiterjed a **Szolgáltató** valamennyi képviselőjére, vezetőjére és az általa használt rendszerek fejlesztőire, üzemeltetőire.

Ezeken kívül a dokumentum hatálya kiterjed a **Szolgáltató** külső, eseti munkakapcsolatban lévő személyekre is, amelyeknek érvényesülését a fenti szerződések tartalmának megfelelő kialakításával kell biztosítani és az adatvédelemért felelős személyek közreműködésével kell megvalósítani.

1.5 Az AVSZ jogszabályi alapja

- az Európai parlament és a Tanács (EU) 2016/679 rendelete a természetes személyek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról (a továbbiakban: GDPR);
- az 1997. évi CLIV. törvényre az egészségügyről;
- az 1997. évi XLVII. törvényre az egészségügyi és a hozzájuk kapcsolódó személyes adatok védelméről;
- a polgárok személyi adatainak és lakcímének nyilvántartásáról szóló 1992. évi LXVI. Törvény.

1.6 Kiadás dátuma, érvényessége

Jelen szabályzat a kiadás napján lép hatályba, és mindaddig érvényesnek tekintendő, amíg annak egy új változata jóváhagyásra nem kerül.

Az AVSZ bármilyen változása verziószám változással jár, melyet a Dokumentum történetben fel kell vezetni, feltüntetve a verziószámot, a kibocsátás napját és a változások vázlatos összefoglalását.

Az AVSZ írásos formában minden érintett számára elérhető a **Szolgáltató** rendelőiben, illetve elektronikus formában a rendelői szerver- és kliens gépeken.

A Szabályzat, illetve mellékleteinek felülvizsgálatára az alábbiak szerint kerül sor:

- rendes: évente egy alkalommal az aktuális belső felülvizsgálat során,

- rendkívüli: megváltozott körülmények hatására a felülvizsgálatot el kell végezni az alábbi események bármelyikének bekövetkezésekor:
    - az információbiztonságot is érintő jogszabály-változás, amennyiben annak hatálya a **Szolgáltató** -re is kiterjed;
    - az információkezelést- és feldolgozást végző vagy támogató folyamatokban, illetve a kezelt adatok körében beállt lényeges változás;
    - a **Szolgáltató** tulajdonában vagy használatában lévő elektronikus információs rendszerekben, illetve azok fizikai környezetében beálló lényeges változás.
- minden olyan esetben, amikor a Szabályzatban leírtakhoz képest egyéb jelentős változás történik.

A mindenkori felülvizsgálat végrehajtása az Informatikai Felelős feladata.

2. Az adatvédelem szervezeti kérdései

Az adatvédelmi tisztviselő, adatvédelmi felelős, adatkezelők, adatfeldolgozók felsorolását a 2. sz melléklet tartalmazza.

Cél: Az adatbiztonsági feladatok ellátására és ellenőrzésére azonosítható szerepkörök álljanak rendelkezésre.

2.1 Általános szabályok

A **Szolgáltató** vezetése e szabályzatban megfogalmazott világos iránymutatással, elkötelezettsége kinyilvánításával, az adatvédelemmel összefüggő felelősségi körök egyértelmű kijelölésével és elismerésével aktív módon támogatja a személyes adatok jogszabályoknak megfelelő kezelését a szervezeten belül. Az ezzel összefüggő részletes feladatokat és felelősségi szabályokat az adott felhasználó munkaköri leírása tartalmazza.

2.2 Az ügyvezető:

(1) Ellátja az adatvédelmi felelős feladatait;

(2) Kiadja az Adatvédelmi Szabályzatot;

(3) Együttműködik a megbízott adatvédelmi tisztviselővel;

(4) Intézkedik az adatvédelmi incidensek ügyében

(5) Kivizsgálja a hozzá érkezett bejelentéseket, jogosulatlan adatkezelés esetén annak megszüntetésére hívja fel az adatkezelőt;

(6) Kezeli a **Szolgáltató** külső szervektől és személyektől érkező megkereséseket, végrehajtja az ezekkel kapcsolatos intézkedéseket

(5) A megkeresésekről, azok teljesítéséről vagy elutasításáról nyilvántartást vezet;

(6) Az adatvédelmi tisztviselő szakami segítségével elkészíti és aktualizálja az Adatvédelmi Szabályzatot és mellékleteit;

2.3 A rendszergazda

Biztosítja, hogy az adatvédelmi szabályzatnak az alkalmazott rendszerek megfelejenek.

2.4 A szerződéses adatvédelmi tisztviselő

(1) Szakmailag irányítja, felügyeli, ellenőrzi a **Szolgáltató** adatvédelmi tevékenységét;

(2) Ellenőrzi a jogszabályok, valamint az Adatvédelmi szabályzat rendelkezéseinek a betartását;

2.5 A betegnyilvántartó rendszer szállítója

Biztosítja, hogy a szállított rendszer az adatvédelmi szabályozásnak megfeleljen.

2.6 A képi diagnosztikai nyilvántartó rendszer szállítója

Biztosítja, hogy a szállított rendszer az adatvédelmi szabályoknak megfeleljen.

2.7 Az adatkezelést végző személy

(1) Tevékenységi körén belül felelős az adatok feldolgozásáért, megváltoztatásáért, törléséért, továbbításáért és nyilvánosságra hozataláért, valamint az adatok pontos, követhető dokumentálásáért,

(2) Kezeli és megőrzi a feladata ellátása során birtokába került adatokat,

(3) Ügyel a nyilvántartások biztonságos kezelésére és tárolására,

(4) Gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz illetéktelen személy ne férhessen hozzá,

(5) Betartja az adatkezelésre vonatkozó jogszabályokat és ügyvezetői utasításokat

2.8 Belső adatvédelmi nyilvántartás

A belső adatvédelmi nyilvántartás a **Szolgáltató** rendelőiben, telephelyein és fióktelephelyein történő, a GDPR előírásai alá tartozó adatkezelésekkel kapcsolatban tartalmazza:

-az adatkezelés célját,

-az adatok fajtáját és kezelésük jogalapját,

-az érintettek körét,

-az adat forrását,

-az esetleges adattovábbítások fajtáját, címzettjét és a továbbítás jogalapját,

-az egyes adatfajták törlésének határidejét.

2.9 Felelősség.

A szervezeti szabályok megfelelő és átlátható kialakításáért **Szolgáltató** ügyvezetője a felelős.

3. Az adatkezelés szabályai

3.1 Személyes és különleges adatok kezelése

A **Szolgáltató** a betegelőjegyzés, betegnyilvántartás és betegellátás során személyes és különleges – egészségügyi dokumentáció – adatokat kezel. Az adatkezelés jogalapja minden eseteben az érintett hozzájárulása, valamint a vonatkozó jogszabályok.

Az érintett az adatkezelőtől tájékoztatást kérhet személyes és különleges adatai kezeléséről, és az adatokba bele is tekinthet. A betekintést úgy kell biztosítani, hogy az érintett más személy adatait ne ismerhesse meg.

Az érintett kérelmére az adatkezelő tájékoztatást ad az általa kezelt adatairól, az adatkezelés céljáról, jogalapjáról, időtartamáról, továbbá arról, hogy kik és milyen célból kapták meg az adatokat.

Adatváltozás vagy téves adatrögzítés észlelése esetén az érintett írásban vagy szóban kérheti kezelt adatainak helyesbítését, illetve kijavítását. A téves adatot az adatkezelő indokolatlan késedelem nélkül, de legkésőbb egy hónapon belül helyesbíteni köteles. (GDPR (59)

A személyes adatok és az egészségügyi dokumentáció (képalkotó diagnosztikai felvétel, lelet) az érintett hozzájárulásával továbbíthatók 3. fél – másik egészségügyi szolgáltató részére – részére.

Olyan adatkezelés esetén, amelynél számolni kell külföldre irányuló adattovábbítással, az érintettek figyelmét erre a körülményre már az adatok felvétele előtt fel kell hívni. Az érintett írásbeli felhatalmazása nélkül személyes adat külföldre nem továbbítható, kivéve, ha ezt törvény lehetővé teszi.

Az adattovábbítás papír alapon vagy elektronikus úton történhet.

Az érintett az adatkezeléssel kapcsolatos jogainak megsértése esetén az illetékes szervezeti egység vezetőjéhez, illetve az adatvédelmi felelőshöz fordulhat.

3.2 Közérdekű adatok kezelése

(1) A **Szolgáltató** kezelésében lévő közérdekű adatot bárki megismerheti az állami és szolgálati titok kivételével.

(2) A közérdekű adat megismerésére irányuló kérelemnek 15 napon belül eleget kell tenni.

(3) Amennyiben a közérdekű adat megismerésére irányuló kérelem nem teljesíthető, a kérelem megtagadásáról és indokairól 8 napon belül írásban értesíteni kell a kérelmezőt.

(4) Amennyiben törvény másként nem rendelkezik a belső használatra készült, valamint a döntés-előkészítéssel összefüggő adat a kezelését követő húsz éven belül nem nyilvános. Kérelemre az adatok megismerését az Ügyvezető(k) e határidőn belül is engedélyezheti(k).

3.3 Az adatbiztonság általános szempontjai

(1) Az adatkezelő köteles gondoskodni az általa kezelt adatok biztonságáról.

(2) Az adatokat védeni kell a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés ellen.

(3) Adatkarbantartást csak az erre felhatalmazott adatkezelő végezhet.

(4) A számítástechnikai rendszerek üzemeltetését ellátó munkatársak a feladataik ellátásához szükséges mértékig az adatállományokhoz hozzáférhetnek, az adatokat azonban más célra nem használhatják fel, és mások tudomására nem hozhatják.

(5) Az adatbiztonság érdekében megfogalmazott előírások betartásáért a betegnyilvántartó rendszer vonatkozásában a **Szolgáltató** ügyvezetője, az egyes rendeléseken történő adatkezelési folyamatok vonatkozásában az adatkezelést végző adminisztrátor a felelős.

3.4 Az adatokhoz való hozzáférés szabályozása

(1) Az elektronikusan tárolt adatokhoz való hozzáférést jelszavas védelemmel és jogosultsági rendszer működtetésével szabályozzuk.

(2) A betegnyilvántartó rendszerhez való hozzáférés jelszavait és jogosultsági rendszerét a **Szolgáltató** ügyvezetője állítja be és kezeli az informatikai folyamatok fejezet(ek)ben leírtak szerint.

(3) A papír alapú egészségügyi dokumentációt zárható rendelőhelyiség, illetve zárható recepció zárral ellátot szekrényeiben kell tárolni. Rendelési időben az 1. sz. Mellékletben felsorolt adatkezelők hozzáférhetnek az adatokhoz; távozáskor azokat a zárt helyiségekben helyezik el.

3.5 Az adatok mentése, az adathordozók biztonsága

(1) Az adatok mentésének és az adathordozók biztonságának általános szempontjait jelen AVSZ pontja rögzíti.

(2) A központi szervereken tárolt adatok rendszeres mentését a **Szolgáltató** rendszergazdája végzi.

3.6 Manuális kezelésű adatok

A **Szolgáltató** rendelőiben az egészségügyi dokumentációt csak az arra jogosultsággal rendelkezők kezelhetik.

A folyamatos aktív kezelésben lévő dokumentációhoz a feldolgozás során csak az illetékességgel rendelkező adminisztrátorok / egészségügyi szakdolgozók / orvosok férhetnek hozzá.

Az papír alapú dokumentációt zárható helyiségben, kell védeni az illetéktelen hozzáféréstől.

A passzív kezelésben lévő dokumentáció archiválását évente el kell végezni. Az archivált iratokat zárható, erre a célra kialakított helyiségben kell tárolni.

A jogszabály által előírt megőrzési idő lejártával a dokumentációt **Szolgáltató** saját hatáskörben megsemmisíti.

3.7 Törvényileg szabályozott adatkezelések

A **Szolgáltató** az alábbi törvényi kötelezettségek alapján őrzik meg a személyes adatokat:

Egészségügyi dokumentáció: az ellátottak egészségügyi adatait tartalmazó dokumentumokat az egészségügyi adatokról szóló 1997. évi XLVII törvény alapján 30 évig kötelező megőrizni.

Munkavédelem: balesetekkel kapcsolatos jegyzőkönyveket a Munkavédelemről szóló 1993. évi XCIII törvény szerint 5 évig kötelező megőrizni.

Munkaügy: a munkavállalók adatait az Adózás rendjéről szóló 2017. évi CL törvény szerint az adó megállapításához való jog elévüléséig, vagyis 5 évig kell megőrizni.

3.8 Felelősség

A **Szolgáltató** rendelőiben irányadó adatvédelmi szabályok megfelelőségéért, azok elérhetőségéért a **Szolgáltató** ügyvezetője felel. A szabályok betartásáért az adatkezelés végző személy felelős.

4. Az informatikai rendszer biztonsága

4.1 A rendszergazda

A **Szolgáltató** informatikai biztonsági felelőse a szervezet rendszergazdája.

Az informatikai biztonság terén feladata:

- A **Szolgáltató** informatikai biztonsági feladatainak tervezése, meghatározása, irányítása és ellenőrzése.
- Az informatikai biztonsági szabályzatok elkészítése, vagy azokban való közreműködés, a szabályzatok betartatása, a vonatkozó részeinek karbantartása.
- Részvétel a biztonsági események felderítésében, elemzésében és kezelésében.
- Az információbiztonsági tevékenység koordinálása.
- Az adat- és információvédelemmel kapcsolatos veszélyforrások felmérése és elemzése.
- Gondoskodás az informatikai biztonsági szabályzatok naprakészen tartásáról, az abban foglaltak betartásának ellenőrzéséről.
- Az informatikai biztonsági eszközök állapotának figyelemmel kísérése, javaslatot azok cseréjére, bővítésére.

4.2 Adatgazda

Az adatgazdai intézmény célja a **Szolgáltató** adatvagyona számára a megfelelő biztonsági környezet kialakítása azáltal, hogy az adatok kezelésének szabályaival kapcsolatos felelősségek az adatokat ténylegesen felhasználó betegállátási folyamatokra, az azt végző személyekre hárulnak.

4.3 Felhasználók

Felhasználó: a **Szolgáltató** összes, elektronikus információs rendszert használó munkatársa ill.

Külső felhasználó: az összes, szerződés alapján a rendelőhelyiségek használatára jogosult egészségügyi szolgáltató (természetes személyek vagy gazdasági társaság) a külső felek a **Szolgáltató** biztonsági szabályainak és elvárásainak betartása mellett férhetnek hozzá a **Szolgáltató** elektronikus információs rendszeréhez.

A külső felhasználók hozzáférését a hozzáférés indokának megszűnte után azonnal, ill. az együttműködés lejártakor automatikusan meg kell szüntetni.

A **Szolgáltató** külső szolgáltató csak egészségügyi tevékenység végzésére szerződhet – tipikusan rendelőbérleti szerződés –, és mint ilyen, számára ugyanazok az egészségügyi jogszabályok a vonatkozók, mint a **Szolgáltató**-re.

4.4 A felhasználói jelszókezelés

A jelszavak felhasználói kezelését szabályozni kell, figyelve arra, hogy a felhasználók titokban tartsák, és megfelelő időközönként változtassák jelszavaikat. Emellett biztosítani kell, hogy a jelszavak kiosztásakor, illetve használatakor csakis a tulajdonos szerezzen tudomást a jelszóról.

Annak érdekében, hogy a jelszavakkal történő hitelesítés kellően megbízható legyen, gondoskodni kell arról, hogy:

a) a jelszavak legalább 6 karakterből álljanak,

b) lehetőleg vegyesen kis és nagybetűket, számokat és írásjeleket is tartalmazzanak,

c) a jelszavakat kéthavonta ki kell cseréltetni a felhasználóval.

A jelszavak titkosak, ezért azokat minden felhasználó köteles úgy kezelni, hogy rajta kívül más tudomására ne jusson.

Tilos a jelszót:

a) más tudomására hozni,

b) más számára ismert vagy hozzáférhető, vagy látható helyen (pl. monitororra ragasztva) tárolni,

c) úgy megválasztani, hogy az adott személyre jellemző és ezért könnyen kitalálható legyen.

4.5 Felhasználói biztonsági követelmények

A hálózati bejelentkezéshez a felhasználóknak felhasználónévvel és jelszóval kell azonosítaniuk magukat.

A munkaállomásokon telepített operációs rendszert úgy kell beállítani, hogy ha a munkatárs 10 percen túl nem használja a rendszert, az automatikusan lezárja a munkaállomást, és a munka újbóli megkezdésekor felhasználónév, jelszóval kell a munkatársnak azonosítania magát.

A felhasználókat kötelezni kell arra, hogy csak az aktuális munkához szükséges dokumentumokat tartsák az asztalon/képernyőn, és ne hagyják ezeket a dokumentumokat, adatokat felügyelet nélküli hozzáférhető helyen.

4.6 Távmunka és távoli elérés szabályai

Szabályozni kell, hogy a biztonságos távoli hozzáférés, illetve munkavégzés érdekében milyen tevékenységek és technikai feltételek szükségesek.

Mivel a **Szolgáltató** által használt beteg- és digitális felvétel nyilvántartó rendszerek szállítóinak székhelye földrajzilag távol esik a **Szolgáltató** rendelőitől, a rendes és rendkívüli szoftverkövetések, valamint az eseti segítségnyújtások távoli eléréssel történnek. Távoli hozzáférés és munkavégzés csak indokolt esetben engedélyezhető, és a hozzáférés, adatcsere biztonsága érdekében külön eljárásokat kell meghatározni és megvalósítani.

Külső rendszerből csak olyan csatlakozás engedélyezhető, amely során a felhasználó csak adatellenőrzésre, és –feldolgozásra képes. Adatmásolás, tárolás vagy továbbítás távoli rendszerbe nem engedélyezhető ilyen kapcsolat esetében.

Szabályozni kell, hogy mekkora az inaktív vagy teljes időtartam, amely után az adatkapcsolatot meg kell szüntetni.

4.7 Adatmentés

Cél: Az elviselhetetlen mértékű adatvesztés megakadályozása, és az elvárt időn belüli adatvisszaállítás biztosítása.

4.7.1 Információk biztonsági mentése

Minden, a **Szolgáltató** kezelésében vagy használatában lévő, elektronikus formában tárolt információról biztonsági mentéseket kell készíteni.

4.7.2 A betegnyilvántartó rendszer mentési eljárása

Biztonsági mentéseknek kell készülnie

a) az online elérhető (éles, tartalék, teszt) adatbázisokról és fájlrendszer könyvtárakról,

b) az offline elérhető (archivált) adatbázisokról és fájlrendszer könyvtárakról.

A mentés normál (Teljes-FULL): azaz minden mentési folyamattal mentésre kerül az összes állomány, függetlenül az előző mentés időpontjától és annak státuszától.

Az adatbázis-mentés ütemezett feladatként automatikusan történik minden munkanap végén.

Az automatikus mentés elindítását munkaidőn túl kell ütemezni, hogy az alkalmazások ne legyenek használatban és ne legyenek nyitott állományok. A mentés eredményességét és futási idejét a mentés másnapján a rendszergazda ellenőrzi.

A mentés Backup szerverre történik, amiről az adatokat havi rendszerességgel kell menteni külső tárolóra. A külső tárolókat zárt archívumszekrényben kell tartani.

4.8 Naplózás

A **Szolgáltató** informatikai rendszere biztonsága szempontjából lényeges események rögzítésére a Windows Eseménynaplót használja. A rendszergazdának havonta ellenőriznie kell a naplóállományok bejegyzéseit.

Biztosítani kell, hogy az elektronikus információs rendszer megvédje a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

4.9 Felelősség

Az adatmentések felelőssége a rendszergazda hatáskörébe tartozik.

5. Az egészségügy szolgáltató adatjelentési kötelezettségei

5.1 Havi teljesítményjelentés a Nemzeti Egészségbiztosítási Alapezelő részére

A **Szolgáltató** a társadalombiztosítás keretein belül történő betegellátásról érvényes finanszírozási szerződése teljesítése során, a jogszabályokban előírt módon havonta egyszer, az erre a NEAK által meghatározott időben (a tárgyhónapot követő hónap 5. munkanapjáig), formában (rekordkép) és úton (elektronikus úton, rejtjelezéssel védett adatátviteli vonalon) tételes adatjelentést küld a NEAK részére.

A finanszírozási jelentésben a **Szolgáltató** a közfinanzírozott szervezeti egységén elvégzett valamennyi gyógyító-megelőző ellátásról adatot szolgáltat.

A finanszírozási adatjelentés részletes szabályait az erről szóló 43/1999. (III. 3.) Korm. rendelet és az egészségügyi szakellátás társadalombiztosítási finanszírozásának egyes kérdéseiről szóló 9/1993. (IV. 2.) NM rendelet rögzíti.

5.2 Elektronikus Egészségügyi Szolgáltatási Tér

A **Szolgáltató** a vonatkozó jogszabályban előírtak pontos betartásával egészségügyi adatokat továbbít a Térbe. Az erre vonatkozó részletes szabályokat az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016. (XII. 21.) EMMI rendelet (EESZT rendelet) rögzíti.

5.3 Felelősség

A jelentéshez és adattovábbításhoz szükséges automatizált informatikai folyamatok biztonságosságáért, a file-ok megfelelő formátumáért (valódiságért) a betegnyilvántartó rendszer licensztulajdonosa felelős.

6. Incidenskezelés

A **Szolgáltató** rendszergazdája folyamatosan figyeli a Kormányzati Eseménykezelő Központ által a kritikus hálózatbiztonsági eseményekről és sérülékenységekről közzétett figyelmeztetéseit (http://www.cert-hungary.hu/aggregator/sources/2), és az egyéb forrásból érkező riasztásokat.

Incidens esemény bekövetkeztekor, vagy ennek alapos gyanúja esetén arról eseti jelentést kell készíteni.

Az információbiztonsági szabályok megsértéséről a rendszergazdának tájékoztatnia kell a **Szolgáltató** ügyvezetőjét, együtt minősítik az incidenst a körülmények ismeretében. Az ügyvezető az incidens súlyának ismeretében dönt a következményekről, az incidens kezeléséről a hibák javításáról.

Amennyiben a sérülékenység jellege olyan, hogy annak elterjedése megelőzhető, hogyha a felhasználók például nem nyitnak meg bizonyos web oldalakat vagy egy adott jellegű elektronikus levélben található linkre nem kattintanak, akkor belső figyelmeztetést kell kiadni a **Szolgáltató** szokásos értesítési rendszerén (pl. e-mail) keresztül.

6.1 Bejelentési kötelezettség

Amennyiben felmerül a gyanú, hogy a **Szolgáltató** rendszere számítógépes biztonsági incidens áldozatává vált, vagy éppen ennek folyamata alatt van, akkor a jogszabályokban meghatározott esemény bejelentési kötelezettség mellett be kell jelenteni ezen incidens tényét és fel kell venni a kapcsolatot az érintett, külön jogszabályban meghatározott szervekkel is.

Amint a **Szolgáltató** ügyvezetőjének tudomására jut egy esetleges az adatvédelmi incidens, azt indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásukra jutott, bejelenteni köteles az illetékes felügyeleti hatóságnál, kivéve, ha az elszámoltathatóság elvével összhangban bizonyítani tudják, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát, az előírt információkat pedig – további indokolatlan késedelem nélkül – részletekben is közölni lehet.

Az adatvédelmi incidensről szóló bejelentést a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) mindenkori kapcsolati pontjára (http://naih.hu/uegyfelszolgalat,--kapcsolat.html) kell eljuttatni.

A bejelentés összeállításának és beadásának felelőse a **Szolgáltató** megbízott adatvédelmi tisztviselője.

A **Szolgáltató** nyilvántartja az adatvédelmi incidenseket, feltüntetve az adatvédelmi incidenshez kapcsolódó tényeket, annak hatásait és az orvoslására tett intézkedéseket.

6.2 Az érintett tájékoztatása az adatvédelmi incidensről

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, **Szolgáltató** indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről.

Az érintettet nem kell tájékoztatni, ha a következő feltételek bármelyike teljesül:

a) A Szolgáltató megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat;

b) a **Szolgáltató** az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett, az említett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg;

c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

6.3 Ügymenet- és ellátás folytonosság

A **Szolgáltató** azonosítania kell a kritikus működési folyamatokat és beépítenie a működésfolytonosságot az informatikai biztonság irányítási követelményeibe más folytonossági követelményekkel, amelyek olyan szempontokra vonatkoznak, mint műveletek, személyzettel való ellátás, fogyóeszközök.

6.4 Felelősség

Az adatvédelmi incidensek kezelése az ügyvezető hatáskörébe tartozik.

7. Adatkezelési kérés- és panaszkezelés

Cél: Gondoskodni arról, hogy a **Szolgáltató** által kezelt személyes adatokról az érintett adatalanyok a megfelelő hatékonysággal és minőségben kapjanak információt és segítséget.

7.1 Alapelvek

A **Szolgáltató** meghatározott rendszerességgel tréningeket szervez, melyeken kiemelt figyelmet fordít arra, hogy alkalmazottai és szerződéses partnerei az érintett magánszemélyek részére a személyes adatok kezelésére vonatkozó, az alábbiakban ismertetett valamennyi információt és tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más módon – ideértve adott esetben az elektronikus utat is – kell megadni. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

Az elsődlegesen információt nyújtó helyeken dolgozó kollégáknak – adminisztrátoroknak – mindig pontosan tisztában kell lenniük az adatkezelési elvekről és jogszabályokról és a megfelelő kommunikációról.

Kérés vagy panasz esetén a **Szolgáltató** indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható.

A **Szolgáltató** a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:

a) az adatvédelmi tisztviselő elérhetőségei, ha van ilyen;

b) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;

c) a **Szolgáltató** vagy harmadik fél jogos érdekei, ha van ilyen;

d) adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái, ha van ilyen;

e) adott esetben annak ténye, hogy a **Szolgáltató** harmadik országba vagy nemzetközi szervezet részére kívánja továbbítani a személyes adatokat.

7.2 Az érintett jogai

A **Szolgáltató** egészségügyi dokumentációt kezel, melynek megőrzésére és kezelésére a már említett jogszabályok irányadók. Az érintett jogait ezen jogszabályokkal összhangban tudja gyakorolni (pl. nem törölhető adat, amennyiben nem járt le a jogszabályban előírt kötelező megőrzési idő).

Az érintett jogosult arra, hogy a **Szolgáltató**.-től visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha ilyen adatkezelés folyamatban van, jogosult arra, hogy a személyes adatokhoz és a következő információkhoz hozzáférést kapjon:

a) az adatkezelés céljai;

b) az érintett személyes adatok kategóriái;

c) azon címzettek vagy címzettek kategóriái, akikkel, illetve amelyekkel a személyes adatokat közölték vagy közölni fogják, ideértve különösen a harmadik országbeli címzetteket;

d) adott esetben a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;

e) az érintett azon joga, hogy kérelmezheti a **Szolgáltató**.-től a rá vonatkozó személyes adatok helyesbítését és törlését a jogszabályban előírt megőrzési időn túl;

f) a valamely felügyeleti hatósághoz címzett panasz benyújtásának joga;

Ha személyes adatoknak harmadik országba való továbbítására kerül sor, az érintett jogosult arra, hogy tájékoztatást kapjon a továbbításra vonatkozóan a megfelelő garanciákról.

A **Szolgáltató** az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátja. Az érintett által kért további másolatokért a **Szolgáltató**. az adminisztratív költségeken alapuló, ésszerű mértékű díjat

számíthat fel. Ha az érintett elektronikus úton nyújtotta be a kérelmet, az információkat széles körben használt elektronikus formátumban kell rendelkezésre bocsátani, kivéve, ha az érintett másként kéri.

Az érintett jogosult arra, hogy kérésére **Szolgáltató** indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat.

Az érintett jogosult arra, hogy a rá vonatkozó, általa a **Szolgáltató** rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa.

7.3 Felelősség

A kérés- és panaszkezelés koordinálása és végrehajtása az ügyvezető hatáskörébe tartozik.

8. Oktatás, képzés, tudatosítás

Cél: Folyamatosan gondoskodni arról, hogy a felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek, és motiválva legyenek a szervezet információvédelmi szabályzatainak és intézkedéseinek a betartására. A felhasználók legyenek oktatva a biztonsági eljárásokról és az adatfeldolgozó eszközök helyes használatáról a lehetséges biztonsági kockázatok minimalizálása érdekében.

8.1 Számítógéphasználati elvek

A **Szolgáltató** minden dolgozója jogosult a munkaköréhez tartozó adat- és információ hozzáféréshez, azok felvitelére és karbantartásra.

A **Szolgáltató** minden belépő új munkatársa köteles a belépésével egyidejűleg az Adatvédelmi szabályzatban és kapcsolódó dokumentumaiban foglaltakat elolvasva megismerni, tudomásul venni.

A **Szolgáltató** az információ feldolgozó eszközöket (számítógépeket, nyomtatókat, fénymásoló- és fax berendezéseket, scannereket, stb.) munkavégzés céljára biztosítja az azokat felhasználó munkavállalóknak.

Az Adatvédelmi szabályzatban és kapcsolódó dokumentumaiban foglaltak be nem tartása szankcionálást von maga után, amely akár a munkaviszony megszűntetését, polgári peres vagy büntetőeljárást is magába foglalhat. A **Szolgáltató** fenntartja magának a jogot, hogy a bármely felhasználó számára dedikált előjogokat, kiváltságokat azonnali hatállyal visszavonja, illetve megszűntesse.

A szervezet ügyvezetője azonnal köteles intézkedést kezdeményezni a **Szolgáltató** munkatársával vagy a külső szerződéses partnerrel szemben, amennyiben azok megsértik az Adatvédelmi szabályzatban és kapcsolódó dokumentumaiban foglaltakat. Az ügyvezető köteles a szükséges intézkedéseket megtenni, amennyiben az adatvédelemre, a számítógép vagy az internet használatra vonatkozó eljárásokat a saját vagy külsős munkatárs megsérti.

A felhasználók semmilyen szoftvert nem telepíthetnek a **Szolgáltató** rendszergazdája jóváhagyása nélkül, beleértve az Internetről letölthető vagy máshonnan beszerzett ingyenes vagy időszakosan szabadon felhasználható programokat. Új szoftver telepítésének igényét a közvetlen vezetőnek kell bejelenteni.

8.2 Internet használata

Mivel **Szolgáltató** számára az Internet kapcsolat üzletileg kritikus, ezért az Internetet használó munkavállalóknak az alábbi szabályokat kell betartaniuk:

- Tilos az Internet illegális (jogszabályokba ütköző) célokra történő használata, mások személyiségi jogainak megsértése; tiltott haszonszerzésre irányuló tevékenység (pl. piramis-, pilótajáték); a szerzői jogok megsértése; software szándékos és tudatos illegális terjesztése,
- Tilos másokra nézve sértő, mások vallási, etnikai, politikai vagy más jellegű érzékenységét sértő, másokat zaklató tevékenység,
- Tilos az Internet hálózathoz kapcsolódó más - hazai vagy nemzetközi - hálózatok szabályaiba ütköző tevékenységek, amennyiben ezek a tevékenységek ezen hálózatokat érintik.
- Tilos a profitszerzést célzó direkt üzleti célú tevékenység, reklámok terjesztése,
- Tilos a hálózat, illetve erőforrásai normális működését megzavaró, veszélyeztető tevékenység,
- Tilos a hálózatot, illetve erőforrásait indokolatlanul, vagy szándékosan túlzott mértékben, pazarló módon igénybevevő tevékenység,
- Tilos az Interneten honlappal rendelkező szállítók, szolgáltatók, azok termékeinek, szolgáltatásainak minősítése,
- Tilos a **Szolgáltató** méltatlan oldalak keresése, látogatása,
- A felhasználók nem tölthetnek le, illetve nem tölthetnek fel az Internetre semmilyen olyan jellegű információt, adatot, szoftvert, amely összeférhetetlen a **Szolgáltató** Adatvédelmi szabályzatával,
- Tilos az Internetről letöltött szoftverek (shareware vagy freeware termékek) informatikai eszközein történő telepítése.
- A szervezet vezetőjének és a rendszergazdának jogában áll a felhasználók előzetes értesítése nélkül is bármely weboldal látogatását megtiltani, illetve a weboldalak látogatását oly módon szabályozni, hogy tételesen megadja a látogatható helyek körét.

8.3 e-mail, elektronikus levelezés

A **Szolgáltató** e-mail címét a **Szolgáltató** rendelői számítógépein az adminisztrátorok és a megbízott orvosok munkavégzés céljából használhatják, meghatározott folyamatokban (pl. páciens-megkeresések megválaszolása, lelet elektronikus formában történő küldése és/vagy fogadása, kapcsolattartás beszállítókkal).

A **Szolgáltató** levelezőrendszerében folytatott minden tevékenységet az előző fejezetekben leírt elveknek megfelelően kell folytatni. Ezeknek az elveknek a betartását a **Szolgáltató** vezetése külön figyelmeztetés nélkül is ellenőrizheti, és erről a tényről a munkaszerződésben, a számítógépes jogosultság kiosztásakor, vagy munkáltatói utasításban tájékoztatja a felhasználóit.

Az elektronikus levelezés munkaáltatói ellenőrzése minden esetben célhoz kötött.

A levelezési rendszer paramétereit, beleértve a szűrőfeltételeket, korlátozásokat (mellékletek szűrése: nagyméretű multimédiás file-ok, futtatható file-ok) a rendszergazda állítja be, az üzleti és biztonsági követelmények figyelembe vételével a **Szolgáltató** ügyvezetőjének egyidejű tájékoztatása és engedélye alapján.

8.4 Oktatási eljárásrend

A szervezet valamennyi munkatársát, és ahol szükséges, a harmadik fél felhasználóit is, megfelelő képzésben kell részesíteni a szervezet biztonsági szabályairól és eljárásairól. Ezeket az ismereteket rendszeresen naprakész ismeretek közlésével fel kell újítani. A képzés foglalja magába a biztonsági követelményeket, a jogi felelősséget, az üzleti óvintézkedéseket, valamint az informatikai eszközök helyes használatát, például a bejelentkezési eljárást, a szoftverek használatát. Az informatikai biztonságtudatossági képzés elvégzését az elektronikus információs rendszer használója aláírásával igazolja. Aláírásként elfogadható az egyértelmű és pontosan beazonosítható elektronikus visszajelzés is (e-mail.)

Kiemelten fontos az adatkezelési műveletekben vevő személyzet tudatosság-növelése és képzése. Az ilyen felhasználóknak pontosan tisztában kell lenniük a mindenkori adatkezelési rendelkezésekkel, azok etikai és jogszabályi vonatkozásaival, az ebből fakadó személyes kötelezettségeikkel és felelősségeikkel.

Az általános biztonságtudatosítási képzés mellett, melynek mindenkire vonatkoznia kell a szervezetben, különleges biztonsági képzés is szükséges az adminisztrátor munkakörben dolgozó személyzet számára. A biztonsági képzés mélységének az informatikának a szervezeten belüli általános fontosságához kell igazodnia, és az adott szerep biztonsági követelményeinek megfelelően kell változnia.

8.5 Felelősség

Az oktatás megszervezése, a tematika kidolgozása és az előadás megszervezése az ügyvezető hatáskörébe tartozik.

9. Ellenőrzési eljárásrend

Cél: Folyamatosan gondoskodni arról, hogy a szabályzatban foglaltak a megfelelő módon kerülnek alkalmazásra.

9.1 Általános elvek

Az Adatvédelmi szabályzatban előírt eljárások és szabályok érvényesítése hagyományos vezetési eszközökkel történik, melynek elemei:

- eseti vagy rendszeresen ismétlődő ellenőrzés (továbbiakban: ellenőrzés);
- felelősségre vonás az ellenőrzéssel feltárt mulasztás miatt (továbbiakban: felelősségre vonás).

A kontrollok kialakításánál elsődlegesen azt kell figyelembe venni, hogy azok által az információbiztonság szintje mérhető legyen. Az ellenőrzési célkitűzés ismeretében meg kell jelölni az ellenőrzés eszközeit (dokumentumok, naplók, szoftverek, adatok, amelyek a biztonsági rendszerről hiteles képet tudnak adni), azok tartalmi követelményeit.

Az ellenőrzés eredményét minden esetben ki kell értékelni, és a megfelelő következtetéseket le kell vonni, illetve vissza kell csatolni a biztonsági folyamatra. Bizonyítható mulasztás feltárása esetén szükség szerinti mértékű felelősségre vonási eljárást kell kezdeményezni.

9.2 Az ellenőrzések területei, célkitűzései

Az informatikai biztonsággal kapcsolatos ellenőrzések az alábbiak:

- **Megfelelőségi vizsgálat**: célja felderíteni, hogy a **Szolgáltató** rendelkezik-e a törvényi előírásokban meghatározott személyi, eljárási, tárgyi feltételekkel.
- **Az informatikai biztonság szintjére vonatkozó vizsgálat:** célja felderíteni, hogy az informatikai biztonság szintje megfelel-e a **Szolgáltató** mint egészségügyi szolgáltatóra vonatkozó kötelezettségeknek.
- **Az informatikai biztonsági szabályok betartásának ellenőrzése:** Célja felderíteni, hogy a **Szolgáltató** informatikai biztonsági szabályait az illetékes személyek ismerik-e, illetve betartják-e. Ez az ellenőrzés az informatikai biztonság egy-egy területére is leszűkíthető.

9.3 Felelősség

Az ellenőrzés a **Szolgáltató** szerződéses adatvédelmi tisztviselője hatáskörébe tartozik.

10. Dokumentum történet

Dátum	Verzió	Módosította	Módosítás oka
2018. 05. 22	1.0	Haraszti Hedvig	Személyreszabás