Adatvédelmi kockázat-értékelés és hatásvizsgálat

DPIA-információ

DPIA

Chirurgus Egészségügyi Szolgáltató Kft., cégjsz.: 13-09-130768 képviselő (orvos) neve dr. László Gyula, címe: 2040 Budaörs, Fém utca 11., e-mail címe info@chirurgus.hu, telefonja: +36 30 9525353, honlapja www.drlaszlogyula.hu www.drissplasztika.hu www.ansariaesthetics.com, működési engedély száma BP-02/NEO/6014-6/2020., adószáma 11793959-1-13.

Szerző neve

Inspekció 99 BT. szakértői és tanácsadó cég

Értékelő neve

dr. Hanti Péter

Jóváhagyó neve

Dr. László Gyula üv.

Létrehozás dátuma

30/01/2021

Adatvédelmi tisztviselő neve

dr. Hanti Péter

Adatvédelmi tisztviselő véleménye

megfelelő kockázatértékelés és hatásvizsgálat

Érintettek véleményének kikérése.

Az adatkezeléssel érintettek véleményének kikérésére nem került sor.

Azon ok megjelölése, ami alapján az érintettek véleményének kikérésére nem került sor.

A potenciális érintettek relative nagy száma és egyéb objektiv körülmények (költségigény), valamint az adatkezelésre vonatkozó strikt jogszabályi környezet miatt az érintettek véleményének kikérésére nem került sor.

Összegzés

Áttekintés

Az adatkezelés rövid bemutatása

Az adatkezelő (egészségügyi) szolgáltató neve és címe (képviselő elérhetőségei):

Chirurgus Egészségügyi Szolgáltató Kft., cégjsz.: 13-09-130768 képviselő (orvos) neve dr. László Gyula, címe: 2040 Budaörs, Fém utca 11., e-mail címe info@chirurgus.hu, telefonja: +36 30 9525353, honlapja www.drlaszlogyula.hu www.drissplasztika.hu www.ansariaesthetics.com, működési engedély száma BP-02/NEO/6014-6/2020., adószáma 11793959-1-13.

Az adatkezelés célja: Alapvetően egészségügyi szolgáltatásban részesülők egészségügyi ellátása; ideértve a szorosan ezen fő célhoz szükségképpen kapcsolódó közegészségügyi-járványügyi-népegészségügyi célokat, a betegjogok érvényesítésének, minőségbiztosítás célját, hatósági-törvényességi-szakmai ellenőrzés célját. Informatikai biztonság. Foglalkoztatottak jogviszonyával kapcsolatos jogszabály által előírt adatrögzítés, számviteli szabályoknak való megfelelés. Honlap működtetése. Marketing cél.

Az adatkezelés jogalapja: Lehet önkéntes (hozzájárulás), törvény által kötelezően előírt, szerződés teljesítése, az érintett vagy más személy létfontosságú érdekeinek védelme, és érdekmérlegelésen alapuló.

Az érintettek köre (kategóriái): Alapvetően az egészségügyi szolgáltatást igénybe vevők, valamint esetleg az adatkezeléshez szükségképpen kapcsolódó harmadik személy érintettek. Honlap látogatói. Foglalkoztatottak.

Az érintettekre vonatkozó adatok (kategóriáinak) leírása: Az egészségügyi szolgáltatáshoz-ellátáshoz jogszabály által előírt illetve szükségesen felvett személyes és egészségügyi adatok. Érintett törvény által előírt személyes adatai számviteli bizonylatok kiállításához. Foglalkoztatottak jogszabály szerint előírt nyilvántartásához szükséges személyes adatai. Marketing céllal név, elérhetőségi adatok. IP cím.

Az adatok forrása: az érintett, a róla jogszerűen információt szolgáltató más szervek és személyek, az adatkezelőhöz jogszerűen került dokumentumok, érintettre vonatkozó információt tároló elkülönült rendszerek (pl. Elektronikus Egészségügyi Szolgáltatási Tér).

Tényleges adatkezelés helye: 2040 Budaörs, Fém utca 11., 1023 Budapest Margit utca 21., 1023 Budapest Margit utca 25., 1125 Budapest, Istenhegyi út 31/B.

Adatmegőrzési időket jellemzően jogszabály határozza meg, egyebekben az adatkezelési tájékoztató szerint történik.

Adattovábbításra jogszabály kötelező előírása illetve az érintett önkéntes hozzájárulása alapján kerül sor jellemzően.

<u>Adatfeldolgozók:</u>

Nemzeti Infokommunikációs Szolgáltató Zrt-t (1081 Budapest, Csokonai u. 3.)

OKFŐ, 1125 Budapest Diós árok 3., tel.: 06 1 356 1522, e-mail: aeek@aeek.hu, honlap: https://e-egeszsegugy.gov.hu

NEAK (1139 Budapest, Váci út 73/A., tel.: 06 1 350-2001, e-mail: neak@neak.gov.hu, honlap: http://www.neak.gov.hu)

Magyar Telekom Nyrt. 1097 Budapest, Könyves Kálmán körút 36.

Vodafone Magyarország Zrt. 1096 Budapest, Lechner Ödön fasor 6.

Google LLC Mountain View, Kalifornia, Egyesült Államok

Yahoo Inc. Kalifornia Sunnyval, Egyesült Államok

Facebook, Menlo Park, Kalifornia, Egyesül Államok

Nextserver Rackhost Zrt. 6722 Szeged, Tisza Lajos körút 41.

Evolutionet kft. 7342 Mágocs, Széchenyi utca 75.

Public Art Multimedia Szolg. Kft. 1055 Budapest, Falk Miksa utca 24-26.

Halasi Zsolt 2517 Kesztölc, Kökény utca 29.

Árpa Solutions 9025 Győr, Töltésszer utca 3.

Magyar Posta (Budapest Üllői u. 114-116., tel.: 06-1-767-8282, e-mail: ugyfelszolgalat@posta.hu)

Mo-Tax kft. 1163 Budapest, Máté utca 2.

OTP Bank Zrt. XVI. ker. fiók 1163 Budapest, Jókai utca 3/B.

Microsoft Redmond Washington Egyesül Államok

Alapvetően betartandó szabályokat a GDPR, az Infotv., az Eüak. és az Eütv. szabályozza. Jóváhagyott magatartási kódexek és adatvédelmi tanúsítványok nincsenek.

Az adatkezeléshez kapcsolódó felelősségi viszonyok bemutatása

A GDPR rendelkezéseivel összhangban adatkezelő és az általa igénybe vett adatfeldolgozók felelőssége elkülönül az általuk az adatokon végzett műveletekért. Az adatfeldolgozóért való felelősség a GDPR alapján elkülönülhet az adatkezelőétől: (lehet önálló), egyetemleges vagy együttes.

Rendelkezik-e az adatkezelésre alkalmazandó valamilyen szabvánnyal?

Adatkezelésre vonatkozó szabvány, jóváhagyott magatartási kódex illetve tanusítvány jelenleg nem áll rendelkezésre.

Véleményezés : Elfogadható

Adatok, az adatkezelés folyamata, az adatok kezelésére szolgáló eszközök

A kezelt személyes adatok köre

A kezelt adatok köre: Az adatokat felvevő-rögzítő egészségügyi dolgozó által, az adott egészségügyi ellátáshoz-szolgáltatás igénybevételéhez szükségesnek tartott releváns, *személyes adataival összekapcsolt* észlelt-vizsgált-mért-származtatott egészségügyi adatok - bármely jogszerű forrásból származzanak is azok (ideértve olyan információt is mely más adatokból levonható következtetésből származik). Értelemszerűen az ellátáshoz szükséges mértékben a korábban keletkezett, múltra vonatkozó adatokat is kezelnek. Közfinanszírozott ellátásokkal összefüggésben egészségügyi adatokat értelemszerűen a Társadalombiztosítási Azonosító Jelhez (TAJ számához) kapcsoljuk, azzal együtt kezeljük. Ha a betegellátó szakmailag indokoltnak tartja: kép-, videó-, illetve hangfelvételt is készíthet az érintett előzetes tájékoztatását követően a szükséges, személyiségi jogait nem sértő módon és mértékben; illetve ezen felvételeket az érintett is rendelkezésre bocsáthatja (pl. saját testi elváltozásairól készített fényképek formájában, kezelések eredményét dokumentáló kezdeti és végleges státuszt rögzítő képi dokumentáció). *Amennyiben kifejezetten hozzájárul ellátása előtt illetve után Önről készült felvételeket közzéteszünk, illetve referenciaként hivatkozunk rá.* Az ellátás jellegéből adódóan szükségképpen harmadik személyekre vonatkozó információk, az érintett kezelése-ellátása érdekében is az indokoltan kezelt adatok közé tartozhatnak; ideértve azt is ha ő közöl másokról információkat (ezen adatok megfelelőségét az elvárható mértékben ő biztosítja). Ez vonatkozik *különleges adatokra is (mint amilyenek pl. az egészségügyi állapottal összefüggő információk is, melyeket szenzitív adatoknak is hívunk).*

Személyes és személyazonosító adatok közül különösen: a név, nem, lakcím, születési idő és hely, születési név, anyja neve, tartózkodási

hely, elérhetőségi adatok (pl. telefon, e-mail, IP cím), családi állapot, TAJ szám, az Európai Gazdasági Térség (EGT) külföldi országaiban biztosított személyeknél az Európai Egészségbiztosítási Kártya (EUCARD) vagy más hasonló funkciójú nyomtatvány adatai, EGT-n kívüli állambeli beteg esetében az útlevél szükséges adatai, közgyógyászati ellátását igazoló okirat száma kelte és lejárati ideje, szükség esetén személyi igazolványának száma, foglalkozás, munkahely; törvényes képviselő adatai, értesítendő, meghatalmazott (képviselni, eljárni, nyilatkozni, aláírni Ön helyett jogosult) személy, tájékoztatható, dokumentációba betekinteni-másolatra az érintett helyett vagy mellett jogosult személy, ellátásával összefüggésben bizonyos döntéseket hozni jogosult, illetve támogató személy azonosításához szükséges adatok-elérhetőségek kerülnek rögzítésre szükség szerint.

Egészségügyi adatok közül különösen: kórelőzmény, vizsgálatok ideje, eredménye; kórismék, kockázati tényezők, szükség esetén védőoltások, az egyes ellátásokba való beleegyezés-visszautasítások ténye és időpontjai; elvégzett beavatkozások-kezelések ideje és eredményei; gyógyszerérzékenység illetve más allergia, szükség esetén egyes alkalmassági vizsgálatok eredményei, a kapott tájékoztatás tartalma, egyéb az egészségi állapotot és ellátását relevánsan befolyásoló körülmény (mint pl. családi-szociális körülmények, fogyatékosság, sport- és szabadidős tevékenységek) kerülnek rögzítésre megfelelő ellátásához szükséges módon és mértékben. *Természetesen egészségügyi adatokon belül különösen szenzitív adatokat is szükség szerint felhasználunk* (így pl. nőgyógyászati, húgy-ivarszervi, szexuális élettel összefüggő, lelki-pszichikai-pszichiátriai, kóros szenvedéllyel-függőséggel stb. összefüggő adatokat is). A dokumentáció részét képezi továbbá különösen minden vizsgálati lelet, konzílium adata, ápolási dokumentáció, szövettani lelet, képalkotó diagnosztika felvételei. Foglalkoztatottak jogszabály által előírt adatai.

Adatmegőrzési idők: A szolgáltatónál tárolt egészségügyi dokumentációját az adott adat felvételét követő főszabályként 30 évig, esetlegesen eljuttatott zárójelentéseit 50 évig, 2012. január 1-ét követően készült képalkotó diagnosztikai felvételeit 10 évig őrzik meg, ezen dátumnál régebbieket pedig 30 évig (rendre ugyanez érvényes ezen tájékoztató megismerésére vonatkozó nyilatkozatára és adatkezelési nyilvántartásra is azzal, hogy megőrzésükre a leghosszabb időtartamú adatkezelést kell alapul venni). Adatvédelmi incidens nyilvántartásuk adatokat 20 évig kezel, adattovábbítási nyilvántartásuk 20 évig. Számviteli bizonylatokat 8 évig őrzik meg. Marketing céllal a hozzájárulás

visszavonásáig. Honlap látogatásával összefüggő „sütiket” legfeljebb 5 évig.

Az adatokhoz hozzáférhetnek: Az érintett kezelésében résztvevő abban közreműködő egészségügyi szolgáltatók és az általuk bármely jogviszonyban foglalkoztatott egészségügyi és egészségügyben dolgozók. Így különösen szakorvosok, más betegellátó kezelőorvosok, ellátásban résztvevő egészégügyi szakdolgozók, ellátással kapcsolatban tevékenységet végző más személyek, szolgáltató által foglalkoztatott illetve közreműködő személyek és szolgáltatók, stb. – akik *mint az érintett adatait kezelők nevét, beosztását és szakképesítését, egyéb nyilvános adatait, valamint a szolgáltatóhoz fűződő jogviszonyát az érintett megismerheti*. Ellátással össze nem függő adathoz legfeljebb annyiban, olyan módon és ideig férhetnek hozzá, mely annak megállapítását lehetővé teszi, hogy az információnak van-e köze az aktuális ellátáshoz. Amennyiben az egészségügyi dolgozót más helyettesíti és ő nyújtja az ellátást, ő is hasonló jogosultságokkal rendelkező jogszerű adatkezelőnek minősül. Szükség esetén különösen a szolgáltató vezetője; informatikus; szakfelügyelő főorvos; egészségügyi dolgozóval szembeni panasz esetén az illetékes etikai bizottság, illetékes egészségügyi hatóság képviselője, az egészségbiztosító feljogosított alkalmazottja, betegjogi képviselő és az őt foglalkoztató szerv, tisztiorvos, járványügyi felügyelő, egészségbiztosítási szerv és képviselői, orvosszakértői szerv, hatóságok a szükséges módon és mértékben szintén megismerhetik az (egészségügyi) adatokat.

Adattovábbítások címzettjei: Két vagy több pácienst kezelő, ellátásban-egészségügyi szolgáltatásban részesítő, abban közreműködő egészségügyi szolgáltató (betegellátó) papíralapon vagy elektronikus info-kommunikációs csatornán keresztül (pl. beutaló, konzíliumkérő, a bármely formában és módon visszaérkező leletek útján; telefonon, e-mail-en, más speciális elektronikus adatátvitellel) az ellátásához szükséges, azzal összefüggő, szakmailag kapcsolatba hozható információkat közvetlenül és kölcsönösen továbbíthatják egymás között (az ellátás eredményeit, a leleteket az azt kérő betegellátó-kezelőorvos természetszerűen megismerheti).

A kiállított recept alapján a gyógyszertár, gyógyászati segédeszköz készítő-javító-forgalmazó, stb. és az ott jogszerűen foglalkoztatott, szintén titoktartásra kötelezett egészségügyi és egészségügyben dolgozók is értelemszerűen kezelhetik az adatokat.

Háziorvos automatikusan értesülhet valamennyi betegét érintő ellátás adatairól elektronikus csatornán vagy papíralapon – *de ezt is megtilthatja az érintett*.

Az érintett ellátásában részt nem vevő ellátók között csak akkor lehetséges kivételesen és a szükséges módon és mértékben adatáram, ha az az adott ellátásához mégis szükséges.

A kapott ellátásokról az Elektronikus Egészségügyi Szolgáltatási Térbe is adatokat töltenek fel elektronikusan, mely ellen teljesen vagy bizonyos adatkezelés tekintetében tiltakozhat.

1. *Számos esetben törvény írja elő a kötelező adattovábbítást (akár az egészségügyi ellátórendszeren kívülre is).* Így különösen:

a.) Munkabalesetek, bizonyos foglalkozási megbetegedések, ártalmak hatósági bejelentése.

b.) Fertőző betegségek (gyanújának) hatósági bejelentése, adattovábbítás az illetékes adatkezelésre jogosult szervekhez.

c.) Bizonyos (kötelező) szűrővizsgálatok eredményeinek hatósági közlése, heveny mérgezések illetékes szervnek történő bejelentése esetében.

d.) Jogszabály alapján kötelező az érintett személyazonosító adataival összekapcsoltan adatait továbbítanunk a különböző jogszabály által előírt betegségregiszterekbe, amennyiben ezekhez kapcsolódó megbetegedése áll fenn.

e.) Hozzátartozók közötti erőszak illetve annak veszélye esetén kötelező jelzéssel élnünk a gyámhivatal felé (kiskorú esetében a szülő egyetértése sem szükséges).

f.) Kiskorú veszélyeztetett állapota miatt/ennek megelőzése érdekében jelzési kötelezettségünk áll fenn a gyermekjóléti szolgálat/gyámhatóság felé (a szülő egyetértése sem szükséges).

g.) Ha a kiskorú sérülése/betegsége vélhetően elhanyagolás/bántalmazás következménye vagy ilyen körülményekről való tudomásszerzéskor (akkor is ha nem minősül súlyosnak): kötelező a gyermekjóléti szolgálatot értesítenünk (a szülő egyetértése sem szükséges).

h.) Súlyos (8 napon túl gyógyuló) sérüléseknél ha az vélhetően bűncselekménnyel függ össze: kötelező a rendőrséget értesítenünk (kiskorú esetében a szülő egyetértése sem szükséges).

i.) Szociális veszélyeztetettség-krízishelyzet esetén: jelzést kell adnunk a családsegítést nyújtó szolgáltatónak.

2. Az alábbi fontosabb szervek illetve személyek főszabálykénti írásbeli megkeresésére, jogszerű célból a kívánt adatok körének megnevezésével továbbítanunk kell a szükséges adatait:

a) Ügyészség, bíróság, igazságügyi szakértő.

b) Büntetőeljárásban a nyomozó hatóság (bizonyos feltételekkel jogosult); szabálysértési hatóság; közigazgatási hatóság.

c) Nemzetbiztonsági szolgálat, terrorelhárítási szolgálat.

d) Bizonyos szociális/társadalombiztosítási ellátások-támogatások illetve kedvezmények megállapításához az orvosszakértői szerv megkeresheti a kezelőorvost (ott alapvetően 5 évig kezelik adatait).

e) Etikai eljárás érdekében az illetékes szakmai kamarai szerv.

Ha az érintett testébe orvosi implantátum került: a NEAK által vezetett kódolt, 50 évig tárolt nyilvántartásból sürgős szükség vagy veszélyeztető állapot megelőzése vagy elhárítása érdekében a NEAK is szolgáltat adatot az arra jogosult egészségügyi szolgáltatónak.

(Feltételezett) gyógyszermellékhatás esetében kötelező az érintett személyes adatait kóddal helyettesítve bejelentést tennie az adatkezelő szolgáltatónak a gyógyszerészeti hatóságnak, a gyógyszerforgalmazónak akik azokat európai adatbázisba is továbbítják.

Néhány hatóság, szerv illetve szervezet csak meghatározott körben és esetben jogosult a szükséges mértékben egészségügyi adatokkal összekapcsolt személyes adatok kezelésére: pl. alapvető jogok biztosa, Állami Számvevőszék, Gazdasági Versenyhivatal, honvédség, oktatási-nevelési szolgáltatórendszer.

Ezen felül általában csak az érintett megfelelő hozzájárulásával továbbíthatnak adatokat az érintett személyes adataival összekapcsoltan.

Az adatkezelési folyamatok bemutatása

A Szolgáltató legfőbb adatkezelési tevékenysége az egészségügyi szolgáltatást igénybe vevők egészségügyi és személyazonosító adatainak kezelése. A jelentkező páciens személyesen a legszükségesebb személyes és egészségügyi adatait megadva jelentkezik ellátásra. A páciens minden szükséges adatát törvény alapján főszabályként önként, ráutaló magatartással jóváhagyva hozzájárulással szolgáltatja, melyet az adatkezelő betegellátó (szakasszisztens vagy kezelőorvos) jellemzően elektronikusan (kisebb részben papíralapon) rögzít. A keletkezett információt főszabályként elektronikusan ennek hiányában papíralapú kartotékrendszerben rögzítenek az érintetthez tartozó elektronikus állományához, míg ezen adatokat a szolgáltató őrzi a kötelező megőrzési időig (szöveges leleteket 30 évig, zárójelentéseket 50 évig, képalkotó felvételeket jelenleg 10 évig). Szükség esetén az arra jogosultaknak ezekből másolatot adnak ki. A kötelező őrzési időt követően az adatokat megsemmisítik.

Melyek a személyes adatok kezelésére szolgáló eszközök?

Az adatokat a rendelői telephelyeken szabványoknak megfelelő papíralapú és elektronikus rendszerekben fizikailag kezelik-tárolják. Felhőalapú adattárolásra e-mail forgalom esetében a Google Inc. 1600 Amphitheatre Pkwy, Mountain View, CA 94043, Egyesült Államok; Yahoo Inc. Kalifornia Sunnyval, Egyesült Államok szolgáltatókat használjuk; míg a medikai szoftver tárhelyét az Árpa Solutions 9025 Győr, Töltésszer utca 3. biztosítja adatfeldolgozóként. A felhőalapú szolgáltatóval, az EESZT-vel biztonságos informatikai csatorna kapcsolja össze a kliens gépek mint végpontok és a központok közötti kommunikáció érdekében. Mindehhez speciális medikai szoftvereket használnak; az adathordozók pedig a Szolgáltató leltárjában kerültek nevesítésre. Szükség és értelem szerint irodai, böngésző és levelezőrendszer is kezelhet személyes adatot.

Véleményezés : Elfogadható azzal, hogy javasolt a Google és a Yahoo mint levélkiszolgálók; illetve a felhőalapú medikai adattárolás használatának felhagyása.

Alapelvek

Arányosság és szükségesség

Az adatkezelés céljai meghatározottak-e, egyértelműek-e és jogszerűek-e?

Az adatkezelés céljai meghatározottak, egyértelműek és jogszerűek, mivel alapvetően az érintettek egészségügyi ellátását célozzák, melyhez szükséges adatkezelést jogszabályok (törvények) tesznek lehetővé illetve kötelezővé. Más célú adatkezelés többnyire jogszabály által előírt kötelező, a honlap látogatásával összefüggő valamint a marketing célú pedig az érintett hozzájárulásával.

Véleményezés : Elfogadható

Mi az adatkezelés jogalapja?

Az adatkezelés jogalapja: jellemzően önkéntes (hozzájárulás), bizonyos esetben törvény által kötelezően előírt, egyes esetekben érdekmérlegelésen alapuló; szerződés teljesítés,

létfontosságú érdekvédelem is jogalap lehet. Egészségügyi szolgáltatás önkéntes igénybevételekor az ahhoz szükséges adatkezelés is önkéntes hozzájáruláson alapul, azonban törvényi vélelem szól ilyenkor a hozzájárulás automatikus megadásáról.

Véleményezés : Elfogadható

A gyűjtött adatok az adatkezelés céljai szempontjából megfelelőek és relevánsak-e, valamint a szükségesre korlátozódnak-e (adattakarékosság)?

Az előzőekben körülírt adatok az érintett egészségügyi ellátásához szükségesek, mert ezt szakmai szabályok, minőségbiztosítási szabályok írják elő. Más célú adatkezelés esetében is megfelelőek, relevánsak az adatok.

Véleményezés : Elfogadható

Pontosak-e az adatok, naprakész állapotban tartják-e azokat?

Az adatminőség megfelelő, mivel azokat pontosan és naprakészen tartja a Szolgáltató. Az érintett egészségi állapotában illetve személyes adataiban bekövetkezett változásokat átvezetik a nyilvántartáson amennyiben arról tudomást szerez az adatkezelő. Jogszabályi változások esetén szükség szerint módosítják az adatkezelési folyamatokat, a hozzájárulás visszavonása esetén is megfelelően reflektálnak.

Véleményezés : Elfogadható

Mi az adatmegőrzés időtartama?

Az egészségügyi adatokkal összekapcsolt személyazonosító adatok megőrzésének fent körülírt időtartamát az Eüak. törvényi szinten írja elő; egyéb adatoknál szintén törvényi szinten van rögzítve az adatmegőrzési idő, illetve a szolgáltató által megállapított, adatkezelési tájékoztatóban írtak szerint történik az adatok tárolása.

Véleményezés : Elfogadható

Az érintettek jogainak biztosítására szolgáló intézkedések

Milyen módon tájékoztatják az érintetteket az adatkezelésről?

Az információkat a pácienseknek szóló Adatkezelési tájékoztatóból szerezhetik meg az érintettek azzal, hogy további kérdések feltételére az adatkezelő által foglalkoztatott dolgozókhoz is van lehetőség az egyénre szabott informálódáshoz. A tájékoztatás tartalma megegyezik az Adatkezelési tájékoztatóban foglaltakkal. Ez elérhető a telephelyen papíralapon, de kérésre az érintettnek meg is küldik.

Véleményezés : Elfogadható

Amennyiben az adatkezelés hozzájáruláson alapul, milyen módon szerzik be az érintettek hozzájárulását?

A szolgáltató dolgozója felhívja az érintett figyelmét az adatkezelési tájékoztatóra, majd az érintett ráutaló magatartással adja önkéntes beleegyezését az adatkezelésbe. Marketing cél esetén írásban dokumentálják. Honlap látogatásakor pedig a böngésző érintett egyértelmű és határozott akaratnyilvánítását követően lehet csak a weblapot használni.

Véleményezés : Elfogadható

Milyen módon érvényesíthetik az érintettek a hozzáférési, illetve az adathordozhatósághoz való jogukat?

Adataihoz hozzáférhet: *Egészségügyi adataival az érintett, az ezt tároló adatbázissal pedig szolgáltatónk rendelkezik.* Szóbeli tájékoztatást kap, nyilvántartásunkba előzetes egyeztetést követően (kérésétől számított főszabálykénti 1 hónapon belül) betekinthet, arról írásbeli másolatot kérhet (egészségügyi adatra vonatkozó információkérés esetén természetesen törekszünk a legrövidebb határidő tartására).

Elektronikus ügyfélkapun illetve a kormányablakon keresztül bizonyos ellátási adataihoz szintén hozzáférhet az EESZT.

Betöltött 16 éves kortól más személyt két tanú igénybevételével írásban is meghatalmazhat akit tájékoztathatunk adatairól, aki betekinthet az érintettre vonatkozó nyilvántartásba illetve aki arról másolatot kérhet. Hacsak betöltött 16. éves kortól nem zárja ki: a kiskorúról a szülő/gyám is információt kap. (14-18 életév között, illetve cselekvőképességet korlátozó gondnokság alatt lévő személy saját adataiba önállóan is betekinthet.) Ha cselekvőképtelen (döntésképtelen) állapotba kerülne vagy bíróság cselekvőképességét kizáró gondnokság alá helyezné: a korábban meghatalmazott, ennek hiányában törvényes képviselője (gondnoka) illetve a törvény szerinti sorrendben jogosultak az érintettről tájékoztatást kapni/adataiba betekinteni meghatározott hozzátartozói (általában rokonsági fok szerint). Ha segítségre szorul az ún. támogatott döntéshozatal során az érintettet támogató személyt is informáljuk. A betegjogi képviselő az érintett hozzátartozói által meghatalmazva is eljárhat, ha ebben ő tartósan akadályozott.

Az érintett, vagy helyette arra meghatározott esetben jogosult személyek [ők lehetnek pl. a megbízottja, egyes hozzátartozói (nem automatikusan), örököse] személyazonosításukat követően jelezhetik kérésüket: ezek után a rá vonatkozó nálunk nyilvántartott adatairól szóban is tájékoztatást adunk, azokba előre egyeztetett időpontban és helyen

betekintést biztosítunk, illetve azokról kérésre elektronikus vagy papíralapú másolatot adunk ki. (Mivel *az eredeti papíralapú/fizikai egészségügyi dokumentumokat, képalkotó felvételeket jogszabály alapján ki nem adhatjuk*, hozott adathordozót pedig informatikai biztonsági és más betegekre vonatkozó titokvédelmi okokból nem fogadhatunk el: csak rajtunk keresztül tud másolatot kérni a rá vonatkozó adatokról. Annak azonban nincs akadálya, hogy a kizárólag rá vonatkozó papíralapú vagy képernyőn/optikailag megjeleníthető információkról saját eszközével fotó- vagy videó-dokumentációt készítsen – utóbbi esetben a rögzített felvétel felbontásától függően azonban a képi információ torzulhat.) *A másolat kiadása díjmentes.* Ugyanazon adatra (dokumentumra) vonatkozó ismételt, vagy több azonos példányban történő másolatkérés is díjmentes szolgáltatónknál.

Adathordozhatóság közvetetten az Elektronikus Egészségügyi Szolgáltatási Tér adatkezelésével valósul meg, illetve a páciens írásos beleegyezése esetén a Szolgáltatónál tárolt adatai másolatát - hiszen a kötelező megőrzési idő a Szolgáltatót ettől függetlenül köti - az érintett által megjelölt, erre technikailag alkalmas szolgáltatóhoz továbbítja (ezen adatkezelővel történt előzetes egyeztetést követően).

Véleményezés : Elfogadható

Hogyan gyakorolhatják az érintettek a helyesbítéshez és törléshez való jogukat?

Helyesbítés: *Ha az érintett kérése egészségügyi adatait érinti és azzal illetékes egészségügyi dolgozónk szakmailag nem ért egyet, kérését szakmai véleményével együtt jegyzi fel a dokumentációjában.* (Ha korábban bizonyos adatait jogszerűen máshová – pl. az őt szintén kezelő más egészségügyi szolgáltatóknak - továbbítottuk, a szükséges helyesbítésről értesítjük ezeket az adatkezelőket is, ám a szükséges illetve lehetséges módosításokról nekik kell gondoskodniuk.) *A javítást úgy kell elvégezni az egészségügyi dokumentációban, hogy az eredeti adat megállapítható legyen speciális törvényi előírás alapján. Nem egészségügyi ellátási célú adatkezelésnél ha a helyesbítés indokolt, korlátozás nélkül eleget teszünk neki.*

Törlés: Kérheti adatai teljes és végleges törlését illetve megsemmisítését is. (Ha korábban bizonyos adatait jogszerűen máshová továbbítottuk, a szükséges adattörlésekről értesítjük ezeket az adatkezelőket is, ám az ottani szükséges illetve lehetséges adattörlésekről nekik kell gondoskodni.)

Adatai törlését-megsemmisítését *egészségügyi adataival kapcsolatban csak korlátozottan kérheti:* Alapvetően akkor, ha a törvényben előírt kötelező nyilvántartási idő már letelt. Ezt megelőzően *az adattörlést is úgy kell elvégeznünk az egészségügyi dokumentációban, hogy az eredeti adat megállapítható legyen speciális törvényi előírás alapján. Az előírt megőrzési idő előtti részleges adattörlésre az adatvédelmi tisztviselővel (DPO) való egyeztetést követően van mód, illetve alternativaként az érintett hozzájárulása esetén pszeudonimizáltan tárolják tovább az adatokat.*

Véleményezés : Elfogadható

Hogyan gyakorolhatják az érintettek az adatkezelés korlátozásához, valamint tiltakozáshoz való jogukat?

Az érintettre vonatkozó **adatkezelés korlátozását**(adatzárolás) – hogy csak bizonyos műveleteket végezhessünk adatain - is kérheti. Ebben az esetben a korlátozás alatt adatait alapvetően csak tároljuk, s a korlátozás feloldásáról tájékoztatjuk. (Ha korábban bizonyos adatait jogszerűen máshová – pl. az őt szintén kezelő más egészségügyi szolgáltatóknak - továbbítottuk, a szükséges korlátozásról értesítjük ezeket az adatkezelőket is, ám az ottani szükséges illetve lehetséges korlátozásokról nekik szükséges gondoskodniuk.)

Egészségügyi adataira vonatkozóan csak bizonyos feltételekkel kérheti (ha pl. tiltakozik az adatkezelés ellen vagy adatai törlését kérte, illetve vita van a jogszerű adatkezelést érintően): az adatok felvételét végző egészségügyi dolgozó jogosultsága eldönteni, hogy milyen adatok kezelésére van szükség a megfelelő egészségügyi ellátásához.

Jogosult egészben vagy részben megtiltani adatai áramlását különösen az őt kezelő egészségügyi szolgáltatók; háziorvosa; az egészségbiztosító (NEAK) ún. betegéletút rendszere; az Elektronikus Egészségügyi Szolgáltatás Tér (EESZT) felé.

Tiltakozhat az érintett a rá vonatkozó adatok véleménye szerinti jogosulatlan kezelése miatt szolgáltatónknál. A hozzájárulás visszavonása nem érinti az addigi adatkezelés jogszerűségét.

Egészségügyi ellátásával összefüggésben az adatkezelési kötelezettséget széleskörű és szigorú jogszabályok írják elő – tiltakozása önkéntesen igénybe vett (jövőbeni) ellátásokra vonatkozóan lehetséges és az további ellátásának

gátját képezheti. Az adatkezelés, a dokumentáció vezetésének módját jogszabályi keretek között a szolgáltató határozza meg. Önálló tiltakozási jog illeti meg az érdekmérlegelésen alapuló adatkezelések esetén.

Véleményezés : Elfogadható

Az adatfeldolgozók kötelezettségeit egyértelműen rögzíti-e az adatfeldolgozási szerződés?

Az adatfeldolgozók egy részével írásbeli szerződést kötött az adatkezelő, melyben kötelezettségeik rögzítésre kerültek, dokumentált utasításokat kaptak.
Az átadott adatok tekintetében titoktartási kötelezettségük van, az adatkezelést bizalmas-biztonságos körülmények között dolgozzák fel.
Bizonyos adatfeldolgozók esetében a jogszabályi környezet nem teszi lehetővé írásbelinek minősülő szerződés megkötését (pl. NISZ Zrt., Magyar Posta Zrt.); más esetekben az ÁSZF-et használó adatfeldolgozó esetében nem volt ráhatása az adatkezelő szolgáltatónak a szerződés feltételeinek kidolgozására (pl. Országos Kórházi Főigazgatóság) mert a szerződő felek pozíciója illetve (a jogszabályi környezetre is figyelemmel) az adatfeldolgozó quasi monopól helyzete és a lényegében szerződéskötési kötelezettség fennállása az adatkezelő részéről ezt nem teszi lehetővé.
Magatartási kódexekhez nem tudott csatlakozni az adatkezelő azok hiánya miatt, és nincs tudomása arról hogy ilyenhez adatfeldolgozói csatlakoztak volna. Adatkezelő adatvédelmi tanusítást nem vett igénybe és szintén nincs tudomása erről adatfeldolgozói körében sem.
112-es segélyhívó számot üzemeltető szolgáltató NISZ ZRT. adatfeldolgozásának időtartama a segélyhívás ideje, hatásköre a legszükségesebb személyes adatok rögzítése alapvetően egészségügyi adatok nélkül, az érintett (sürgősségi) egészségi ellátása érdekében.

Az EESZT-t üzemeltető Országos Kórházi Főigazgatóság adatfeldolgozásának időtartama a korábban körülírt és jogszabályban meghatározott tárolási időtartamok, hatásköre jellemzően ezek rögzítésére, tárolására és módosításának, lekérdezhetőségének biztosítására terjed ki, mely adatfeldolgozás igénybevétele jogszabály alapján kötelező; az érintett egészségügyi ellátásának céljából.
Internetszolgáltatónk és e-mail szolgáltatóink az internetes kommunikáció lehetőségét biztosítják, az adatfeldolgozó által ÁSZF-ben meghatározott időtartamig őriz (személyes) adatokat ebből a célból, az adatkezelő törekszik hogy minimális egészségügyi adatot áramoltasson rajtuk keresztül, az érintett spontán kommunikációs kezdeményezése alapján ezt biztosítani teljesen értelemszerűen nem képes. Levélkiszolgálóról az esetlegesen spontán megadott illetve beérkezett egészségügyi adatokat haladéktalanul saját adattárolóra helyezéssel egyidejűleg eltávolítjuk.
Telekommunikációs (elsősorban hanghívás) szolgáltatónk adatkezelőnek minősülő betegellátókkal és az érintettekkel valamint más jogosult személyekkel szükséges kapcsolatot biztosítja, az adatfeldolgozók saját ÁSZF-nek megfelelő megőrzési időkkel (hangrögzítést az adatkezelő, adatfeldolgozók nem végeznek).
Medikai szoftverfejlesztő-karbantartó informatikai adatkezelőnk szoftverfejlesztés és karbantartás céljából kezelhet adatokat a legszükségesebb mértékben oly módon,

hogy lehetőség szerint tesztelésképpen szükség esetén csak kódolt illetve nem valós (illetve anonimizált) betegadatokhoz férhet hozzá az adatminimalizálás, szükségesség-arányosság tekintetében. Felhőalapú adattárolásra e-mail forgalom esetében a Google Inc. 1600 Amphitheatre Pkwy, Mountain View, CA 94043, Egyesült Államok; Yahoo Inc. Kalifornia Sunnyval, Egyesült Államok szolgáltatókat használjuk; míg a medikai szoftver tárhelyét az Árpa Solutions 9025 Győr, Töltésszer utca 3. biztosítja adatfeldolgozóként.
Számviteli szolgáltatóink csak a jogszabály előírta szabályos számviteli bizonylatokon szereplő legszükségesebb személyes adatok feldolgozását végezhetik. Postai szolgáltatónk saját adatkezelési és szerződési feltételekkel dolgozik.

Véleményezés : Elfogadható azzal, hogy javasolt a Google és a Yahoo mint levélkiszolgálók; illetve a felhőalapú medikai adattárolás használatának felhagyása.

Az Európai Unión kívülre történő adattovábbítás esetén megfelelő védelemben részesülnek-e a személyes adatok?

E-mail szolgáltatóink közül a Google Inc. korábban csatlakozott az azóta hatályát vesztett USA Privacy Shield-hez (EU-USA közti EU-konform garanciákat adó adatvédelmi pajzshoz). Webanalitikai adatforgalommal szintén előbbi érintett. Digitális konzultációhoz használt Skype (Microsoft Redmond Washington Egyesül Államok) és közösségi média felületünk (Facebook, Menlo Park, Kalifornia, Egyesül Államok) valósít meg harmadik állambeli adatforgalmat. Az érintetteket kiemelten tájékoztatjuk és felhívtuk figyelmüket az adatkezelés lehetséges kockázataira.

Véleményezés : Javasolt a Google, a Yahoo mint levélkiszolgálók használatának felhagyása. A Skype helyett dedikált egészségügyi adatátvitelt biztosító medikai rendszer javasolt amennyiben az az érintett felhasználók rendelkezésére is áll. A közösségi médiában szenzitív adatkezelés kerülése javasolt.

Kockázatok

Tervezett vagy meglévő intézkedések

Titkosítás

Az adatbázisok jelszóval védettek, meghatározott jelszóképzési rend szerint időközönként váltottak, képzésük megfelelő. Hitelesítési eljárásokat, jelszóhasználati szabályokat (minimum hossz, használható karakterek, érvényesség időtartama, téves jelszóhasználatok száma az adatkezelő betegellátó jogosultságának zárolása előtt) alkalmaznak.
A naponta végzett váltott adathordozón történő biztonsági mentések előbbiekhez hasonlóan védettek mely a szolgáltató képviselőjének birtokából nem kerülnek ki. EESZT-hez való hozzáférés PIN kód és személyi igazolvány (azaz tudás és birtoklás) alapú a jogosult adatkezelők körében.

Véleményezés : Elfogadható

Anonimizálás

Az egészségügyi ellátásban csak kivételesen van mód anonimizálásra vagy pszeudonimizált adatkezelésre; míg más cél esetén az nem értelmezhető. Anonim adatkezelést alkalmazhatunk pl. statisztikai célú adattovábbításokhoz; közérdekű adatigénylésekkor. Pszeudonimizálást bizonyos jogszabályi előírásokkor, illetve az érintett kifejezett kérésére végzünk ha annak technikai feltételei rendelkezésre állnak.

Véleményezés : Elfogadható

Nyomon követhetőség (naplózás)

Naplózásra legfeljebb a medikai rendszer használatával összefüggésben, a foglalkoztatottakat érintően kerülhet sor (akiket erről tájékoztattunk), de az Infotv. vonatkozó elektronikus naplót illető szabályának hatálya nem terjed ki a szolgáltatónál végzett adatkezelésekre.

Véleményezés : Elfogadható

Archiválás

Az egészségügyi dokumentációnak az Eüak.-ban előírt előbbi őrzési időket követően történő megőrzésére abban az esetben van lehetőség, ha

a) az az érintett egyéb, 30 évnél nem régebbi egészségügyi adatkezelésével kapcsolatba hozható, valamint

b)annak tudományos jelentősége van

ba) a betegség természete, vagy

bc) a kezelés jellege, vagy

bd) az érintett személy, vagy

be) általános tudomány- és kultúrtörténeti okok miatt. Ekkor azok archiválásra kerülnek.

Ha a dokumentációnak tudományos jelentősége van, akkor a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár (1013 Budapest, Apród u. 1–3.) részére kell azt átadni.

A ba)-be) pontjai szerinti minősítést az adatvédelmi tisztviselő kezdeményezésére a Szolgáltató ügyvezetője állapítja meg.

Papíralapon történő archiválásnál ügyelni kell arra, hogy savmentes – azaz lignint, savas adalékanyagot és színezéket nem tartalmazó –, nem fertőzött papíranyaggal érintkezhet csak a karton. Az elektronikus vagy papíralapú archiváláshoz adatfeldolgozót igénybe venni csak az adatvédelmi tisztviselő jóváhagyásával lehet.

Ellenőrizni szükséges az archivált adatállomány sértetlenségét-felhasználhatóságát.

Nem egészségügyi ellátási cél esetén jogszabályi előírások szerint történik az archiváció.

Véleményezés : Elfogadható

Papír alapú dokumentumok biztonsága

A papíralapú adatok nyomtatása-tárolása során bizalmas és fizikailag védett körülményeket biztosítunk különösen elemi kár, lopás, moral hazard, illetéktelen hozzáférés, elveszés ellen. A nyomtatott iratok előállítása során az azokon lévő adatok előírt megőrzési ideig történő olvashatósága technikailag biztosított. Megsemmisítés esetén olyan iratmegsemmisítőt vagy égetést használunk mely nem teszi lehetővé az adatok érintettel való újra összekapcsolását.

Véleményezés : Elfogadható

Adatminimalizálás

Az érintett biztonságos egészségügyi ellátásához szükséges valamennyi adat jogszerűen kezelhető; az adott ellátásban részt nem vevő betegellátó adatkezelők főszabályként nem férhetnek hozzá az adatokhoz; illetve a résztvevő ellátók az adott ellátással össze nem függő adatokhoz főszabályként szintén nem férhetnek hozzá - legfeljebb annyiban, olyan módon és ideig, mely annak megállapítását lehetővé teszi, hogy az információnak van-e köze aktuális ellátásához. Más cél esetén a legszükségesebb, illetve jogszabály által előírt adatokat kezeljük.

Véleményezés : Elfogadható

Üzembiztonság

Az operációs rendszerek, medikai szoftver és egyéb informatikai alkalmazások jogtiszta használata mellett, minden a gyártó által ajánlott frissítéssel rendelkeznek, azok szabályos installálása rendszeresen megtörténik.

Véleményezés : Elfogadható

Rosszindulatú software-ek kiszűrése

Minden munkaállomást mint végpontokat és a szervereket vírusvédelmi és egyéb kártékony kód elleni alkalmazás valamint tűzfal védi. Hasonlóan védekezünk a kibertámadások ellen.

Véleményezés : Elfogadható

A munkaállomások kezelése

Programjaik rendszeresen frissítésre kerülnek, a konfiguráció beállítások rendszeresen ellenőrzésre kerülnek. A kliensgépek fizikai megközelítése is jogosultság-ellenőrzéshez kötött mechanikai úton. Szükség szerint igénybe veszünk informatikai segítséget is a végpontok védelmére.

Véleményezés : Elfogadható

Biztonsági mentés

A biztonsági mentéseket meghatározott mentési rend szerint végzik (váltott, fizikailag is elkülönített adathordozókra; mentési média és a mentett adatállomány ellenőrzése, mentési média jelszavas védelme, biztonságos helyen tárolva azokat).

Véleményezés : Elfogadható

Karbantartás

A hardware-k fizikai karbantartása az informatikai szolgáltató adatfeldolgozón keresztül történik.

Véleményezés : Elfogadható

Adatfeldolgozók igénybevétele során alkalmazandó követelmények

Az adatfeldolgozók által kezelt személyes adatok megfelelő védelemmel rendelkeznek. Kizárólag olyan adatfeldolgozók vehetők igénybe, akik ehhez megfelelő garanciát biztosítanak (különösen a szakértelem, megbízhatóság és a megfelelő források terén). Az adatfeldolgozóknak dokumentálniuk kell a garanciák hatékonyságának biztosítását. Ezek a garanciák különösen a következők: titkosítás; szükség esetén az adatátvitel titkosítása és hálózati védelem, nyomon-követhetőség, jogosultságkezelés, hitelesítés. Az adatfeldolgozókkal szerződésekkel rendelkezünk.

Véleményezés : Elfogadható

Hálózatbiztonság

Az egészségügyi szolgáltatással összefüggően titkosított internetes csatornán keresztül folyik az EESZT-vel kötelező kommunikáció.
Egyéb elektronikus kommunikációra, így pl. levelezésre a nyilvános internetet használjuk tűzfalas és vírusirtó védelmében.

Véleményezés : Elfogadható

Fizikai hozzáférésvédelem

Az adatkezelés telephelyi fizikai védelménél a betegek kísérőik és hozzátartozóik csak a számukra kijelölt helyen mozoghatnak és tartózkodhatnak, felügyelet-kíséret nélkül nem maradnak. Az adatkezeléssel érintett helységeket zárjuk. Belépési jogosultsággal ezen kívül az ott dolgozók bírnak csak.

Véleményezés : Elfogadható

A nem emberi eredetű kockázatokkal szembeni védelem

Tűzvédelmi eszközöket használunk (pl. porral oltó, szünetmentes tápforrásokat alkalmazunk) a saját teleppel nem rendelkező eszközök esetében.

Véleményezés : Elfogadható

Szervezet

Az adatvédelemmel kapcsolatos feladat- és felelősségi körök az Adatvédelmi-adatkezelési-adatbiztonsági szabályzatban meghatározottak.

Véleményezés : Elfogadható

Szabályzatok

Az adatvédelmi célokat és szabályokat magában foglaló dokumentumok az Adatkezelési-adatvédelmi-adatbiztonsági szabályzat, az Adatkezelési tájékoztató.

Véleményezés : Elfogadható

Adatvédelmi kockázatok kezelése

Szolgáltatónk adatvédelmi kockázatelemzést és annak alapján hatásvizsgálatot végez a kockázatok azonosítása és kezelése, minimalizálása, menedzselhetősége érdekében.

Véleményezés : Elfogadható

Az adatvédelem beépítése a projektekbe

Minden újonnan kezdett adatkezelési műveletbe a jogszabályok és belső szabályzataink előírásait beépítjük.

Véleményezés : Elfogadható

A személyes adatokkal kapcsolatos jogsértések kezelése

Észlelésre és kezelésre kerülnek az érintettek személyiségi jogait és magánszféráját fenyegető incidensek törekedve ezek elkerülésére megfelelő technikai-szervezési intézkedésekkel a beépített-alapértelmezett adatvédelem alapján.

Véleményezés : Elfogadható

Humánerőforrás-menedzsment

Minden új adatkezelő foglalkoztatott adatvédelmi oktatáson vesz részt, melyet évente ismétlünk adatvédelmi tudatosságuk növelése érdekében. A szolgáltatóval foglalkoztatási jogviszonyát megszüntető dolgozó esetében hozzáférési jogosultságait kivétel nélkül haladéktalanul töröljük.

Véleményezés : Elfogadható

Az adatokhoz való jogosulatlan hozzáférés

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

Érintettek adatai nem célhoz kötötten, nem a jogosulti kör számára válnak elérhetővé, mely miatt sérül az orvosi titoktartáshoz fűződő joguk (egészségügyi ellátási célú adatkezelésnél), nyilvánosságra kerülés, adatintegritás, hitelesség, bizalmasság sérülése.

Mely fő fenyegető veszélyek idézhetik elő a kockázatot?

lopás-rablás, nem jogosult személyek adatkezelése, vírus-, kémprogram, károkozó kód, hacker támadás, rendszertúlterhelés, nem megfelelő titkosítás, adattovábbítási hiba, személyzeti moral hazard, adathordozók elvesztése, adatfeldolgozók körében felmerült adatvédelmi incidens, hálózati kockázat bekövetkezése

Melyek a kockázat forrásai?

szervezeten belüli és kívül emberi tényezők, illetve nem emberi-technikai tényezők

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Titkosítás, papír alapú dokumentumok biztonsága, rosszindulatú software-ek kiszűrése, a munkaállomások megfelelő kezelése, adatfeldolgozók igénybevétele során alkalmazandó követelmények, hálózatbiztonság, fizikai hozzáférésvédelem, a nem emberi eredetű kockázatokkal szembeni védelem, szabályzatok, humánerőforrás-menedzsment.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott - a tervezett intézkedésekkel a bekövetkezhető kockázatok következményeinek lehetséges súlyossága korlátozott értéken tartható.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott - a tervezett intézkedésekkel a bekövetkezhető kockázatok esélye korlátozott értéken tartható.

Véleményezés : Elfogadható

Az adatok véletlen vagy jogellenes megváltoztatása

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

adatintegritás, hitelesség, megbízhatóság sérülése, rendelkezésre állás-funkcionalitás csökkenése-elveszése

Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?

elírás, hibás adatfelvitel, véletlen törlés, nemkívánt módosítás, elemi kár, kezelői ügyetlenség, rongálás/rongálódás, vírus-, kémprogram, károkozó kód, hacker támadás, rendszertúlterhelés, programhiba, adathordozók sérülése, műszaki hibája, túlfeszültség, szoftverhiba

Melyek a kockázat forrásai?

szervezeten kívüli belüli és nem emberi tényezők

A megadott intézkedések közül melyek megfelelőek a kockázatok kezelésére?

Rosszindulatú software-ek kiszűrése, a munkaállomások kezelése, fizikai hozzáférésvédelem, a nem emberi eredetű kockázatokkal szembeni védelem, az adatvédelem beépítése a projektekbe.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott - a lehetséges kockázatok súlyossága korlátozott mértéken tartható az alkalmazott intézkedésekkel.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott – a lehetséges kockázatok valószínűsége korlátozott mértéken tartható az alkalmazott intézkedésekkel.

Véleményezés : Elfogadható

Adatvesztés

Milyen főbb következményekkel járna az érintettekre, ha a kockázat bekövetkezne?

integritás, funkcionalitás sérülése, hitelesség sérülése, rendelkezésre állás sérülése

Milyen fő fenyegető veszélyek idézhetik elő a kockázatot?

kezelői ügyetlenség, elemi kár, lopás-rablás, rongálás-rongálódás, illetéktelenek adatkezelése, vírus és egyéb kártékony kód, programhiba, áramszünet, személyzeti moralhazard, adathordozók sérülése, túlfeszültség, szoftverhiba, műszaki hiba, mobil adathordozó elvesztése

Melyek a kockázat forrásai?

szervezeten belüli és kívüli emberi tényezők és nem emberi tényezők

A megadott intézkedések közül melyek szolgálnak a kockázat kezelésére?

Archiválás, papír alapú dokumentumok biztonsága, üzembiztonság, rosszindulatú software-ek kiszűrése, a munkaállomások kezelése, biztonsági mentés, karbantartás, hálózatbiztonság, fizikai hozzáférésvédelem, a nem emberi eredetű kockázatokkal szembeni védelem, szabályzatok.

Hogyan becsüli meg a kockázat súlyosságát, különösen a lehetséges következményekre és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott - az intézkedésekkel a kockázatok súlyossága korlátozott szinten tartható.

Hogyan becsüli meg a kockázat valószínűségét, különösen a fenyegető veszélyekre, a kockázatforrásokra és a kockázatok kezelését célzó tervezett intézkedésekre való tekintettel?

Korlátozott - az intézkedésekkel a kockázatok esélye korlátozott szinten tartható.

Véleményezés : Elfogadható

Intézkedési terv

Áttekintés


Alapelvek
Célok
Jogalap
Megfelelő adatok
Pontosság
Adatmegőrzési határidő
Az érintettek tájékoztatása
A hozzájárulás megszerzése
Az érintettek tájékoztatása
A helyesbítéshez és a törléshez való jog
Az adatkezelés korlátozáshoz és a tiltakozáshoz való jog
Adatfeldolgozók igénybevétele
Adattovábbítások
Tervezett vagy meglévő intézkedések
Titkosítás
Anonimizálás
Nyomon követhetőség (naplózás)
Archiválás
Papír alapú dokumentumok biztonsága
Adatminimalizálás
Üzembiztonság
Rosszindulatú software-ek kiszűrése
A munkaállomások kezelése
Biztonsági mentés
Karbantartás
Adatfeldolgozók igénybevétele során alkalmazandó követelmények
Hálózatbiztonság
Fizikai hozzáférésvédelem
A nem emberi eredetű kockázatokkal szembeni védelem
Szervezet
Szabályzatok
Adatvédelmi kockázatok kezelése
Az adatvédelem beépítése a projektekbe
A személyes adatokkal kapocsolatos jogsértések kezelése
Humánerőforrás-menedzsment
Kockázatok
Adatokhoz való jogosulatlan hozzáférés
Az adatok véletlen vagy jogellenes megváltoztatása
Adatvesztés
Korrekciós Intézkedések
Elfogadható Intézkedések

Alapelvek

Nincs bejelentett szükséges intézkedési terv.

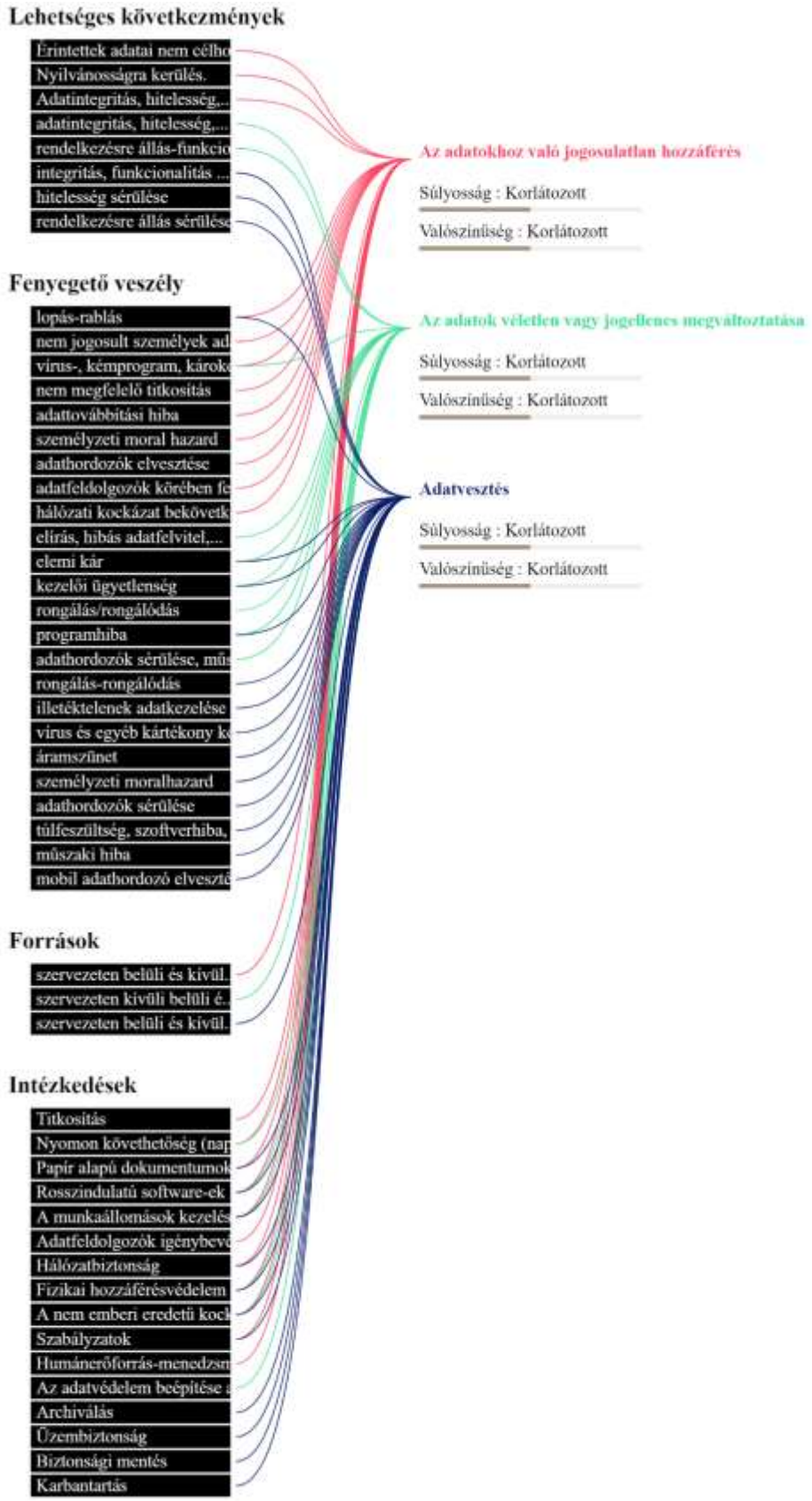
Meglévő vagy tervezett intézkedések

A Google, a Yahoo mint levélkiszolgáló; illetve a felhőalapú medikai adattárolás használatának felhagyása. A Skype helyett dedikált egészségügyi adatátvitelt biztosító medikai rendszer javasolt amennyiben az az érintett felhasználók rendelkezésére is áll. A közösségi médiában szenzitív adatkezelés kerülése javasolt.

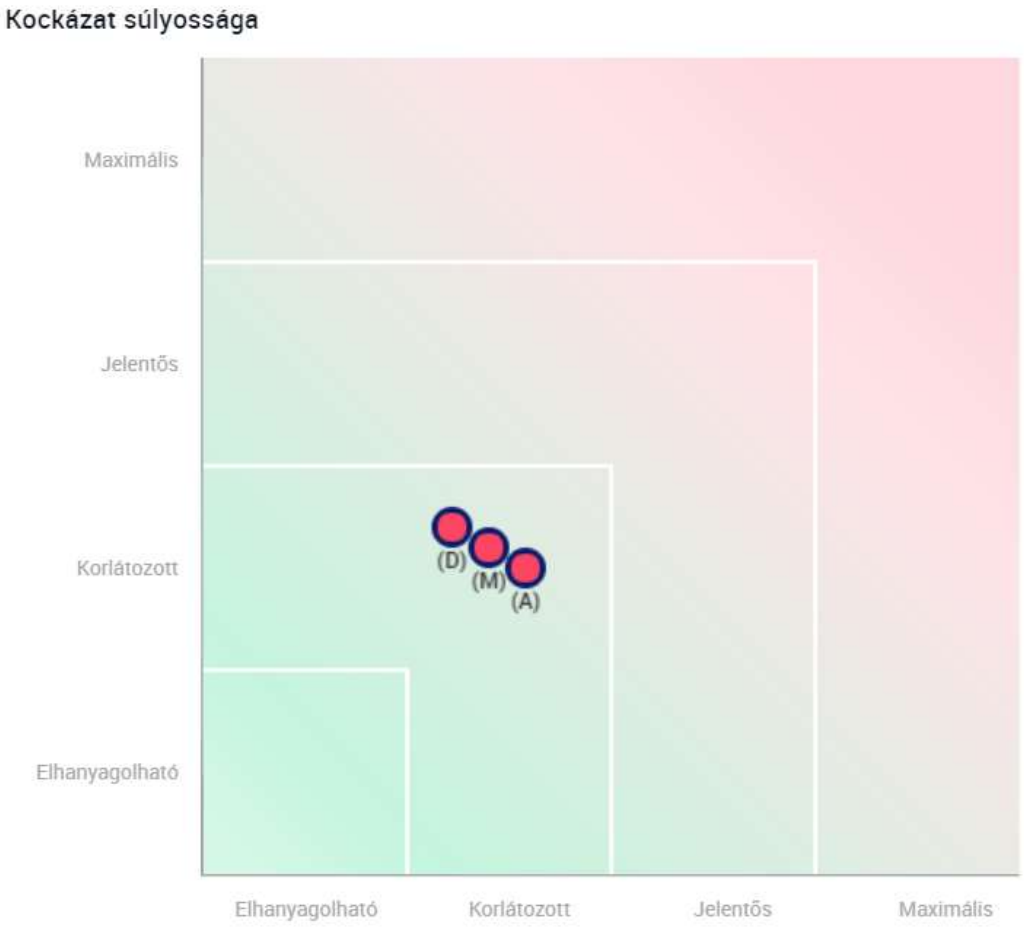
Kockázatok

Nincs bejelentett szükséges intézkedési terv.

A kockázatok áttekintése



A kockázatok feltérképezése



- Tervezett vagy meglévő intézkedések figyelembevételével
- A korrekciós intézkedéseket is tekintetbe véve
- (A)Adatokhoz való jogosulatlan hozzáférés
- (M)Az adatok véletlen vagy jogellenes megváltoztatása
- (D)Adatvesztés