Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelése és védelme

Jelen dokumentum csak akkor tekinthető érvényesnek, ha azonosító adatai megegyeznek az intranetes előírás-nyilvántartásban közöltekkel (intranet/Minőségirányítás).

készítés dátuma	változás tárgya	módosítás helye
2006-02-21	-	-
2010-07-01	Kiegészítve a betegdokumentáció kérés-kiadás rendjével, magán és hivatalos kérésre. Kiegészítve az adatbiztonságra vonatkozó meghatározásokkal.	Az 5. fejezetbe új 6. és 9. pont beillesztése. A következő helyek tartalma módosult még: 2.1. 2.3. 3.2. 3.3. 4.7. 6.3.3.
2012-09-26	Kiegészítés, pontosítás és aktualizálás. Törölve lett az "irányított betegellátás szervezését végző szervezetre" szöveg és az "ellátásszervező" szöveg	1.1., 1.4. pontok. 2.1. 2) kiegészítve az e. ponttal, a 3) kiegészítve v és w pontokkal. A 4.2. és 4.7. felsorolása kiegészítve egy új bekezdéssel. A 2.2.-ben és a 2.4.-ben törlés.
2013-01-11	Kiegészítés, törlés, pontosítás: adatkezelés céljairól, epidemiológiai vizsgálatok, elemzések adatkezeléseiről, eü. dokumentációról	2.1. alfejezet 3)u, x, y, z. 4.6. alfejezet 3. bekezdés. 4.7. új alfejezet. 5.4. végén új bekezdés. 5.5. a. 5.6. 1) és 2) végén. 2, 5 és 8. melléklet.
2015-11-20	Aktualizálás és kiegészítés, többek között az Info. tv. (2011. évi CXII. törvény) változásaival. Adatvédelmi incidens és a közérdekből nyilvános adat fogalma.	1.1. pont. 1.2. pont. 2.3. 3.2. 3.4. 4.2. 4.8. 5.1. 5.4. 5.6. 5.10. új alpont.
2018-05-25	Módosult az EU Általános Adatvédelmi Rendelete (Európai Tanács és Parlament 2016/679 rendelete, General Data Protection Regulation – GDPR).	A teljes tartalom és szerkezet változott.
2018-09-25	Változások a betegdokumentáció kérés-kiadás rendjében. A Betegdokumentáció kérő lap tartalma módosítva lett és tájékoztató készült a dokumentációkéréshez.	9. fejezet és az 5. melléklet. Új melléklet a 10. számú: Tájékoztató egészségügyi dokumentáció másolatot kérelmezők részére
2020-10-01	A betegdokumentáció kérés-kiadás kiegészült az EESZT lehetőségével és az első másolati példány térítésmentes kiadásáról szóló jogszabályi leírással.	9. fejezet teljes tartalma és az 5. mellékletben a 3. oldal harmadik bekezdése
2022-03-28	Új követelményeknek megfelelően aktualizálva a teljes szabályzat. Egy új melléklettel kiegészítve: 11. sz. Incidenskezelési űrlap	Teljes tartalom.

készítette/módosította és ellenőrizte
Izsák Tünde osztályvezető, adatvédelmi tisztviselő

jóváhagyta + dátum 2022 ÁPR 22.
Dr. Németh Csaba főigazgató

Tartalom

1 Szabályzat célja, hatálya, alapelvek

Bevezető rendelkezések

A Tolna megyei Balassa János Kórház (a továbbiakban: intézmény), jelen szabályzatban határozza meg a természetes személyek személyes adatainak kezelésével és védelmével kapcsolatos irányelveket, valamint az adatvédelmi tevékenység ellátásában résztvevő szervezeti egységek feladatait és együttműködésük kereteit.

A szabályzat hatálya alá tartozó személyek kötelesek a tevékenységük során az intézmény kezelésében lévő személyes adatokat a mindenkori jogszabályi rendelkezéseknek megfelelően kezelni. Különösen *a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló 2016/679/EU európai parlamenti és tanácsi rendeletre* vonatkozóan (a továbbiakban: GDPR). Továbbá *az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény* (a továbbiakban: Infotv.) rendelkezéseinek és az intézményre irányadó egyéb jogszabályok rendelkezéseinek figyelembevételével.

Az intézmény a személyes adatok kezelésével járó tevékenysége során érvényre juttatja a GDPR alapelveit, így különösen:

a) jogszerűség, tisztességes eljárás és átláthatóság elve
b) célhoz kötöttség elve
c) adattakarékosság elve
d) pontosság elve
e) korlátozott tárolhatóság elve
f) integritás és bizalmas jelleg
g) beépített adatvédelem elve
h) alapértelmezett adatvédelem elve

A szabályzat célja

Jelen szabályzat célja, hogy

a) biztosítsa az intézmény tevékenysége során a személyes adatok védelméhez fűződő jog érvényesülését, továbbá, hogy az intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes és különleges adatok kezelése során irányadó adatvédelmi szabályokat.
b) meghatározza azokat a szervezési és technikai intézkedéseket, amelyek kialakításával az intézmény gondoskodik a személyes adatok kezelése során a személyes adatok biztonságáról. Erre tekintettel a szabályzat az intézmény által folytatott adatkezelési tevékenységek során figyelembe veendő és követendő elveket, rendelkezéseket tartalmaz. Ezeket az előírásokat minden egyes adatkezelési folyamat, tevékenység során, annak teljes tartama alatt figyelembe kell venni.
c) meghatározza az intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét, valamint biztosítsa a személyes adatok védelme elveinek és az adatbiztonság követelményeinek érvényesülését.

Szabályzat személyi hatálya

Jelen szabályzat személyi hatálya kiterjed az intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyek (a munkavégzésre irányuló jogviszony jellegétől függetlenül), továbbá azon természetes személyekre (a továbbiakban: érintett), akik személyes adatait a jelen szabályzat hatálya alá tartozó adatkezelések tartalmazzák, továbbá azon érintettekre, akik jogait vagy jogos érdekeit az adatkezelés érinti. Az intézmény megbízásából személyes adatok kezelését vagy feldolgozását végzők esetén az erre a jogviszonyra az intézmény által kötött szerződésben a GDPR 28. cikkének megfelelően rendelkezni kell arról, hogy az intézmény által megbízott adatfeldolgozó a feladata ellátása során hogyan juttatja érvényre jelen szabályzat rendelkezéseit.

Szabályzat tárgyi hatálya

A szabályzat tárgyi hatálya az intézmény mindazon adatkezeléseire kiterjed – függetlenül attól, hogy az adatkezelés elektronikusan vagy papíralapon történik –, amelyek

a) az egészségügyi ellátás nyújtásához kapcsolódó adatkezelést valósítanak meg a szabályzat 2. pontjában felsorolt jogszabályok és belső szabályzatok szerint;
b) az egészségügyi ellátáson kívüli ügyfélkapcsolati jellegű adatkezelést valósítanak meg (az Intézménnyel kapcsolatba lépni szándékozó, kapcsolatban álló vagy kapcsolatban állt személyek, beleértve ezek meghatalmazottait, képviselőit is);
c) foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg [az Intézménnyel közalkalmazotti jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek);
d) az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

Dokumentációs kötelezettség

Az intézmény felelős a személyes adatok kezelésére vonatkozó alapelvek [GDPR 5. cikk (1) bek.] betartásáért. Az intézménynek képesnek kell lennie a személyes adatok kezelésére vonatkozó alapelvek betartásának igazolására [GDPR 5. cikk (2) bek.]. A megfelelőség igazolása különösen az adatkezeléshez kapcsolódó döntéseket megalapozó körülmények és a döntések (pl. az adatkezelés feltételeit meghatározó döntéselőkészítő iratok), az érintetteknek szóló adatkezelési tájékoztatók, az érintettől származó nyilatkozatok (pl. hozzájáruló nyilatkozatok, az adatkezelési tájékoztató megismerését igazoló dokumentumok), továbbá a személyes adatokat tartalmazó (elektronikus vagy papír alapú) dokumentumok szervezeten belüli vagy azon kívüli mozgásának megfelelő dokumentálásával történik. Az intézmény – a GDPR 30. cikkének megfelelően – nyilvántartást vezet az általa végzett adatkezelésekről.
A megfelelőség igazolása adatvédelmi incidens esetén különösen az incidenssel érintettek körének, az incidenssel érintett személyes adatok körének, az incidens kezelése során tett intézkedéseket megalapozó körülmények és a döntések dokumentálásával történik. Az intézmény – a GDPR 33. cikkének megfelelően – nyilvántartást vezet a bekövetkezett incidensekkel kapcsolatos tényekről és intézkedésekről.

2 A szabályzathoz kapcsolódó jogszabályok, belső szabályzatok

GDPR	Az Európai Parlament és a Tanács (EU) 2016/679 Rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [az Infotv-nek a GDPR hatálya alá eső adatkezelésekre alkalmazandó szabályai – lsd. Infotv. 2. § (2) és (4) bekezdése]
Eüak.	1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről, és a végrehajtására kiadott jogszabályok
Eütv.	1997. évi CLIV. törvény az egészségügyről, és a végrehajtására kiadott jogszabályok
Ebtv.	1997. évi LXXXIII. törvény kötelező egészségbiztosítás ellátásairól, és a végrehajtására kiadott jogszabályok
Eszjtv	528/2020. (XI. 28.) Korm. rendelet az egészségügyi szolgálati jogviszonyról szóló 2020. évi C. törvény végrehajtásáról
Mt.	2012. évi I. törvény a Munka Törvénykönyvéről
IG0904	a Tolna Megyei Balassa János Kórház Közérdekű adatok közzétételéről szóló Igazgatói Utasítása
	a Tolna Megyei Balassa János Kórház informatikai biztonsági szabályzata és az informatikai szabályzata
IG2133	a Tolna Megyei Balassa János Kórház Informatikai hibakezelési (incidenskezelési) eljárás rendje
IG0815	a Tolna Megyei Balassa János Kórház Iratkezelési szabályzata
IG0601	Személyes, egészségügyi, gazdasági, pénzügyi, munkaügyi adatokat tartalmazó, papír alapú dokumentációk selejtezési szabályzata

3 Fogalmak

Jelen szabályzat alkalmazása során a GDPR 4. cikkében és az Infotv. 3. § 1, 2, 3., 4., 6.,7, 8, 12., 13.,14, 15, 16., 21., 23-24. pontjában meghatározott fogalmakon kívül az alábbi fogalmakat kell alkalmazni:

Orvosi titok: az egészségügyi ellátás során az adatkezelő tudomására jutott egészségügyi és személyes adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat.

Egészségügyi dokumentáció: az egészségügyi ellátás során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától.

Közeli hozzátartozó: a házastárs, az egyenes ágbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs.

Közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől. Így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat.

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli. A közfeladatot ellátó szerv feladat- és hatáskörében eljáró személy neve, feladatköre, munkaköre, vezetői megbízása, a közfeladat ellátásával összefüggő egyéb személyes adata, valamint azok a személyes adatai, amelyek megismerhetőségét törvény előírja.

Különleges adat: faji eredetre, nemzeti, nemzetiségi és etnikai hovatartozásra, pártállásra, vallásra, egészségi állapotra, kóros szenvedélyre, szexuális életre vonatkozó személyes adatok, valamint a bűnügyi személyes adat.

Adatvédelmi incidens jellege: személyes adatok megsemmisülése, személyes adatok jogosulatlan megsemmisítése, személyes adatok rendelkezésre állásának sérülése, személyes adatok integritásának sérülése, személyes adatok elvesztése, személyes adatok jogosulatlan megváltoztatása, személyes adatok jogosulatlan közlése vagy jogellenes továbbítása, személyes adatokhoz történő jogosulatlan hozzáférés, személyes adatok bizalmasságának sérülése (pl. titoksértés) stb.

Az érintett hozzájárulása: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat, vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adta az őt érintő személyes adatok kezeléséhez.

Adatvédelmi tisztviselő: az intézmény szervezetében működő, a GDPR 39. cikkében meghatározott feladatokat az intézmény jelen szabályzatában foglaltak szerint ellátó, az intézménnyel foglalkoztatási jogviszonyban álló természetes személy,

Érdekmérlegelési teszt: jogos érdeken alapuló adatkezelés tervezett bevezetése esetén annak írásbeli dokumentálása, hogy az adatkezelő számba vette az adatkezelést megalapozó érdekeket, érveket, valamint az érintettek személyes adatok védelméhez fűződő – a tervezett adatkezelés ellen ható – jogait és érdekeit, és ezen érdekek és érvek összevetésével megalapozza az adatkezelés bevezetését vagy a bevezetés elutasítását,

Adatvédelmi felügyeleti hatóság: a Nemzeti Adatvédelmi és Információszabadság Hatóság (a továbbiakban: Hatóság),

Adatvédelmi hatásvizsgálat: olyan vizsgálat, amelyet az adatkezelésért felelős szervezeti egység kijelölt munkavállalója (adatkezelési megbízott) köteles elvégezni, amennyiben valamely tervezett adatkezelés – figyelemmel annak jellegére, hatókörére, körülményeire és céljaira, ideértve különösen az új technológiák alkalmazásának esetét – valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, és amelynek célja annak megállapítása, hogy a tervezett adatkezelés a személyes adatok védelmét hogyan érinti. Az adatvédelmi hatásvizsgálat egy olyan eljárás, amelynek során az adatkezelő a

tervezett adatkezelési műveletet vagy műveleteket áttekinti, megvizsgálja az adatkezelés érintettekre gyakorolt esetleges hatását, felméri annak kockázatait, a kockázatok kezelésének módját, és mindezt megfelelően dokumentálja,

4 Adatvédelmi tevékenységben résztvevők

A főigazgató felelős azért, hogy az intézmény – mint adatkezelő, illetve adatfeldolgozó – működése az adatvédelmi szabályoknak megfeleljen. Ennek érdekében:

a) gondoskodik az adatvédelmi tevékenység irányításában és ellátásában résztvevő szervezeti egységek kijelöléséről, feladataik, az adatvédelmi tárgyú ügyekkel kapcsolatos döntési jogkörök meghatározásáról, az egyes adatkezelési döntési szintek kialakításáról;
b) biztosítja az adatvédelmi tevékenység irányításához és ellátásához, valamint az érintett jogai gyakorlásához szükséges személyi és tárgyi feltételeket;
c) felelős az adat- és titokvédelmi, valamint biztonsági és informatikai biztonsági szabályzatok kiadásáért és betartatásáért;
d) gondoskodik arról, hogy az adatvédelmi tevékenység során esetleg előforduló, feltárt hiányosságok megszűntetéséről, szükség szerint a felelősségre vonásról;
e) kinevezi az intézmény adatvédelmi tisztviselőjét, és az adatvédelmi tisztviselő nevét és elérhetőségét bejelenti a Nemzeti Adatvédelmi és Információszabadság Hatóságnak;
f) munkajogi értelemben vett közvetlen felettese az adatvédelmi tisztviselőnek.

A főigazgató vagy az általa kijelölt személy

a) adatvédelmi incidens esetén közreműködik az érintettek tájékoztatásának módjáról és a tájékoztatás tartalmáról való döntés előkészítésében,
b) adatvédelmi incidens esetén – az adatvédelmi tisztviselő közreműködésével – szükség esetén sajtóközleményt bocsát ki és kizárólagos kapcsolatot tart a sajtó képviselőivel.

A Főigazgató

a) biztosítja az intézmény adatvédelmi tisztviselője feladatainak ellátásához szükséges személyi és tárgyi feltételeket;
b) az adatvédelmi tisztviselő szükség szerinti közreműködésével ellátja az érintetti jogok gyakorlásával kapcsolatos beadványok megválaszolását, a GDPR szerinti jogaik gyakorlását érintő panaszok kivételével.

Az adatvédelmi tisztviselő

a) Az adatvédelmi tisztviselőt a főigazgató nevezi ki az olyan, az Intézménnyel foglalkoztatási jogviszonyban álló természetes személyek közül, aki ismeri az intézmény működését, feladatait, és megfelelő végzettséggel rendelkezik. Az adatvédelmi tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről;
b) Az adatvédelmi tisztviselőt tisztsége fennállása alatt és annak megszűnését követően titoktartási kötelezettség terheli a tevékenysége során tudomására jutott, közérdekű vagy közérdekből nem nyilvános adatnak nem minősülő információk kapcsán;
c) Az adatvédelmi tisztviselő az adatvédelmi tisztviselői feladatokon kívül a főigazgató döntése alapján más munkakörhöz kötődő feladatokat is elláthat, amennyiben azok nem eredményeznek összeférhetetlenséget;

d) Az adatvédelmi tisztviselő nevét és elérhetőségeit az intézmény honlapján, székhelyén, telephelyén a nyilvánosság részére mindenkor elérhetővé kell tenni. Az intézmény továbbá közli az adatvédelmi tisztviselő nevét és elérhetőségét a Nemzeti Adatvédelmi és Információszabadság Hatósággal;
e) Az adatvédelmi tisztviselő véleményét – a jelen szabályzat rendelkezései szerint – ki kell kérni az adatkezelést érintő döntések, szerződések és belső szabályzatok tervezetéről;
f) Az intézmény elősegíti az adatvédelmi tisztviselő megfelelő szakmai feladatellátását, ennek érdekében az intézmény biztosítja különösen az adatvédelmi tisztviselő feladatai végrehajtásához, a személyes adatokhoz és az adatkezelési műveletekhez való hozzáférést, valamint a szakértői szintű ismereteinek fenntartásaihoz szükséges forrás biztosítását.

Az adatvédelmi tisztviselő feladatai:

a) közreműködik, illetve segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában;
b) ellenőrzi a GDPR, az Infotv. és az adatkezelésre vonatkozó más jogszabályok, valamint a jelen szabályzat, továbbá az intézmény egyéb belső szabályzatai rendelkezéseinek a megtartását, belső adatvédelmi ellenőrzési eljárást folytat le;
c) kivizsgálja – az érintett szakterületek és a Jogi osztály bevonásával – a neki címzett panaszokat, jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelőt vagy az adatfeldolgozót;
d) elkészíti az adatvédelmi és adatbiztonsági szabályzatot az informatikai szakterülettel együttműködve;
e) gondoskodik az adatvédelmi ismeretek oktatásáról [elsősorban az intraneten közzétett segédanyagok útján];
f) személyes adatok kezelésére vonatkozó előírásokról tájékoztatást nyújt, tanácsot ad;
g) személyes adatot is kezelő új informatikai rendszer belső fejlesztéssel történő bevezetése során közreműködik az adatvédelmi hatásvizsgálatot lefolytatásában;
h) az adatvédelmi incidenskezeléssel kapcsolatban ellátja a jelen szabályzat szerinti feladatokat;
i) vezeti az Adatkezelési Nyilvántartást;
j) éves összefoglaló jelentést készít a főigazgatónak;
k) kapcsolatot tart és – Jogi osztály és az ügy természetéből adódóan esetenként egyéb szakterület munkatársainak bevonásával – együttműködik a Hatósággal;

Tolna Megyei Balassa János Kórház adatvédelmi tisztviselője: Izsák Tünde
Elérhetőségei:
Telefonszám: 0674/501-533
email: adatvedelmitisztviselo@tmkorhaz.hu

Az informatikai szakterület szervezeti egységei

Az intézmény szervezeti és működési szabályzatában, valamint az intézmény informatikai biztonsági szabályzatában meghatározott feladatkörükben:

a) ellátják az informatikai biztonsági biztonsággal kapcsolatos feladatokat a folyamatos üzemeltetési feladatok kivételével, különösen az intézmény informatikai biztonsági szabályzatában meghatározott feladatokat;
b) ellátják az informatikai fejlesztéseknél és beszerzéseknél a beépített adatvédelem kontrolljai meglétének biztosításával, az adatminőség biztosításával, az informatikai

biztonság kockázatarányos szintjét biztosító jogosultsági és naplózási rendszer kialakításának megfelelőségével, a biztonságos szoftverfejlesztés alapelveinek érvényesítésével kapcsolatos feladatokat,

c) az informatikai rendszerek üzemeltetése területén ellátják a személyes adatok kezelésével kapcsolatos technikai védelem megvalósítását, ellátják – az intézmény informatikai biztonsági szabályzatában meghatározott – hatáskörükbe tartozó információbiztonsági feladatokat, valamint rendelkezésre állási kontrollok biztosítását, a tárolt és továbbított személyes adatok bizalmasságának védelmét, az incidens felderítési és kezelési tevékenység támogatását,

d) az érintett szervezeti egységek vezetőivel együttműködve gondoskodnak az információbiztonsági előírások, szabályzatok megismertetéséről, rendszeres oktatásáról.

A Jogi osztály:

a) szakmai támogatást nyújt az adatkezeléssel összefüggő, nem adatvédelmi jogszabályok értelmezésében,

b) az intézmény a belső szabályozók előkészítésére és kiadására vonatkozó szabályok szerint biztosítja, hogy az adatvédelmi tisztviselő véleményét kikérjék az intézmény adatvédelmi tárgyú vagy adatvédelmi vonatkozású belső szabályzatainak előkészítése során,

c) biztosítja az intézmény képviseletét az érintett által az intézmény ellen az érintett adatvédelmi jogainak megsértése miatt indított, illetve az intézmény által a Nemzeti Adatvédelmi és Információszabadság Hatóság határozatainak felülvizsgálata iránt indított perekben, illetve egyéb eljárásokban.

5 Az érdekmérlegelési teszt és a hatásvizsgálat módszertana

Az érdekmérlegelési teszt elvégzésének módszertana:

Amennyiben az intézmény valamely adatkezelésének az intézmény vagy harmadik személy jogos érdeke a jogalapja [GDPR 6. cikk (1) bekezdés f) pont], érdekmérlegelési tesztet kell elvégezni és azt dokumentálni. Jogos érdek az a törvényes, kellően pontosan megfogalmazott, valós és fennálló, illetve elérhető előny, amelyet az adatkezelő származtat – vagy a harmadik személy származtathat – az adatkezelésből.
Az érdekmérlegelési tesztet az intézmény adatvédelmi tisztviselője végzi el. Az érdekmérlegelési tesztet írásban kell elvégezni. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését követően kezdhető meg.
Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

Az érdekmérlegelési teszt részei:

a) a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,

b) az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),

c) az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),

d) az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,

e) az adatkezelés biztosítékainak leírása,
f) az érdekmérlegelési teszt eredménye.

Az adatvédelmi hatásvizsgálat elvégzésének módszertana

Ha az adatkezelés valamely, különösen új technológiákat alkalmazó típusa valószínűsíthetően magas kockázattal jár a természetes személyek jogaira nézve az adatkezelést megelőzően hatásvizsgálatot kell végezni. Olyan egymással hasonló típusú adatkezelési műveletek, amelyek egymáshoz hasonló kockázatokat jelentenek, egyetlen adatvédelmi hatásvizsgálat (továbbiakban hatásvizsgálat) keretei között is értékelhetők.

A hatásvizsgálat elvégzésének szükségességéről a tervezett adatkezelésért felelős szervezeti egység adatkezelési megbízottja szükség esetén kikéri az adatvédelmi tisztviselő véleményét. Az adatvédelmi hatásvizsgálatot az adatvédelmi tisztviselő készíti, a hatásvizsgálat megállapításait írásban kell rögzíteni. Ha az adatvédelmi tisztviselő úgy ítéli meg, hogy az adatkezelés nem jár magas kockázattal, úgy meg kell indokolnia és dokumentumokkal igazolnia a mellőzés okait. A bevezetendő adatkezelés kizárólag a hatásvizsgálat elvégzését követően kezdhető meg.

Adatvédelmi hatásvizsgálatot a GDPR 35. cikk (3) bekezdésében, illetve a Nemzeti Adatvédelmi és Információszabadság Hatóság által közzétett jegyzékben (https://www.naih.hu/files/GDPR_35_4_lista_HU_mod.pdf) szereplő adatkezelések, adatkezelési műveletek esetén kell végezni.

A fenti eseteken túl minden olyan bevezetésre kerülő – különösen az új technológiákat alkalmazó – adatkezelés esetén is hatásvizsgálatot kell végezni, mely adatkezelés az ügyfélre tekintettel jelentős joghatással bír/az ügyfelet jelentős mértékben érinti.

A hatásvizsgálat módszertanát minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani. Egy lehetséges módszertant alkalmazó szoftver található a Nemzeti Adatvédelmi és Információszabadság Hatóság honlapján (https://naih.hu/adatvedelmi-hatasvizsgalati-szoftver.html).

A hatásvizsgálat megállapításait az adatkezelési tevékenységbe vissza kell csatolni és ennek megfelelően kell kialakítani az adatkezelést.

A hatásvizsgálatot legalább háromévente felül kell vizsgálni, szükség esetén újra el kell végezni.

6 Az adatbiztonsági intézkedések (technikai és szervezési intézkedések) meghatározása és végrehajtása

Az adatkezelő köteles gondoskodni az adatok biztonságáról, köteles megtenni azokat a technikai és szervezési intézkedéseket, és kialakítani azokat az eljárási szabályokat, amelyek a törvény, valamint az egyéb adat-és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés ellen. A személyes adatok technikai védelmének biztosítása érdekében külön védelmi intézkedéseket kell tennie az adatkezelőnek, az adatfeldolgozónak, az informatikai eszköz üzemeltetőjének, ha a személyes adatok továbbítása hálózaton vagy egyéb informatikai eszköz útján történik.

Az adatbiztonsági szabályok kialakítása során különös gondot kell fordítani a beépített és az alapértelmezett adatvédelem elveinek (GDPR 25. cikk) betartására, valamint arra, hogy az

intézmény által alkalmazott adatbiztonsági intézkedések megfeleljenek a GDPR 32. cikkében írt követelményeknek.

Az intézmény működése során betartandó adatbiztonsági szabályokat (GDPR 32. cikk) külön szabályzatok tartalmazzák, így különösen a mindenkor hatályos

a) informatikai biztonsági szabályzat,
b) katasztrófa terv (informatikai szabályzat).

Az adatbiztonsági szabályok tervezetének kialakításába – a véleményezésre vonatkozó egyéb szabályokat nem érintve – az adatvédelmi tisztviselőt be kell vonni.

7 A közös adatkezelői és az adatfeldolgozói szerződések megkötésére vonatkozó szabályok

Közös adatkezelés

Közös adatkezelésnek minősül, ha az adatkezelés céljait és eszközeit az intézmény egy vagy több másik adatkezelővel közösen határozza meg (GDPR 26. cikk). Amennyiben döntés születik a közös adatkezelés bevezetéséről, az adatvédelmi jogi megfelelőség biztosítása tekintetében az adatvédelmi tisztviselő és egyéb jogszabályi követelményeknek való megfelelés szerződéses biztosítása tekintetében a Jogi osztály közreműködésével, továbbá az informatikai szakterület véleményének kikérésével előkészíti a közös adatkezelésről szóló megállapodás tervezetét és azt felterjeszti a szerződés megkötésére jogosult személynek.

Adatfeldolgozói megállapodás

Adatfeldolgozó igénybevétele esetén az adatfeldolgozóval kötendő szerződésnek tartalmaznia kell a GDPR 28. cikk (1)-(4) bekezdésében foglalt tartalmi elemeket

Az adatbiztonsági intézkedések megfelelőségének megítélése az informatikai szakterület hatáskörébe tartozik

Amennyiben döntés születik az adatfeldolgozó igénybevételéről, az adatvédelmi tisztviselő az informatikai szakterület véleményének kikérésével, szükség esetén a Jogi osztály közreműködésével előkészíti az adatfeldolgozóval kötendő szerződés tervezetét és azt felterjeszti a szerződés megkötésére

8 Általános adatkezelési szabályok

Az adatvédelmi alapelvek iránymutatásként szolgálnak, annak érdekében, hogy az intézményben történő személyes, és a hozzájuk kapcsolódó egészségügyi adatok kezelése maradéktalanul megfeleljen a jogszabályi előírásoknak.

Az adatvédelmi szabályzat elvei megkülönböztetés nélkül érvényesek valamennyi adatkezelésre, függetlenül attól, hogy az adatkezelés papír, vagy elektronikus módon történik.

Jelen szabályzat az adatok informatikai területen történő védelmét az informatikai biztonsági szabályzatban meghatározottakkal összhangban valósítja meg.

A jogellenes adatkezelés mindenféle eredmény, következmény nélkül kimeríti az adatkezelési incidens fogalmát.

Az adatkezeléssel megbízott személy kezeli és megőrzi a munkaköréhez, feladatellátáshoz szükséges adatokat. Gondoskodik arról, hogy az általa vezetett nyilvántartások adataihoz

illetéktelen személy ne férjen hozzá, ügyel a nyilvántartások biztonságos kezelésére és tárolására. Betartja a személyes és egészségügyi adatok kezelésére vonatkozó jogszabályi rendelkezéseket, igazgatói utasításokat, előírásokat.

Adatkezelés alapelvei:

a) Jogszerűség, tisztességes adatkezelés, az érintett személy részére átlátható adatkezelést kell biztosítani
b) Célhoz kötöttség – személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése céljából kezelhető
c) Adattakarékosság, Korlátozott tárolhatóság - személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető
d) Pontosság - Az adatkezelés során biztosítani kell az adatok pontosságát, teljességét és - ha az adatkezelés céljára tekintettel szükséges - naprakészségét, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani,
e) az adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”),
f) Elszámoltathatóság- az adatkezelő felelős az adatkezelés szabályainak megfelelősségéről, továbbá képesnek kell lennie a megfelelés igazolására.

Adatkezelés jogszerűsége az EU Tanács 2016/679 Rendelet 6. cikke értelmében:

a) az érintett hozzájárulását adta személyes adatainak egy vagy több konkrét célból történő kezeléséhez;
b) az adatkezelés olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél, vagy az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges;
c) az adatkezelés az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez szükséges;
d) az adatkezelés az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges;
e) az adatkezelés közérdekű vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához szükséges;
f) az adatkezelés az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges,

Az egészségügyi és személyazonosító adat kezelésének célja elsődlegesen:

a) Az egészség megőrzésének, javításának, fenntartásának előmozdítása,
b) A betegellátó eredményes gyógykezelési tevékenységének elősegítése, ideértve a szakfelügyeleti tevékenységet is,
c) Az érintett egészségi állapotának nyomon követése,
d) A népegészségügyi, közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele,
e) A betegjogok érvényesülése

A fentieken túl:

a) egészségügyi szakember-képzés,
b) orvos-szakmai és epidemiológiai vizsgálat, elemzés, az egészségügyi ellátás tervezése, szervezése, költségek tervezése,
c) statisztikai vizsgálat,

d) hatásvizsgálati célú anonimizálás és tudományos kutatás,
e) az egészségügyi adatot kezelő szerv vagy személy hatósági vagy törvényességi ellenőrzését, szakmai vagy törvényességi felügyeletét végző szervezetek munkájának elősegítése, ha az ellenőrzés célja más módon nem érhető el, valamint az egészségügyi ellátásokat finanszírozó szervezetek feladatainak ellátása,
f) a társadalombiztosítási, illetve szociális ellátások megállapítása, amennyiben az az egészségi állapot alapján történik, valamint a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról szóló törvény szerinti rendvédelmi egészségkárosodási ellátás megállapítása, továbbá a Nemzeti Adó- és Vámhivatal személyi állományának jogállásáról szóló törvény szerinti egészségkárosodási ellátás megállapítása,
g) az egészségügyi ellátásokra jogosultak részére a kötelező egészségbiztosítás terhére igénybe vehető szolgáltatások rendelésének és nyújtásának, valamint a gazdaságos gyógyszer-, gyógyászati segédeszköz- és gyógyászati ellátás rendelési szabályai betartásának a vizsgálata, továbbá a külön jogszabály szerinti szerződés alapján a jogosultak részére nyújtott ellátások finanszírozása, illetve az ártámogatás elszámolása, valamint a társadalombiztosítási ellátások megállapítása, kifizetése és a kifizetett ellátások visszafizetése, megtérítése érdekében,
h) bűnüldözés, továbbá a rendőrségről szóló 1994. évi XXXIV. törvényben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés,
i) a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása, az abban kapott felhatalmazás körében,
j) közigazgatási hatósági eljárás,
k) szabálysértési eljárás,
l) ügyészségi eljárás,
m) bírósági eljárás,
n) az érintettnek nem egészségügyi intézményben történő elhelyezése, gondozása,
o) a munkavégzésre való alkalmasság megállapítása függetlenül attól, hogy ezen tevékenység munkaviszony, közalkalmazotti, kormányzati szolgálati, politikai szolgálati, adó- és vámhatósági szolgálati, biztosi vagy közszolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik,31
p) köznevelés, szakképzés, illetve felsőoktatás céljából az oktatásra, illetve képzésre való alkalmasság megállapítása,
q) a katonai szolgálatra, illetve a személyes honvédelmi kötelezettség teljesítésére való alkalmasság megállapítása,
r) munkanélküli ellátás, foglalkoztatás elősegítése, valamint az ezzel összefüggő ellenőrzés,
s) az egészségügyi ellátásokra jogosultak részére vényen rendelt gyógyszer, gyógyászati segédeszköz és gyógyászati ellátás folyamatos és biztonságos kiszolgáltatása, illetve nyújtása érdekében,
t) a munkabalesetek, foglalkozási megbetegedések - ideértve a fokozott expozíciós eseteket is - kivizsgálása, nyilvántartása és a szükséges munkavédelmi intézkedések megtétele,
u) az egészségügyi dolgozókkal szemben lefolytatott etikai eljárás,
v) eredményesség alapú támogatásban részesülő gyógyszerek, gyógyászati segédeszközök eredményességének, támogatásának megállapítása, és ezen gyógyszerekkel kezelt kórképek finanszírozási eljárásrendjének alkotása,
w) betegút-szervezés,
x) az egészségügyi szolgáltatások minőségének értékelése és fejlesztése, az egészségügyi szolgáltatások értékelési szempontjainak rendszeres felülvizsgálata és fejlesztése,

y) az egészségügyi rendszer teljesítményének ellenőrzése, mérése és értékelése,
z) az egészségügyi ellátásokra jogosult részére a hatásos és biztonságos gyógyszerelés elősegítése, valamint a költséghatékony gyógyszeres terápia kialakítása érdekében,
zs) az Európai Unión belüli határon átnyúló egészségügyi ellátáshoz kapcsolódó jogok érvényesítése.

9 Az egészségügyi ellátó hálózat szerveinek adatkezelése

Az egészségügyi ellátó hálózaton belül az egészségügyi és személyazonosító adat kezelésére – amennyiben a törvény másként nem rendelkezik – jogosult: a betegellátó, az intézményvezető, az adatvédelmi felelős.

Különleges adat az érintett írásos hozzájárulása alapján kezelhető.

A 16. életévét betöltött kiskorú érintett hozzájárulását tartalmazó jognyilatkozatának érvényességéhez törvényes képviselőjének beleegyezése vagy utólagos jóváhagyása nem szükséges.

Az egészségügyi adat felvétele a gyógykezelés része.

Az egészségügyi és személyazonosító adatok kezelése során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, vagy megsemmisüléssel, megváltozással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá.

Az egészségügyi dolgozót, valamint az egészségügyi szolgáltatóval munkavégzésre irányuló jogviszonyban álló más személy minden, a beteg állapotával kapcsolatos, valamint az egészségügyi szolgáltatás nyújtása során tudomására jutott adat és egyéb tény vonatkozásában, időbeli korlátozás nélkül titoktartási kötelezettség terheli, függetlenül attól, hogy az adatokat közvetlenül a betegtől, vizsgálata, vagy gyógykezelése során, illetve közvetetten az egészségügyi dokumentációból vagy bármely más módon ismer meg. A titoktartási kötelezettség nem vonatkozik arra az esetre, ha ez alól a beteg felmentést adott vagy a jogszabály az adat szolgáltatásának kötelezettségét írja elő.

A személyazonosításra alkalmatlan egészségügyi adat időbeli és területi korlát nélkül továbbítható.

Adatfelvétel és módosítása

Az adatfelvétel során az egészségügyi dokumentációban rögzíteni kell az adatfelvétel időpontját és az adatfelvevő személyét. Az osztályokon dolgozók **aláírás mintáját** nyilvántartásban kell rögzíteni.

Az egészségügyi dokumentációban szereplő hibás egészségügyi adatot – az adatfelvételt követően - úgy kell **kijavítani** vagy **törölni**, hogy az eredetileg felvett adat megállapítható legyen. A módosítást kézjeggyel el kell látni.

A nyilvántartott adatokról, az egészségügyi dokumentációról az adatkezelő hiteles másolatot készít, ha ezt az adatbiztonság vagy a tárolt adatok fizikai védelme, illetve azt törvényben előírt adatközlési kötelezettség szükségessé teszi.

Az egészségügyi és személyes adatokat ért sérülés vagy megsemmisülés esetén a rendelkezésre álló adatforrásból meg kell kísérelni – a lehetséges mértékig – a károsodott adatok pótlását. Sérült adat pótlására annak a szervezeti egységnek a vezetője felelős, ahol a sérülés bekövetkezett. A pótolt adatokon a pótlás tényét fel kell tüntetni. A pótlásról jegyzőkönyvet kell felvenni.

10 Tájékoztatási jog és kötelezettség

Az érintett személy (egészségügyi ellátást igénybevevő beteg) személyes adatai kezeléséről szóló tájékoztatást kérhet az érintett egészségügyi szolgáltatótól.

Abban az esetben, ha az érintett önként fordul az egészségügyi ellátó hálózathoz, a gyógykezeléssel összefüggő egészségügyi és személyazonosító adatainak kezelésére szolgáló hozzájárulását - ellenkező nyilatkozat hiányában - megadottnak kell tekinteni, és erről az érintettet (törvényes képviselőjét) tájékoztatni kell. Sürgős szükség, valamint az érintett belátási képességének hiánya esetén az önkéntességet vélelmezni kell.

Az adatok helyesbítésére, módosítására, törlésére irányuló kérelmet az ellátást nyújtó szervezeti egységen, az adatok hitelességét igazoló okmány bemutatását követően az adatkezelő végzi el. A betegellátást követően, a beteg írásos kérelem ellenében kérheti adatainak módosítását, az intézmény adatvédelmi tisztviselőjétől, vagy az Orvos igazgatótól. Amennyiben a kérelem megalapozott, az adatvédelmi tisztviselő, vagy az Orvos igazgató az adatok módosítását elvégzi, és a kérelmezőt írásban értesíti az eredményről.

Az érintett, jogosult tájékoztatást kapni a gyógykezeléssel összefüggésben történő adatkezelésről, a rá vonatkozó egészségügyi és személyazonosító adatokat megismerni, az orvosi dokumentációba betekinteni, arról másolatot kapni. Minden további másolatért díjfizetési kötelezettség terheli a kérelmezőt. Az egészségügyi dokumentáció megismerésének joga az Elektronikus Egészségügyi Szolgáltatási Tér (a továbbiakban: EESZT) által elektronikusan kezelt egészségügyi dokumentáció vonatkozásában az EESZT útján is gyakorolható.

Az érintett betegellátásának időtartama alatt az általa írásban felhatalmazott személyt is megilletik a fenti jogok. Az érintett ellátásának befejezését követően az általa teljes bizonyító erejű magánokiratban felhatalmazott személyt is megilletik a fenti jogok.

Az érintett halála esetén az érintett közeli hozzátartozója, törvényes képviselője, örököse jogosult a halálozással összefüggő, vagy összefüggésbe hozható, a megelőző kezeléssel kapcsolatos egészségügyi adatokat megismerni, arról saját költségére hiteles másolatot kérni, ha az érintett korábban másként nem rendelkezett.

Betegdokumentáció kiadás rendjéről szóló tájékoztatót az intézmény a honlapján is közzéteszi.

Az adatkezelési tevékenység nyilvánossága

Az intézmény honlapján (www.tmkorhaz.hu) közzéteszi az Adatvédelmi szabályzatot, és az Adatkezelési tájékoztatót.

Az adott szervezeti egységeken, a fekvőbeteg ellátás kezdetekor a beteg, vagy törvényes képviselőjének részére át kell adni az Adatkezelési tájékoztatót. Az Általános Hozzájárulási Nyilatkozaton a beteg, vagy törvényes képviselője nyilatkozik az adatkezelésekhez kapcsolódó hozzájárulásról. A hozzájáruló nyilatkozatnak tartalmaznia kell a törvényes képviselőnek arra vonatkozó nyilatkozatát, hogy jogosult az érintett helyett a jognyilatkozat megtételére.

Ellátásban részesülő személy részére átadott záródokumentáció (Ellátási Lap, Zárójelentés) tartalmaz egy rövidített adatkezelési tájékoztatót, utalva a részletes tájékoztató elérhetőségére.

Belső intranet hálózaton a dolgozók számára elérhetőek az adatkezeléssel kapcsolatos, hatályos igazgatói utasítások, szabályzatok, eljárásrendek, oktatási anyagok.

Az intézmény kezelésében lévő közérdekű adatok közzétételéről, illetve rendelkezésre bocsátásáról külön szabályzat rendelkezik

11 Az egészségügyi és személyazonosító adatok nyilvántartása

A beteg vizsgálatával, és gyógykezelésével kapcsolatos adatokat az egészségügyi dokumentáció tartalmazza. Az egészségügyi dokumentációt úgy kell vezetni, hogy az a valóságnak megfelelően tartalmazza az ellátás folyamatát.

Egészségügyi dokumentációban kötelezően rögzítendő adatokat az egészségügyről szóló 1997. évi CLIV. törvény 136§-a tartalmazza.

Az egészségügyi dokumentáció részeként meg kell őrizni az egyes vizsgálatokról készült leleteket, gyógykezelés, és konzílium során keletkezett iratokat, az ápolási dokumentációt, képalkotó diagnosztikus eljárások felvételeit, valamint a beteg testéből kivett szövetmintákat. Fekvőbeteg ellátás során Papír alapú kórlap-dokumentáció keletkezik, az egészségügyi és teljesítmény dokumentáció vezetés szabályairól az IG0604. számú igazgatói utasítás rendelkezik.

Az egészségügyi és személyazonosító adatok az egészségügyi ellátó hálózaton belül továbbíthatók, illetve összekapcsolhatók. Ennek keretében az adatokat csak addig az időpontig, és olyan mértékig lehet összekapcsolni, ameddig az a megelőzés, gyógykezelés, közegészségügyi, járványügyi intézkedések megtételéig feltétlenül szükséges.

Elektronikus Egészségügyi Szolgáltatási Tér (EESZT): Az egészségügyi szolgáltató, a jogszabályi rendelkezés értelmébe köteles az EESZT útján megküldeni az egészségügyi ellátás során keletkezett dokumentumokat. Az egészségügyi dokumentáció megismerésének joga EESZT által elektronikusan kezelt egészségügyi dokumentáció vonatkozásában az EESZT útján is gyakorolható.

Külföldre történő adattovábbítás esetén is e törvény rendelkezéseit kell alkalmazni azzal, hogy az egészségügyi és személyazonosító adatok csak akkor továbbíthatók, ha a külföldi adatkezelőnél az 1997.évi XLVII. tv. 6. § előírásai minden egyes adatra nézve teljesülnek. E törvény előírásait alkalmazni kell a meghalt személyre vonatkozó egészségügyi adatok esetén is.

Egészségügyi adatok, betegdokumentáció kérés, kiadás, magán, illetve hivatalos kérésre

Betegdokumentáció kiadás rendjéről szóló tájékoztatót, és az Egészségügyi dokumentációt kérő lap formanyomtatványt, az intézmény hivatalos honlapján közzéteszi. http://portal.tmkorhaz.hu/dokumentacio-kikeres-folyamata-es-adatlapok/

Hivatalos szerv általi dokumentáció kiadás céljából küldött kérelemre, és a válasz kiadására a Hivatali kapu szolgáltatást kell alkalmazni**.**

Egészségügyi dokumentáció megőrzése

Teljes kórlap-dokumentáció megőrzése az intézmény központi irattárában történik.

A dokumentumok megőrzési idejét a mindenkor hatályos 1997. évi XLVII. törvény rendelkezései szerint kell meghatározni.

A megőrzési időn túli dokumentumok megsemmisítésre történő elszállítása az IG0601 számú szabályzat alapján történik.

12 Adatvédelmi incidens bejelentése, nyilvántartás

Az Európai Uniós Irányelv (GDPR) 33. cikkének előírása szerint az adatkezelőnek bejelentési kötelezettsége van a felügyeleti hatóságnak, adatvédelmi incidens esetén.

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges legkésőbb 72 órán belül az után, hogy az adatvédelmi incidens a tudomására jutott, bejelenti a felügyeleti hatóságnak, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságára nézve. Ha a bejelentés nem történik meg 72 órán belül, mellékelni kell hozzá a késedelem igazolására szolgáló indoklást is.

A nyilvántartásban rögzíteni kell:

a) az incidensben érintett személyes adatok körét; és számát,
b) az adatvédelmi incidenssel érintettek körét, és számát,
c) az adatvédelmi incidens tudomásszerzés időpontját,
d) az adatvédelmi incidens körülményeit, hatásait,
e) az adatvédelmi incidens elhárítására megtett intézkedéseket,
f) az adatvédelmi incidenssel kapcsolatban adott tájékoztatások adatait.

Amennyiben az adatkezelő adatfeldolgozót vesz igénybe. Az adatfeldolgozónál előforduló incidensről az adatfeldolgozónak az adatkezelőt kötelessége tájékoztatni.

Az intézmény az adatvédelmi incidens kivizsgálásával kapcsolatos papíralapú és elektronikus dokumentumokat 10 évig köteles megőrizni. Az adatvédelmi incidensek vizsgálata során keletkezett iktatott dokumentumokat az adatvédelmi tisztviselő az incidens vizsgálatának lezárásától számított minimálisan 10 évig őrzi meg, illetéktelenek számára hozzá nem férhető zárt helyen.
Amennyiben az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintett személy jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja az érintettet az adatvédelmi incidensről. Az érintettek részére nyújtott tájékoztatásban közérthetően ismertetni kell az adatvédelmi incidens jellegét.

Az érintettet nem kell tájékoztatni, ha

a) az adatkezelő megfelelő technikai és szervezési intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazzák,
b) az adatkezelő tovább intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat továbbiakban valószínűsíthetően nem valósul meg,
c) a tájékoztatás aránytalan erőfeszítést tenne szükségessé,

13 Harmadik országba irányuló adattovábbítás szabályai

Amennyiben személyes adatnak harmadik országba történő továbbításának szükségessége merül fel, az érintett szervezeti egység köteles az adatvédelmi tisztviselő véleményét kérni az adattovábbítás megengedhetőségéről, illetve az adattovábbítás lehetséges módjáról, figyelembe véve a GDPR szabályait és az aktuális országbesorolást.

Az adatvédelmi tisztviselő – szükség esetén a Jogi osztály és az informatikai szakterület véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

14 Belső adatvédelmi ellenőrzési eljárás

A belső adatvédelmi ellenőrzési eljárás célja, hogy az adatvédelmi tisztviselő meggyőződjön arról, hogy az intézmény egyes szervezeti egységei az adatvédelemmel kapcsolatos jogszabályoknak és belső szabályzatoknak megfelelően kezelik-e az adatokat.

Az adatvédelmi tisztviselő éves ellenőrzési tervet készít. Az éves ellenőrzési tervnek az ellenőrzés alá vont szervezeti egység nevét és az ellenőrzés várható időpontját, továbbá az ellenőrzés tárgykörét kell tartalmaznia. Az éves ellenőrzési terveket úgy kell elkészíteni, hogy négyéves időtartam alatt lehetőség minden szerint szervezeti egység ellenőrzésére sor kerüljön. Az éves ellenőrzési tervet legkésőbb adott év február 28. napjáig kell elkészíteni és az intézmény főigazgatója részére bemutatni.

Az éves ellenőrzési tervet az intézmény főigazgatója hagyja jóvá.

Az adatvédelmi tisztviselő az ellenőrzés lefolytatásáról az érintett szervezeti egység vezetőjét az ellenőrzés kezdete előtt 10 nappal tájékoztatja, melyben az eljárás kezdő időpontjára is javaslatot tesz. A szervezeti egység vezetője köteles gondoskodni arról, hogy az adatvédelmi tisztviselő a javasolt időpontban megkezdhesse ellenőrzését, illetve szükség esetén – legfeljebb tíz munkanapon belüli – új időpontra tesz javaslatot.

Az ellenőrzés során az adatvédelmi tisztviselő a szervezeti egység irodahelységeibe beléphet, a szervezeti egység – ellenőrzés tárgyával összefüggésben kezelt – irataiba betekinthet, a szervezeti egység munkatársaitól tájékoztatást kérhet adott üggyel kapcsolatos adatkezelésről.

Az adatvédelmi tisztviselő az ellenőrzés megtörténtéről jegyzőkönyvet készít, melyet az ellenőrzött szervezeti egység vezetőjével mindketten aláírnak. A jegyzőkönyv az ellenőrzött szervezeti egység, valamint annak vezetője nevét, az ellenőrzés lefolytatásának tényét, annak időpontját és időtartamát tartalmazza.

Az adatvédelmi tisztviselő a lefolytatott ellenőrzésről vizsgálati jelentést készít, melynek mellékletét képezi az ellenőrzésről készült jegyzőkönyv. A vizsgálati jelentés tartalmazza az adott szervezeti egységnél vizsgált körülményeket, adatokat, megállapításokat. A vizsgálati jelentés tervezetére a szervezeti egység vezetője 10 napon belül észrevételt tehet. Az észrevételezés elmaradása a szervezeti egység vezetőjének egyetértését jelenti.

Ha az adatvédelmi tisztviselő megállapítja, hogy az adatkezelés az ellenőrzés alá vont szervezeti egységnél nem a belső szabályzatoknak vagy jogszabályoknak megfelelően történik, javaslatot tesz a szabályszerű adatkezelés – meghatározott határidőn belüli – helyreállítására. Az ezek alapján megtett intézkedésekről a szervezeti egység vezetője tájékoztatást nyújt. Az adatvédelmi tisztviselő a megtett intézkedéseket, illetve azok betartását bármikor jogosult ellenőrizni.

Az adatvédelmi tisztviselő rendkívüli ellenőrzést is lefolytathat, ha adatvédelmi szempontból az indokolt, különösen, ha a személyes adatkezeléssel érintettek száma jelentős. Rendkívüli ellenőrzésnek minősül az éves ellenőrzési tervben nem szereplő ellenőrzés. A rendkívüli ellenőrzést az intézmény főigazgatója előzetesen engedélyezi.

Az adott ellenőrzéssel kapcsolatban az intézmény főigazgatója külön tájékoztatást kérhet az adatvédelmi tisztviselőtől, egyébként az adatvédelmi tisztviselő évente egy alkalommal,

legkésőbb a tárgyévet követő év február 28. napjáig összefoglaló jelentést készít az általa a tárgyévben lefolytatott ellenőrzésekről, amelyet az intézmény főigazgatója részére küld meg.

15 Hatályosság

Az Adatvédelmi szabályzat a Tolna Megyei Balassa János Kórházában történő adatkezelést szabályozza. Intézményi adatvédelmi tisztviselőt nevez ki a főigazgató főorvos.

Az egyes osztályokon az Adatvédelmi szabályzat betartásáért az adott szervezeti egység vezetője felel, vagy esetleg ellenőrzési jogkörét megosztja az általa kijelölt adatvédelmi felelőssel.(EAVF).

A szabályzat érvényessége a hatálybalépéstől a felülvizsgálatig terjed. A szabályzat felülvizsgálandó jogszabályi, szervezeti felépítésben történt változás esetén.

Az Adatvédelmi szabályzatot minőségirányítási rendszerünk előírásai szerint az intraneten és a honlapon közzétesszük.

16 Adatvédelmi szabályzat mellékletei

1. Az intézmény szervezeti felépítése
2. Kórlaptárolás folyamata
3. Adatkezelési szervezet felépítése
4. Megbízás EAVF részére
5. Betegdokumentációt kérő lap
6. Betegtájékoztató az egészségügyi és személyazonosító adatok kezeléséről (Adatkezelési tájékoztató)
7. Nyilatkozat az adatkezelés tiltásáról (Általános hozzájárulási nyilatkozat)
8. Házirend
9. Aláírás minta nyilvántartása
10. Tájékoztató egészségügyi dokumentáció másolatot kérelmezők részére
11. Incidenskezelési űrlap