ADATKEZELÉSI ÉS ADATVÉDELMI SZABÁLYZAT
ÉS
INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Készítette:	Dr. Varga Gábor adatvédelmi tisztviselő	2019.12.12. dátum	
	Dr. Balikó Gergely ügyvéd		
Jóváhagyta:	Dr. Nagy Zoltán főigazgató	2019.12.12. dátum	
Minőségügyi szempontból ellenőrizte:	Horváth Lőrincné minőségirányítási vezető	2019.12.12. dátum	

BALIKÓ ÜGYVÉDI IRODA
DR Balikó Gergely ügyvéd
8400 Ajka, Szabadság tér 2. fsz. 1.
Adószám: 19385240-1-19
KISADÓZÓ

MAGYAR IMRE KÓRHÁZ Veszprém megye Ajka FŐIGAZGATÓ

A dokumentáció kódja:	SZMSZ-M-05
Változat száma:	05.
Érvénybelépés időpontja:	2019.12.12.
Oldalak száma:	26.
Mellékletek száma:	5.
Iktatószám:	268-21/2019/0500/MIG/4/0/1

MÓDOSÍTÁSOK JEGYZÉKE

Módosította aláírás / dátum	Módosítást követő verziószám	Módosított oldalszám	Jóváhagyta aláírás / dátum	Ellenőrizte aláírás/dátum	Kibocsátás dátuma

Nyilvántartott példány: ☒ Munkapéldány: ☐

A példány sorszáma: ☐☐

TARTALOMJEGYZÉK

1. JOGSZABÁLYOK ÉS RÖVIDÍTÉSEK JEGYZÉKE

Az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény - Eüak.

Az információs önrendelkezési jogról és az információszabadságról szóló 1997. évi 2011. évi CXVII. törvény - Infotv.

Az Európai Parlament és 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 rendelet hatályon kívül helyezéséről - GDPR

Magyar Imre Kórház a továbbiakban egészségügyi szolgáltató, Kórház vagy munkáltató

2. A SZABÁLYZAT CÉLJA, HATÁLYA

Az adatvédelmi és adatkezelési szabályzat célja, hogy az egészségügyi szolgáltatóval kapcsolatba kerülő természetes személyek esetén biztosítsa az információs önrendelkezési jog érvényesülését, a magánszféra tiszteletben tartását, az adatkezelés célhoz kötöttségét, az adatok védelmét. Célja továbbá, hogy meghatározza az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének feltételrendszerét a hatályos jogszabályokkal összhangban.

E szabályzat ***személyi hatálya*** kiterjed a Magyar Imre Kórház egészségügyi dolgozóira és az egészségügyben dolgozókra, függetlenül a foglalkoztatás formájától, a Kórházzal szerződéses jogviszonyban álló jogi személyekre (a továbbiakban: betegellátó); az egészségügyi szolgáltatóval kapcsolatba kerülő betegekre és hozzátartozóikra.

A szabályzat az informatikai rendszerrel kapcsolatos, biztonságos adatkezelési és adatvédelemi eljárásokat és feladatokat rögzíti: a számítástechnikai eszközök beszerzésének és használatának, a saját készítésű és vásárolt szoftverek alkalmazásának a folyamatát, továbbá egyes személyek informatikai biztonságot érintő feladatait.

A szabályzat ***tárgyi hatálya*** kiterjed:

- az egészségügyi szolgáltatónál keletkező egészségügyi dokumentációra, függetlenül annak hordozójától, vagy formájától;
- valamennyi használatban lévő, vagy tárolt informatikai berendezésre és azok műszaki dokumentációjára függetlenül attól, hogy az személyi használatra vagy szervezeti egység használatába került kiadásra;
- az egészségügyi szolgáltatónál keletkezett minden elektronikus adatra, annak keletkezésének, felhasználásának és feldolgozásának helyétől és megjelenési formájától függetlenül;
- a Magyar Imre Kórház által használt felhasználói programokra és rendszerprogramokra;
- az informatikai rendszerben megjelenő valamennyi dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési).

A személyes adatok védelméért, az adatkezelés jogszerűségéért a szervezet vezetője felelős.

3. AZ ILLETÉKESSÉG ÉS FELELŐSSÉG MEGHATÁROZÁSA

A szabályzat kidolgozásáért felelős:	főigazgató
A szabályzat jóváhagyásáért	főigazgató
A szabályzat tartalmáért felelős:	adatvédelmi tisztviselő
Az utasítás alkalmazásának, ellenőrzésének megszervezéséért a belső felülvizsgálatok során:	minőségirányítási vezető

4. MEGHATÁROZÁSOK

Érintett: bármely információ alapján azonosított vagy azonosítható természetes személy.

Egészségügyi személyes adatok: az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról. Ide tartoznak az alábbi a természetes személyre vonatkozó olyan adatok, amelyeket az egészségügyi szolgáltatások céljából történő nyilvántartásba vétel, vagy ilyen szolgáltatások nyújtása során gyűjtöttek, a természetes személy egészségügyi célokból történő egyéni azonosítás érdekében hozzá rendelt szám, jel, adat, valamely testrész, vagy testet alkotó anyag - beleértve a genetikai adatokat és a biológiai mintákat is - tesztelésből vagy vizsgálatokból származó információk, és bármilyen, az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától.

Genetikai adat: olyan a természetes személy örökölt vagy szerzett genetikai jellemzőivel összefüggő minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi információt hordoz, és amely az érintett személytől vett biológiai mintaelemzések eredménye, különösen kromoszómaelemzések, dezoxiribonukleinsav (DNS) vagy ribonukleinsav (RNS) vizsgálatának, vagy ezekből nyerhető információkkal megegyező információk kinyerését lehetővé tevő bármilyen más elem vizsgálat.

Biometrikus adat: egy természetes személy fizikai, fiziológiai vagy viselkedési jellemzőire vonatkozó olyan, sajátos technikai eljárásokkal nyert személyes adat, amely lehetővé teszi vagy megerősíti a természetes személy egyedi azonosítását, mint például az arckép vagy a daktiloszkópiai adat;

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

Adatkezelő: az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely - törvényben vagy az Európai Unió kötelező jogi aktusában meghatározott keretek között - önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja;

Adatkezelés: az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége. Így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése;

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele;

Harmadik személy: olyan természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére irányuló műveleteket végeznek;

Hozzájárulás: az érintett akaratának önkéntes, határozott és megfelelő tájékoztatáson alapuló egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy az akaratát félreérthetetlenül kifejező más magatartás útján jelzi, hogy beleegyezését adja a rá vonatkozó személyes adatok kezeléséhez;

Adatvédelmi incidens: az adatbiztonság olyan sérelme, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisülését, elvesztését, módosulását, jogosulatlan továbbítását vagy nyilvánosságra hozatalát, vagy az azokhoz való jogosulatlan hozzáférést eredményezi;

Profilalkotás: személyes adat bármely olyan - automatizált módon történő - kezelése, amely az érintett személyes jellemzőinek, különösen a munkahelyi teljesítményéhez, gazdasági helyzetéhez, egészségi állapotához, személyes preferenciáihoz vagy érdeklődéséhez, megbízhatóságához, viselkedéséhez, tartózkodási helyéhez vagy mozgásához kapcsolódó jellemzőinek értékelésére, elemzésére vagy előrejelzésére irányul;

Álnevesítés: személyes adat olyan módon történő kezelése, amely - a személyes adattól elkülönítve tárolt - további információ felhasználása nélkül megállapíthatatlanná teszi, hogy a személyes adat mely érintettre vonatkozik, valamint műszaki és szervezési intézkedések megtételével biztosítja, hogy azt azonosított vagy azonosítható természetes személyhez ne lehessen kapcsolni;

5. ADATKEZELÉS ÁLTALÁNOS SZABÁLYAI

5.1. AZ ADATKEZELÉS ALAPELVEI

Személyes adat kizárólag egyértelműen meghatározott, jogszerű célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok gyűjtésének és kezelésének tisztességesnek és törvényesnek kell lennie.

Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.

A személyes adat az adatkezelés során mindaddig megőrzi e minőségét, amíg kapcsolata az érintettel helyreállítható. Az érintettel akkor helyreállítható a kapcsolat, ha az adatkezelő rendelkezik azokkal a technikai feltételekkel, amelyek a helyreállításhoz szükségesek.

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.

Az adatkezelés során arra alkalmas műszaki vagy szervezési - így különösen az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisülésével vagy károsodásával szembeni védelmet kialakító - intézkedések alkalmazásával biztosítani kell a személyes adatok megfelelő biztonságát.

5.2. ADATKEZELÉS ALAPJA

Egészségügyi és hozzá kapcsolódó személyes adatot kezelni jogszerűen csak az alábbi feltételek valamelyikének teljesülése esetén lehetséges:

- azt törvény közérdeken alapuló célból elrendeli,
- az adatkezelő törvényben meghatározott feladatainak ellátásához feltétlenül szükséges és az érintett a személyes adatok kezeléséhez kifejezetten hozzájárult,
- az érintett vagy más személy létfontosságú érdekeinek védelméhez, valamint a személyek életét, testi épségét fenyegető közvetlen veszély elhárításához vagy megelőzéséhez szükséges és azzal arányos és az törvényben kihirdetett nemzetközi szerződés végrehajtásához feltétlenül szükséges és azzal arányos, vagy azt az Alaptörvényben biztosított alapvető jog érvényesítése, továbbá a nemzetbiztonság, a bűncselekmények megelőzése, felderítése vagy üldözése érdekében vagy honvédelmi érdekből törvény elrendeli.

Különleges adatok kezelése esetén az adatkezelő, illetve a megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó megfelelő műszaki és szervezési intézkedésekkel biztosítja, hogy az adatkezelési műveletek végzése során a különleges adatokhoz kizárólag az rendelkezzen hozzáféréssel, akinek az adatkezelési művelettel összefüggő feladatának ellátásához feltétlenül szükséges.

Az érintett személy hozzájárulása esetén az adatkezelőnek kell igazolnia a hozzájárulás meglétét. A hozzájárulás megadásának írásbelinek kell lennie.

5.3. ADATVÉDELMI INTÉZKEDÉSEK

A szervezetnél nyilvántartott adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozatal, illetve a sérülés, törlés, vagy megsemmisülés ellen.

Iratot munkaköri feladat ellátásán kívül a munkahelyről kivinni, valamint munkahelyen kívül feldolgozni, tárolni csak a szervezet vezetője egyetértésével lehet, azzal a feltétellel, hogy az irat tartalmát illetéktelen személy ne ismerje meg. Az iratok kezelése, tárolása során ki kell zárni annak a lehetőségét, hogy illetéktelen személy az iratok tartalmába betekintést nyerjen. Az iratokat a szervezetnél zárható helységben, elkülönítetten kell tárolni. A munkavégzés céljára szolgáló irodákat a köztisztviselő, munkavállaló távozásakor kulcsra kell zárni.

Az irodahelységek nyitva tartása miatti iratokhoz történő illetéktelen hozzáférés esetén az érintett fegyelmi és kártérítési felelősséggel tartozik.

5.4. EGÉSZSÉGÜGYI ÉS A HOZZÁJUK KAPCSOLÓDÓ SZEMÉLYES ADATOK KEZELÉSÉNEK SZABÁLYAI

Az egészségügyi és személyazonosító adat kezelésének célja:

a) az egészség megőrzésének, fenntartásának előmozdítása,

b) a betegellátó eredményes gyógykezelési tevékenységének elősegítése,

c) az érintett egészségi állapotának nyomon követése,

d) a közegészségügyi és járványügyi érdekből szükségessé váló intézkedések megtétele.

Az fenti adatkezelési célok eléréséhez csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelési cél megvalósításához elengedhetetlenül szükséges.

Az adatkezelő és adatfeldolgozó az orvosi titkot köteles megtartani, az alábbi kivételével:

- az érintett, illetve törvényes képviselője ehhez írásban hozzájárul, az abban foglalt korlátozásokon belül, valamint,
- törvény előírásai miatt.

Az érintett (törvényes képviselője) jogosult tájékoztatást kapni a gyógykezeléssel összefüggésben történő adatkezelésről, a rá vonatkozó egészségügyi és személyazonosító adatokat megismerheti, az orvosi dokumentációba betekinthet, valamint azokról - saját költségére - másolatot kaphat.
Az egészségügyi adatok felvétele a gyógykezelés része. A kezelést végző orvos dönti el, hogy a szakmai szabályoknak megfelelően - a kötelezően felveendő adatokon kívül - mely egészségügyi adat felvétele szükséges.
Az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy a kezelést végző orvos utasításának megfelelően, illetve a feladatai ellátásához szükséges mértékben vehet fel egészségügyi adatot.
Az egészségügyi és a személyazonosító adatoknak az érintett részéről történő szolgáltatása önkéntes, az alábbi esetek kivételével:

a) ha valószínűsíthető vagy beigazolódott, hogy az 1. számú mellékletben felsorolt valamely betegség kórokozója által fertőződött, vagy fertőzéses eredetű mérgezésben, illetve fertőző betegségben;
b) ha arra a 2. számú mellékletben felsorolt szűrő- és alkalmassági vizsgálatok
c) elvégzéséhez van szükség,
d) heveny mérgezés esetén,
e) ha valószínűsíthető, hogy az érintett a 3. számú melléklet szerinti foglalkozási eredetű megbetegedésben szenved,
f) ha az adatszolgáltatásra a magzat, illetve a kiskorú gyermek gyógykezelése, egészségi állapotának megőrzése vagy védelme érdekében van szükség,
g) ha bűnüldözés, bűnmegelőzés céljából, továbbá ügyészségi, bírósági eljárás, illetve szabálysértési vagy közigazgatási hatósági eljárás során az illetékes szerv a vizsgálatot elrendelte,
h) ha az adatszolgáltatásra a nemzetbiztonsági szolgálatokról szóló törvény szerinti ellenőrzés céljából van szükség.

Sürgős szükség, valamint az érintett belátási képességének hiánya esetén az önkéntességet vélelmezni kell.
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.
A betegellátó haladéktalanul továbbítja az ÁNTSZ intézetének az adatfelvétel során tudomására jutott egészségügyi és személyazonosító adatot, a törvényben előírt járványügyi, illetve közegészségügyi esetekben.
Az érintett egészségügyi adatai statisztikai célra - a törvény által engedélyezett kivételektől eltekintve -, vagy az érintett írásbeli hozzájárulásával, vagy személyazonosításra alkalmatlan módon kezelhetők.
Tudományos kutatás céljából az intézményvezető vagy az adatvédelmi felelős engedélyével a tárolt adatokba be lehet tekinteni, azonban tudományos közleményben nem szerepelhetnek egészségügyi és személyazonosító adatok oly módon, hogy az érintett személyazonossága megállapítható legyen. Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.
A tárolt adatokba tudományos kutatás céljából betekintett személyekről, a betekintés céljáról és időpontjáról nyilvántartást kell vezetni.
A nyilvántartás kötelező megőrzési ideje 10 év.

A kutatási kérelem megtagadását az intézményvezető vagy az adatvédelmi felelős köteles írásban megindokolni.

A következő szervek írásbeli megkeresésére az Intézmény az érintett egészségügyi és személyazonosító adatait átadja a megkereső szervnek. A megkeresésben a fel kell tüntetni a megismerni kívánt egészségügyi és személyazonosító adatokat, illetve az adatkezelés pontos célját:

a) büntetőügyben a nyomozó hatóság, az ügyészség, a bíróság, az igazságügyi orvos szakértő, polgári és közigazgatási ügyben az ügyészség, a bíróság, az igazságügyi orvos szakértő,
b) szabálysértési eljárás során az eljárást lefolytató szervek,
c) hadköteles személy esetén az illetékes jegyző, a hadkiegészítő parancsnokság, illetve a katonai egészségügyi alkalmasságot megállapító bizottság,
d) a nemzetbiztonsági szolgálatok, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében.

Az érintett első ízben történő orvosi ellátásakor, ha az érintett 8 napon túl gyógyuló sérülést szenvedett és a sérülés feltehetően bűncselekmény következménye, a kezelőorvos a rendőrségnek haladéktalanul bejelenti az érintett személyazonosító adatait.

A kiskorú érintett első ízben történő egészségügyi ellátásakor - a gyermekek védelméről és a gyámügyi igazgatásról szóló 1997. évi XXXI. törvény 17. §-ára is tekintettel - az ellátást végző egészségügyi szolgáltató ezzel megbízott orvosa köteles az egészségügyi szolgáltató telephelye szerint illetékes gyermekjóléti szolgálatot haladéktalanul értesíteni, ha

a) feltételezhető, hogy a gyermek sérülése vagy betegsége bántalmazás, illetve elhanyagolás következménye,
b) a gyermek egészségügyi ellátása során bántalmazására, elhanyagolására utaló körülményekről szerez tudomást.

Amennyiben az érintett egészségügyi adatai más személyt is érintenek, az egészségügyi és személyazonosító adatok továbbításához e harmadik személy (törvényes képviselője) írásbeli hozzájárulását be kell szerezni.

Az egészségügyi dokumentációt - a képalkotó diagnosztikai eljárással készült felvételek, az arról készített leletek kivételével - az adatfelvételtől számított legalább 30 évig, a zárójelentést legalább 50 évig kell megőrizni. A kötelező nyilvántartási időt követően gyógykezelés vagy tudományos kutatás érdekében - amennyiben indokolt - az adatok továbbra is nyilvántarthatók. Ha a további nyilvántartás nem indokolt a nyilvántartást meg kell semmisíteni.

Képalkotó diagnosztikai eljárással készült felvételt, valamint a felvétel esetén az arról készített leletet kell - a felvétel készítésétől számított - legalább 30 évig megőrizni.

Amennyiben az egészségügyi dokumentációnak tudományos jelentősége van, a kötelező nyilvántartási időt követően át kell adni a Semmelweis Orvostörténeti Múzeum, Könyvtár és Levéltár részére.

Az egészségügyi dokumentációban szereplő hibás egészségügyi adatot - az adatfelvételt követően - úgy kell kijavítani vagy törölni, hogy az eredetileg felvett adat megállapítható legyen.

5.5. SZEMÉLYZETI BÉR- ÉS MUNKAÜGYI NYILVÁNTARTÁS

A személyzeti, bér- és munkaügyi nyilvántartás az Intézmény dolgozóira, az Intézménnyel szerződéses jogviszonyban álló személyekre vonatkozó tények dokumentálására szolgáló adatkezelés alapját, a közalkalmazottak jogállásáról szóló 1992. évi XXXIII. törvény, az Intézmény Működési Szabályzata, Kollektív Szerződése és a Bér- és Munkaügyi Szabályzat képezi.
A személyzeti nyilvántartás adatai az alkalmazotti jogviszonyával kapcsolatos tények megállapítására, a besorolási követelmények igazolására és statisztikai adatszolgáltatásra használhatók fel.

A dolgozói nyilvántartásba felvehető adatok köre:

- név, születési hely és idő, állampolgárság;
- állandó és ideiglenes lakcím, telefonszám;
- munkaviszonyra, közalkalmazotti jogviszonyra vonatkozó adatok,
- iskolai végzettség, szakképesítés, alkalmazási feltételek, képesítési feltételek alóli mentesítés,
- továbbképzés, szakirányú továbbképzés, továbbképzésben szerzett szakképesítés,
- tudományos fokozatok, címek,
- idegen nyelv tudása,
- kinevezési okmány, munkakör, munkaköri leírás,
- vezetői megbízások,
- gyakornoki idő, vizsga, próbaidő,
- fegyelmi eljárás, büntetés, felmentés,
- fizetési fokozat,
- tudományos kutatás (publikáció), tudományos kapcsolatok,
- munkában töltött idő, közalkalmazotti jogviszonyba beszámítható idő, besorolással kapcsolatos adatok,
- dolgozó által kapott kitüntetések, díjak és más elismerések, címek,
- munkakör, munkakörbe nem tartozó feladatra történő megbízás, munkavégzésre irányuló további jogviszony, - fegyelmi, büntetés, kártérítésre kötelezés,
- munkavégzés ideje, túlmunka ideje, alapilletmény, pótlékok (jogcím szerint), illetménykiegészítés, megbízási díj, továbbá az azokat terhelő tartozás és annak jogosultja,
- szabadság, kiadott szabadság,
- dolgozó részére történő kifizetések és azok jogcímei,
- a dolgozó részére adott juttatások és azok jogcímei,
- a dolgozó munkáltatóval szemben fennálló tartozásai, azok jogcímei,
- a többi adat az érintett hozzájárulásával.

A személyzeti, nyilvántartás adatait az érintett szolgáltatja. Az alkalmazotti jogviszony keletkezésekor történik meg az elsődleges adatfelvétel.
A személyzeti, bér- és munkaügyi nyilvántartás kezelője Bér- és Munkaügyi Osztály. Az Intézmény szervezetén belül a személyzeti, bér- és munkaügyi nyilvántartásból csak a főigazgató, Gazdasági Igazgatóság, Bér- és Munkaügyi Osztályvezető, valamint azon szervezeti egységek vezetői, illetve személyzeti kérdésekben illetékes ügyintézői részére teljesíthető adatszolgáltatás, amelyeknél az érintett tényleges munkát végez.

6. AZ ADATVÉDELEMÉRT FELELŐS SZEMÉLYEK ÉS FELADATAIK

Az egészségügyi intézményen belül az egészségügyi és személyazonosító adatok védelméért a nyilvántartás megőrzéséért a főigazgató felelős.

6.1. A FŐIGAZGATÓ FELADATAI

A főigazgató tevékenysége során

a) Kijelöli az intézeti adatvédelmi tisztviselőt és ellenőrzi annak tevékenységét,
b) Kijelöli az intézmény önálló egészségügyi adatkezelési rendszereit,
c) Gondoskodik az intézmény adatvédelmi szabályzatának elkészíttetéséről,
d) Gondoskodik az intézmény iratkezelési szabályzatának elkészíttetéséről,
e) Engedélyezi az orvosi dokumentációba való betekintést.

6.2. ADATVÉDELMI TISZTVISELŐ FELADATAI

a) Összehangolja az Intézmény egyes szervezeti egységeinek adatvédelemhez kapcsolódó szabályozásait, eljárásait, munkaköri leírásait, rögzíti a felelősségi, ellenőrzési kompetenciákat,
b) Az adatbiztonsági-adatvédelmi feladatokról, az adatvédelemmel kapcsolatos problémákról folyamatos tájékoztatás az főigazgató részére
c) Javasolja és támogatja az adatvédelem, ill. adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazását.
d) Kapcsolatot tart az ellátási területen dolgozó orvosokkal a korszerű és biztonságos adatcsere elősegítése céljából,
e) Egységesíti az adatvédelemhez kapcsolódó bizonylatokat.
f) Elkészíti, aktualizálja az Adatvédelmi Szabályzatot.
g) Összehangolja az adatvédelmi ellenőrzési tevékenységet, melynek különböző szintű megvalósulása érdekében központi ellenőrzési tervet dolgoz ki.
h) Megszervezi az Eüaktv. Által előírt adatvédelmi oktatás Intézmény-szintű oktatási rendjét.
i) Személyesen részt vesz az oktatásban, egységesíti az Intézmény által előírt adatvédelmi vonatkozású oktatási segédanyagok tartalmát.
j) Ellenőrzi az Intézményben végzett személyazonosítóval összekapcsolt egészségügyi adatok kezelésének rendjét az intézeti adatvédelmi felelősök, adatvédelmi munkatársak és osztályos adatvédelmi felelősök munkáján keresztül.
k) Kezdeményezi az adatvédelem, és adatbiztonság területén kifejlesztett új technológiák és eszközök, eljárások alkalmazását, és ezekkel kapcsolatban javaslatot tesz a Főigazgatónak.

l) Eljár a Főigazgató által rábízott, adatvédelemmel kapcsolatos panaszok kivizsgálásában.
m) Szervezi és szakmailag irányítja az adatvédelem munkáját, felelős a vezetése alatt álló egység működéséért, továbbá a feladatkörébe utalt feladatok teljesítéséért és ellenőrzéséért.
n) Az egységvezetők kijelölése alapján megbízza az Egység adatvédelmi felelősöket.
o) Gondoskodik az intézmény általános adatvédelmi, adatkezelési szabályzatának betartásáról.
p) Betartja és betartatja az eljárási rend adatvédelmi incidens esetén.
q) 1 évenként felülvizsgálja az adatkezelési szabályzatokat.

6.3. AZ EGYSÉG ADATVÉDELMI FELELŐS

Feladatai:

- Gondoskodik az egységen belül az adatvédelmi szabályok betartásáról, oktatást tart éves szinten az egységen belül az adatvédelmi kérdésekről.
- Minden év végén írásos beszámolót készít az előző év adatvédelméről.
- Nyilvántartja a kötelező és hivatalos adatszolgáltatási kötelezettségeket és gondoskodik azok előírásszerű teljesítéséről.
- Érvényesíti a betegek adatvédelmi jogaik megismerésének lehetőségét és gyakorlásának feltételeit.
- Kapcsolatot tart az ellátási területen dolgozó orvosokkal a korszerű és biztonságos adatcsere elősegítése céljából.
- Ellenőrzi az orvosi titok megtartását.
- Ellenőrzi a szabályzatok betartását, az aláírás minták vezetését.
- Figyelemmel kíséri az egység egységben történő valamennyi adatkezelést az adatvédelmi szabályzat betartásának szempontjából.
- Betartja és betartatja az eljárás- rendet adatvédelmi incidens esetén. Adatvédelmi vagy információbiztonsági incidensek esetén haladéktalanul jelzi azokat az Adatvédelmi Tisztviselőnek .
- javaslatot tesz az Adatvédelmi tisztviselőnek az adatvédelem betartása érdekében szükséges intézkedésekre.
- Joga van betekinteni az adatvédelemmel kapcsolatos minden szóba jöhető iratba és dokumentációba.
- Felméri és figyelemmel kíséri az osztályon történő valamennyi adatkezelési folyamatot az adatvédelmi szabályzat előírásainak megfelelően. Felméri és naprakészen tartja az osztályos adatvagyon leltárt. Az osztályon történő adatkezelés során az érintetteknek tájékoztatást ad az érvényes adatvédelmi szabályokról

6.4. ADATKEZELŐ

Adatkezelő az adatkezeléssel meghatározott tevékenységet végző vagy mással végeztető szerv vagy személy.
Az adatkezelő

a.) Köteles megtenni minden olyan technikai és szervezési intézkedést, amelyek szükségesek az adatvédelmi és titokvédelmi jogszabályok érvényre jutásához,

b.) Védje az adatokat különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás, törlés, sérülés vagy megsemmisülés ellen.

c.) Az adatkezelő - törvény által meghatározott kivétellel - az orvosi titkot köteles megtartani.

Az adatkezelőknek ismerniük kell az adatkezelés szabályait:

a) gondoskodniuk kell arról, hogy az általuk kezelt adatokhoz és adathordozókhoz illetéktelenek ne juthassanak hozzá,

b) a munkájuk során tudomásukra jutott egészségügyi információkat a jogosultak kivételével senkivel nem közölhetik,

d) a titoktartási kötelezettség a közalkalmazotti jogviszony vagy munkaviszony megszűnése után is fennmarad.

7. ÉRINTETTEK (PÁCIENSEK) JOGAI

7.1. ÁTLÁTHATÓ TÁJÉKOZTATÁS JOGA

A Páciensnek alapvető joga a megfelelő, átlátható tájékoztatáshoz való jog, mely kötelezettségként az intézményt terheli. A tájékoztatást közérthető módon, ingyenesen kell megadni a Páciens részére.
Amennyiben a Páciens tájékoztatást kér, azt számára indokolatlan késedelem nélkül, de legfeljebb 30 napon belül meg kell adni.

(1) Az érintett kérelmére tájékoztatást kell adni:
a) a kezelt személyes, és egészségügyi adatairól,
b) az adatkezelés céljáról, jogalapjáról, időtartamáról,
c) kik és milyen célból kapják vagy kapták meg az adatokat,
d) az érintett adatkezeléssel kapcsolatos jogairól, jogorvoslati lehetőségeiről.

(2) Az érintett egészségügyi dokumentációval kapcsolatban jogosult:
a) a gyógykezeléssel összefüggő adatainak kezeléséről tájékoztatást kapni,
b) a rá vonatkozó egészségügyi és személyazonosító adatokat megismerni,
c) az egészségügyi dokumentációba betekinteni, valamint azokról saját költségére másolatot kapni,
d) az Intézményből történő elbocsátásakor zárójelentést /ambulánslapot kapni,
e) egészségügyi adatairól indokolt célra - saját költségére - összefoglaló vagy kivonatos írásos véleményt kapni,
f) A beteg jogosult az általa pontatlannak vagy hiányosnak vélt - rá vonatkozó - egészségügyi dokumentáció kiegészítését, kijavítását kezdeményezni, amelyet a kezelőorvos, illetve más adatkezelő a dokumentációra saját szakmai véleményének feltüntetésével jegyez rá.

(3) A beteg kórházi ellátása ideje alatt aktuálisan keletkezett dokumentációja megismerésére, azokról (saját költségre) másolat készítésére, írásban hatalmazhat fel általa megjelölt cselekvőképes személyt. A beteg életében, egészségügyi ellátásának befejezését követően csak a beteg által adott teljes bizonyító erővel rendelkező magánokiratban felhatalmazott személy jogosult az egészségügyi dokumentációba való betekintésre, és arról másolat készítésére.

Hozzáférés joga:
A hozzáférés joga alapján az Adatkezelő (Intézmény) a Páciens kérésére az adatkezelés tárgyát képező személyes adatok másolatát a Páciens rendelkezésére kell bocsátania.

Az adathordozhatósághoz való jog:
Az adathordozhatósághoz való jog alapján az Érintett (Páciens) jogosult arra, hogy a rá vonatkozó Intézmény mint Adatkezelő rendelkezésére bocsátott adatokat, tagolt széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra is, hogy ezeket az adatokat egy másik Adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az Intézmény megakadályozná.

Helyesbítéshez való jog:
Ezen jog alapján a Páciens jogosult arra, hogy kérésére az Intézmény indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes és különleges adatokat.

Elfeledtetéshez (törléshez) való jog:
Alapján a Páciens, amennyiben az adatkezelésnek más jogalapja nincsen, kérheti az Intézményben kezelt személyes és különleges adatainak törlését, továbbá az adatok kezelése nyomainak eltüntetését.

Tiltakozás joga:
Jogos érdeken alapuló adatkezelés esetén az Érintett (Páciens) írásban tiltakozhat személyes adatainak törlésére irányuló kérelme ellenére történő további adatkezelése ellen. Ebben az esetben az Intézménynek kell bizonyítani, hogy az Érintett adatainak további kezeléséhez jogos érdeke fűződik. Adatkezeléssel kapcsolatos jogainak megsértése esetén az érintett a Főigazgatóhoz, betegjogi képviselőhöz, ápolási igazgatóhoz, a Főigazgatóhoz vagy a NAIH-hoz fordulhat.

Adatkezelés korlátozásához való jog (Zároláshoz való jog):
Az Érintett jogosult arra, hogy kérésére az adatkezelő korlátozza az adatkezelést ha az alábbi feltételek közül bármelyik teljesül:

-érintett vitatja a személyes adatok pontosságát -adatkezelés

jogellenes, de az érintett ellenzi az adatok törlését
-az adatkezelőnek már nincsen szüksége a személyes adatokra adatkezelés céljából, de az érintett igényli azokat jogi igény előterjesztéséhez, érvényesítéséhez, védelméhez

-az érintett tiltakozott a jogos érdeken alapuló adatkezelés ellen, ez esetben a korlátozás addig tart amíg megállapításra nem kerül, hogy az adatkezelő jogos érdeke elsőbbséget élvez.

8. ADATVÉDELMI INCIDENS KEZELÉSE:

Adatvédelmi incidens:
Adatvédelmi incidensnek minősül a személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés vagy sérülés.

Eljárási rend adatvédelmi incidens esetén:
Az adatvédelmi incidenskezelés elsődlegesen az adatkezelő feladata, továbbá
-az incidens természetes személyek jogára és szabadságára vonatkozó kockázat alapján történő kategorizálása is, amelyet észelést követő 24 órán belül köteles jelenteni az Adatvédelmi tisztviselőnek, aki mérlegelés után gondoskodik az incidens 72 órán belüli felügyeleti hatóság felé történő jelentéséről.

Az Adatvédelmi tisztviselő intézkedést hoz:

- az incidens megszűntetésére, orvoslására
- a felelősök megállapítása
- a érintettek tájékoztatása.

Jogorvoslati lehetőségek:

Panasz jog:
Ha az Érintett természetes személy úgy ítéli meg, hogy a rá vonatkozó személyes adatkezelés nem felel meg a jogszabályi követelményeknek panaszt nyújthat be Nemzeti Adatvédelmi és Információszabadság Hatósághoz a NAIH-hoz. A NAIH döntése ellen a panaszos bírósági jogorvoslattal élhet.

Kártérítési igény:
Minden olyan személy aki az Info törvényben és a Rendeletben foglaltak megsértése következtében kárt szenved, jogosult arra, hogy követelje a vagyoni és nem vagyoni kárának megtérítését az adatkezelőtől, illetve az adatfeldolgozótól.
Az adatkezelő és az adatfeldolgozó mentesül a felelősség alól, ha bizonyítja, hogy a kárt előidéző eseményért őt semmiféle módon nem terheli felelősség.

9. INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

9.1. ADATOK ÉS PROGRAMOK VÉDELME

Az Intézet számítógépes adat-feldolgozási folyamatába kerülő információra és programokra is érvényesek az általános adatkezelési szabályok.
Az Intézetnél működő számítógépeken csak előzetesen ellenőrzött programot szabad futtatni. Az ellenőrzésnek ki kell terjednie a vásárolt vagy átvett program tesztelésére, esetleges működést akadályozó hibák felderítésére. A feltárt hiányosságokról jegyzőkönyvet kell felvenni, melyet a programot szállító szervhez haladéktalanul el kell juttatni. Hibás programot üzembe helyezni tilos.
A „Informatikai rendszerek hozzáférési szabályzatának” értelmében minden új szoftver bevezetésénél a rendszert az ott szereplő biztonsági fokozatnak megfelelő csoportok valamelyikébe be kell sorolni, és az ott szereplő követelményeknek megfelelően a hozzáférési jogosultságot ki kell osztani.
Tilos vírusellenőrzés nélkül adathordozót a számítógépbe helyezni, arról programot vagy adatot a rendszerbe tölteni!
Vásárolt programokról, vagy elektronikus formában tárolt hivatalos adatokról, amennyiben azt a licence szerződés nem tiltja, biztonsági másolatot kell készíteni, és elzártan kell tárolni.
A programok felhasználói dokumentációját a felhasználás helyén, illetve - biztonsági másolat formájában -az Informatikai Osztályon kell elhelyezni.
Feldolgozásra kerülő adatok előkészítése:

a) Számítástechnikai feldolgozásra csak tartalmilag és formailag ellenőrzött adatok kerülhetnek.
b) Az ellenőrzésért az adatfelelősség elve szerint adatlapos rögzítés esetén a z adatlapot kiállító, adatlap nélküli rögzítés esetén feldolgozást végző kijelölt adatkezelő felelős. Lehetőség szerint biztosítani kell, hogy az adatok a keletkezés helyén kerüljenek rögzítésre.

Feldolgozás folyamata

a) Az adatállományok módosítását kizárólag csak a feldolgozásra készült programmal lehet elvégezni, az arra jogosult személyek által. A rendszerekhez történő hozzáférést az 1. Melléklet szabályozza.
b) Az adatfeldolgozás során a számítógép- vagy programhibából adódó adatvesztés fordulhat elő. Ilyenkor az adatrögzítést azonnal be kell fejezni, és a további adatvesztés elkerülése érdekében az Informatikai Osztályt haladéktalanul értesíteni kell.

Mentés

a) A számítógépeken tárolt információk biztonságos megőrzése céljából az adatokat szükséges rendszerességgel menteni kell.
c) Naponta mentést kell végezni a hálózati működést biztosító központi gépen történt adatváltozásokról.
d) Egyedi gépek vagy programok esetén a mentés gyakoriságát az adott adatfeldolgozási tevékenységet felügyelő illetékes vezető határozza meg.
e) Az egyedi gépekről a mentést az egyedi gép használója, az Intézet szervergépéről a mentést a kijelölt számítástechnikai munkatárs végzi el.

Másolás

A számítógépes programok a szerzői jog szerint védelmet élveznek, ezért másolásuk, harmadik fél számára történő továbbadásuk tilos.

Törlés

Mágneses adathordozókon tárolt adatok és programok törlését csak a tevékenységet felügyelő illetékes vezető írásbeli engedélye alapján lehet elvégezni. Külön figyelmet kell fordítani az irattározási és selejtezési szabályok betartására.
Hálózati alkalmazások esetében az adatvesztés elkerülésére és az adatbiztonság fokozására személyre lebontott hozzáférési jogosultságot kell meghatározni.
A számítógépes rendszerbe történő belépés egységvezetők döntés alapján a személyes jelszón kívül a hozzáférési jogosultsággal rendelkező személyi azonosítója megadásával történhet. A belépés csak a legszükségesebb körben engedélyezhető.
A számítógépes rendszerbe való belépés engedélyezéséről az (Informatikai Osztály) nyilvántartást vezet.

9.2. SZÁMÍTÓGÉPEK, ESZKÖZÖK ÉS DOKUMENTÁCIÓK VÉDELME

A számítógépek és eszközök rendeltetésszerű használatáért a személyi leltár szerint a használatra kijelölt adatkezelő felelős.
A hálózati működő számítógépeken kizárólag az erre kiképzett szakemberek dolgozhatnak.
Meghibásodás megelőzéséről folyamatos karbantartással kell gondoskodni, üzemzavar esetén a javítást csak arra kiképzett szakember végezheti.
Fizikai sérülések megelőzésére (pl.: hálózati vezetékszakadás) a számítógépet telepítési helyéről elmozdítani, vagy áthelyezni nem szabad.
Vagyonvédelmi megfontolásból az adatkezelő köteles a munkaidő végzetével a számítógépet kikapcsolni, az azok elhelyezésére szolgáló irodahelységet bezárni. Az Intézményből javításra, vagy más célból elszállítani eszközöket csak bizonylatolás után lehet.

9.3. MÁGNESES ADATHORDOZÓK VÉDELME

A mágneses adathordozók védelmére és azonosítására az adathordozókat azonosítóval (címkével) kell ellátni, és azokról nyilvántartást kell vezetni.
A mentést tartalmazó adathordozók megőrzési idejét úgy kell meghatározni, hogy azokról az aktuális adatállomány sérülés esetén visszaállítható legyen.

Vírust tartalmazó, nem mentesíthető adathordozót használatban tartani nem lehet. Az adathordozót óvni kell a szennyeződésektől és a fizikai sérüléstől, ezért használat közben óvakodni kell a mágnesezhető réteg megérintésétől, használat után, pedig zárható dobozban, vagy a gyári csomagolásban elektromos erőterektől távol (monitor, televízió, hangszóró, ventilátor, telefon, rádió, stb.) kell tartani.

10. ELEKTRONIKUS MEGFIGYELŐRENDSZER (KAMERA) HASZNÁLATA

Az elektronikus megfigyelőrendszerek alkalmazása szempontjából nincs szükség a munkavállaló hozzájárulására.
Az elektronikus megfigyelőrendszerrel kapcsolatos adatkezelést **be kell jelenteni az adatvédelmi nyilvántartásba**. Amennyiben a munkáltató vagyonőrt alkalmaz, akkor adatkezelőként őket is terheli a bejelentési kötelezettség.

10.1. A KAMERÁK HASZNÁLATÁNAK CÉLJA, KORLÁTAI

- Elektronikus megfigyelőrendszert elsődlegesen az emberi élet, testi épség, személyi szabadság védelme, a veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme, valamint vagyonvédelem, parkolóhasználat ellenőrzése céljából lehet alkalmazni.
- Nem lehet olyan kamerát elhelyezni, amely kizárólag egy dolgozót és az általa végzett tevékenységet figyeli meg. Nem lehet kamerát elhelyezni olyan helyiségben, amelyben a megfigyelés az emberi méltóságot sértheti, így különösen az öltözőkben, zuhanyzókban, az illemhelyiségekben vagy kórházi kórteremben, orvosi szobában, illetve az ahhoz tartozó váróban, illetve a közalkalmazottak munkaközi szüneténekeltöltése céljából kijelölt helyiségekben.
- A munkáltató az elektronikus megfigyelőrendszert kizárólag a saját tulajdonában (vagy a használatában) álló épületrészek, helyiségek és területek, illetőleg az ott történt események megfigyelésére alkalmazhatja.

10.2. A RÖGZÍTETT FELVÉTELEK TÁROLÁSÁNAK IDŐTARTAMA ÉS INDOKLÁSA

- A rögzített felvételeket főszabályként három munkanapig lehet tárolni. A munkáltatónak igazolnia kell azt, hogyha valamely munkakör betöltése olyan kivételes esetet jelent, amely esetén a felvételeket három munkanapnál hosszabb időtartamig szükséges megőrizni.
- A felvételek megtekintésére kizárólag az alábbi személyek jogosultak:
    - főigazgató
    - ágazati igazgatók

10.3. A RÖGZÍTETT FELVÉTELEK MEGTEKINTÉSÉNEK, TOVÁBBÍTÁSÁNAK INDOKA

- A felvételek megtekintésének indoka kizárólag rendkívüli esemény jelentése, vagy törvényben meghatározott esetekben bírósági, illetve hatósági megkeresés lehet, mely a célhoz kötöttség elvén alapuló rögzített felvételekkel igazolhatók. A megtekintésre kizárólag az előző pontban felsorolt jogosultak köre hivatott, illetve adhat utasítást arra vonatkozóan.
- Bíróság vagy más hatóság megkeresésére a rögzített felvételt részükre haladéktalanul meg kell küldeni.
- Az informatikai osztályvezető a rendszer működését technikailag köteles felügyelni.
- Amennyiben a rögzített felvételek megtekintése szükségessé válik, az adatokat megismerő személy nevét és a megismerés indokát és idejét rögzíteni kell. Erre a célra alkalmas az Adattovábbítási nyilvántartás, melyet az Informatikai Osztályon vezetnek.

10.4. TÁJÉKOZTATÁS MEGFIGYELŐ RENDSZER ALKALMAZÁSÁRÓL

A munkáltatónak az elektronikus megfigyelőrendszer alkalmazására vonatkozó tájékoztatóban minden egyes kamera vonatkozásában pontosan meg kell jelölnie, hogy az adott kamerát milyen célból helyezte el az adott területen és milyen területre, berendezésre irányul a kamera látószöge. Általánosságban tett tájékoztató nem fogadható el.

(1) A közalkalmazottak írásbeli tájékoztatása megfigyelő rendszer alkalmazásáról:

- A munkáltatónak gondoskodnia kell arról is, hogy a közalkalmazottakat az elektronikus megfigyelőrendszerrel kapcsolatban megfelelően írásban tájékoztassa, s a közalkalmazott ezt írásban ellenjegyezze.
- A munkáltató köteles továbbá figyelemfelhívó jelzést elhelyezni arról a tényről, hogy az adott területen elektronikus megfigyelőrendszert alkalmaznak
- Az Intézmény területén kizárólag vagyonvédelem céljából szükséges a megfigyel ő kamerák működtetése. A megfigyelés zártláncú rögzített felvételek formájában történik.
- A megfigyelő kamerák működése nem minden esetben 24 órás. Egyes területeken, folyosókon, ahol meghatározott időpontban betegek, hozzátartozók, várakozók is tartózkodhatnak, a rögzítés a munkaidőn kívüli időszakokra korlátozódik.
- A megfigyelőrendszer üzemeltetője az Intézmény.
- A rögzített felvételek tárolása az Informatikai Osztály egy kijelölt szerverén történik.
- A rögzített felvételek tárolásának időtartama: 3 munkanap
- A rögzített felvételek fizikai biztonságát az Informatikai Osztály garantálja.
- Az adatok megismerésére a 66.) pontban felsorolt döntési joggal rendelkező vezetők jogosultak.

Adattovábbítás csak és kizárólag törvényi előírásoknak megfelelően történhet.

(2) Betegek, látogatók, várakozók írásbeli tájékoztatása a megfigyelő rendszer alkalmazásáról:

- Jól látható helyen és jól olvasható módon tájékozódást elősegítő figyelemfelhívó jelzést kell elhelyezni arról a tényről, hogy az adott területen megfigyelőrendszert alkalmaznak.

- A tájékoztatásnak ki kell térnie
  - az adatkezelés céljára
  - az adatkezelés jogalapjára.
  - felvétel tárolásának helyére, időtartamára
  - a rendszert alkalmazó (üzemeltető) személyére
  - az adatok megismerésére jogosultak körére
  - jogérvényesítés és jogsérelem esetén igénybe vehető eljárásokra.

10.5. A MEGFIGYELŐ RENDSZEREK ALKALMAZÁSÁNAK MÓDJAI, JOGÉRVÉNYESÍTÉS

(1) Alkalmazási módok:

D zártláncú rögzített felvételekkel

D kijelölt személy(ek) által folyamatosan megfigyelt nem rögzített alkalmazás D kijelölt személy(ek) által folyamatosan megfigyelt és rögzített

(2) Jogérvényesítés információs önrendelkezési jog megsértése esetén:

- A megfigyelő kamerák használatával kapcsolatos panasz bejelentése, észrevétel jelzése történhet az intézmény főigazgatójához. Betegeink ezen túlmenően panaszbeadványukkal fordulhatnak a Betegjogi képviselőhöz is. A személyes és egészségügyi adatok kezelésével kapcsolatos panasztétel szabályait az intézmény panaszkezelés tárgyú belső szabályzata tartalmazza.
- Akinek a jogát, jogos érdekét érinti a rögzített felvétel (kép- vagy hangfelvétel), az kérheti 3 munkanapon belül, hogy az adat kezelője azt ne semmisítse meg (feltéve, hogy igazolja jogát vagy jogos érdekét). Ha ilyen kérés az őrzési időn belül nem érkezik, akkor a felvételek törlése megtörténik.

11. AZ INFORMATIKAI RENDSZER VÉDELMÉNEK ÁLTALÁNOS SZABÁLYAI

Az Intézményben alkalmazott informatikai rendszereket védelmi szempontból az alábbi biztonsági csoportokba kell sorolni:

- „D” csoport: minimális védelem
- „C” csoport: szelektív és ellenőrzött védelem
- „B” csoport: kötelező és ellenőrzött védelem
- „A” csoport: bizonyított védelem

<u>„D” biztonsági csoport:</u>

Biztonsági szempontból elenyésző kockázatú adatok, informatikai rendszerek csoportja.

<u>„C” biztonsági csoport:</u>

Ez a személyes adatok, pénzügyi adatok, illetve az Intézmény belső szabályozásában hozzáférési korlát alá eső és nyílt adatok feldolgozására, tárolására alkalmas rendszerek biztonsági csoportja.

„B” biztonsági csoport:

Betegadatok, valamint a nem minősített adatok közül a különleges személyi adatok, nagy tömegű személyes adatok feldolgozására, tárolására alkalmas rendszerek biztonsági csoportja.

„A” biztonsági csoport:

Az államtitok, katonai szolgálati titok, stb. feldolgozására, tárolására alkalmas rendszerek biztonsági csoportja.

Intézményünknél alkalmazott informatikai rendszerek biztonsági besorolását a 5. fejezet tartalmazza. Mivel „A” besorolású rendszerünk nincs, a „D”-re pedig nincsenek biztonsági előírások, a továbbiakban csak az „C” és a „B” biztonsági csoportokra vonatkozó követelményeket ismerteti ez a szabályzat.

11.1. „C” BIZTONSÁGI CSOPORT KÖVETELMÉNYEI

- Az azonosítás és hitelesítés keretében a hozzáférést jelszavakkal kell ellenőrizni. A jelszómenedzselést úgy kell biztosítani, hogy a jelszó ne juthasson illetéktelenek tudomására, ne legyen könnyen megfejthető, megkerülhető.
- A felhasználó azonosítása egyedi, jellemző, ellenőrizhető s hitelesítésre alkalmas legyen.
- Biztosítani kell a felhasználói azonosítók időszakos vagy végleges tiltását.
- A felhasználók közé sorolandók a természetes személyek, folyamatok vagy egyéb eszközök.

A hitelesítés legáltalánosabb módja a jelszó megadása. Kezelésére az alább szabályokat kell alkalmazni:

- A munkaállomásokon a hitelesítési folyamatban a beírt jelszó összefüggő szövegként ne legyen olvasható.
- A jelszó és a felhasználó azonosító soha nem kerülhet egy postai küldeménybe, még elektronikus levelezésben sem.

A felhasználói jelszavakkal kapcsolatban biztosítani kell az alábbi követelményeket:

- minimális jelszóhossz megadása,
- a jelszó egyedisége,
- a jelszó maximális élettartamát,
- a jelszó zárolását,
- a jelszóképzés szabályainak meghatározását.

A rendszer felhasználóihoz hozzáférési jogokat kell rendelni. A jogokat egyedi, illetve csoporttulajdonosi szinten kell megadni, amelyek az alábbiak lehetnek:

- olvasási jog (betekintés)
- írási jog (létrehozás, módosítás)
- törlési jog.

A hozzáférési események esetén jogosultság-ellenőrzést kell végrehajtani.

A hozzáférés-vezérlés a felhasználókhoz rendelt jogok és az objektumokhoz rendelt tulajdonságok és jogok összevetése alapján történik.

A jogosultsági rendszernek támogatni kell a jogosultságok módosítását, átadását másik személynek, törlését és időleges korlátozását.

Új jogosultság kiosztását, jogosultság törlését vagy átmeneti felfüggesztését csak erre felhatalmazott rendszergazda végezheti el.

11.2. „B" BIZTONSÁGI CSOPORT KÖVETELMÉNYEI

Ez a biztonsági csoport magában foglalja a „C" osztály követelményeit, de ezen túlmenően, további megszorításokat tartalmaz:

A felhasználóhoz olyan biztonsági „címke" van rendelve, amely meghatározza, hogy az adott személy milyen biztonsági szintű adatokhoz és mely adatcsoportokhoz férhet hozzá.

Olyan regisztrálási és naplózási rendszert kell kialakítani, amely lehetővé teszi, hogy utólag meg lehessen állapítani az informatikai rendszerben bekövetkezett fontosabb eseményeket.

12. INFORMATIKAI RENDSZEREK BIZTONSÁGI BESOROLÁSA

12.1. BESOROLÁSA: „D" BIZTONSÁGI CSOPORT.

Az Intézményünknél a munkaállomásokon Windows alapú vegyes operációs rendszer működik (Win XP, Win 2000, stb), ezért ezek biztonsági szempontból nem szabályozottak.

Az operációs rendszerekért felelős rendszergazda feladata a gépek felhasználók általi folyamatos elérésének biztosítása, ezét, amennyiben ez lehetséges minden gépnek rendelkeznie kell egy rendszergazdai jelszóval, amellyel bármilyen beavatkozás elvégezhető. A felhasználók részére az operációs rendszer paraméterezésének, szoftver telepítésének lehetőségét minimálisra kell korlátozni.

12.2. OPERÁCIÓS RENDSZEREK (NOVELL, LINUX, MS SERVER)

Besorolása: „C" biztonsági csoport.

Felhasználók a szerverek eléréséhez közvetlenül nem rendelkezhetnek jogokkal. A szerveren tárolt adatokhoz, szoftverekhez, illetve a szerverek, szoftverek paramétereihez nem férhet hozzá. Azokba nem tekinthet be, nem végezhet módosításokat, vagy törléseket.

A felhasználóknak a szerverekhez való hozzáférése a részére megengedett felhasználói program eléréséhez, használatához szükséges minimális szintig engedélyezet.

Minden szervernek külön-külön ki kell alakítani egy rendszergazdai hozzáférést, amely lehetővé teszi a szerverek, vagy azokon futó programok menedzselését, paraméterezését, teljes körű hozzáférését. Ennek jelszavát csak a munkaköri leírásukban kijelölt informatikai dolgozók ismerhetik, illetve módosíthatják.

Az aktuális jelszavakat az Informatikai Osztályon váratlan helyzetek esetére zárt borítékban, elzárt helyen kell tárolni. Az elzárt jelszó aktualitásáért a mindenkori rendszergazda felel.

12.3. MEDWORKS KÓRHÁZI INFORMATIKAI RENDSZER (ORACLE ADATBÁZIS KEZELŐ)

Besorolása: „B" biztonsági csoport.

A program beteg- és személyes adatok nyilvántartását, kezelését nagy mennyiségben végzi, ez indokolja a szigorúbb, „B" besorolást.
A programrendszer nagyon komoly biztonsági rendszerrel ellátott, külön védelmi modullal (Guard) rendelkezik. Ez a modul szabályozza az adatok és az alkalmazások hozzáférhetőségét, és ez által védi is azokat. Saját felhasználói adatbázis alkalmazásával a rendszerben való feladatkörök ellátásának jogai felhasználónként különbözhetnek.
A bejelentkezéskor a felhasználói név és jelszó alapján a rendszer felismeri a felhasználót, és a megfelelő jogosultságok birtokában engedélyezi, hogy a felhasználó által elérhető, feldolgozhatóak legyenek az adatok. A rendszer a biztonsági szintjének megfelelően, az összes munkavégzést naplózza.
A védelmi rendszer kizárólag, a munkaköri leírásában is rögzített, kiemelt jogkörrel rendelkező Informatikai Osztály munkatársai, illetve rendszergazda részére érhető el.
A felhasználók jogai megadhatok egyedileg és csoportosan. A csoportos jogadáshoz kialakításra kerültek jogosultsági csoportok, amelyek módosíthatók, vagy szükség estén továbbiak hozható létre.
A jogosultsági csoport szabályozza, hogy a csoportba tartozó felhasználó, mely modulhoz, és azon belül milyen funkciókat végezhetnek.
Új jogosultsági csoportok létrehozását, vagy a meglévők módosítását csak a kijelölt rendszergazda végezheti. Felhasználók jógait, a követhetőség miatt, egyedileg változtatni tilos.
Mivel egy felhasználó is több jogosultsági csoportba tartozhat, tartozik is, szükséges felhasználó csoportok definiálása, ami az azonos jogosultsági csoportokhoz tartozó felhasználókat fogja össze.
A felhasználó csoportokról elektronikus formában kell nyilvántartást vezetni, amelynek tartalmaznia kell a felhasználó csoport kódját, megnevezését és a hozzájuk rendelt jogosultsági csoport kódjait.
A nyilvántartás mindenkori aktualizálásáért a terület rendszergazdája felel.
Az egyes felhasználók egységekhez, és felhasználó csoporthoz történő rendelésével a programrendszeren belüli hozzáférése pontosan szabályozott. Ennek megadása az egységvezető feladata, amelyet a „Jogosultság bejelentőlap"-on tesz meg, és aláírásával igazol.

Az informatika arra kijelölt munkatársa e dokumentum alapján beállítja a felhasználó jogokat, és ennek megtörténtét aláírásával igazolja. A „Jogosultság bejelentőlap" és a programban jogosultsága közötti összhang megteremtéséért a terület rendszergazdája felel.

12.4. INTEGRÁLT GAZDASÁGI RENDSZER

Besorolása: „C” biztonsági csoport.
A szoftver több önálló programból áll, ahol programonként és az egyes programok menüpontjai rendelhetők az egyes felhasználókhoz.

A gazdasági terület rendszergazdája végzi a felhasználói jogosultságváltozások átvezetését a rendszerben.

12.5. IRODAI ALKALMAZÁSOK ÉS EGYÉB ÁLTALÁNOS CÉLÚ SZOFTVEREK (GRAFIKA, STB.)

Besorolása: „D” biztonsági csoport.
Ezen szoftverek hozzáférését e szabályzat nem korlátozza, de az általuk készített elektronikus dokumentációk az informatikai egység által meghatározott szerveren kell elhelyezni, amelynek adatvédelmét a szerver nyújtotta védelmi rendszerrel kell védeni. Munkaállomásokon védendő dokumentum nem helyezhető el.

12.6. ALKALMAZOTTAK JOGOSULTSÁGÁNAK KEZELÉSE

Az alkalmazottak jogosultágának napra készen tartásáért az Informatikai Osztályvezető helyettese a felelős.

A rendszeradminisztrátori tevékenységet az egyes terület rendszergazdája látja el, a területükhöz kapcsolódó szoftverek szerint:

a. / orvosi terület rendszergazdája:
MedWorks kórházi informatikai rendszer

b. / gazdasági terület- és egyéb szoftverek rendszergazdája:
EcoStat integrált gazdasági rendszer
Linux hálózati operációs rendszer
Munkaállomások operációs rendszerei

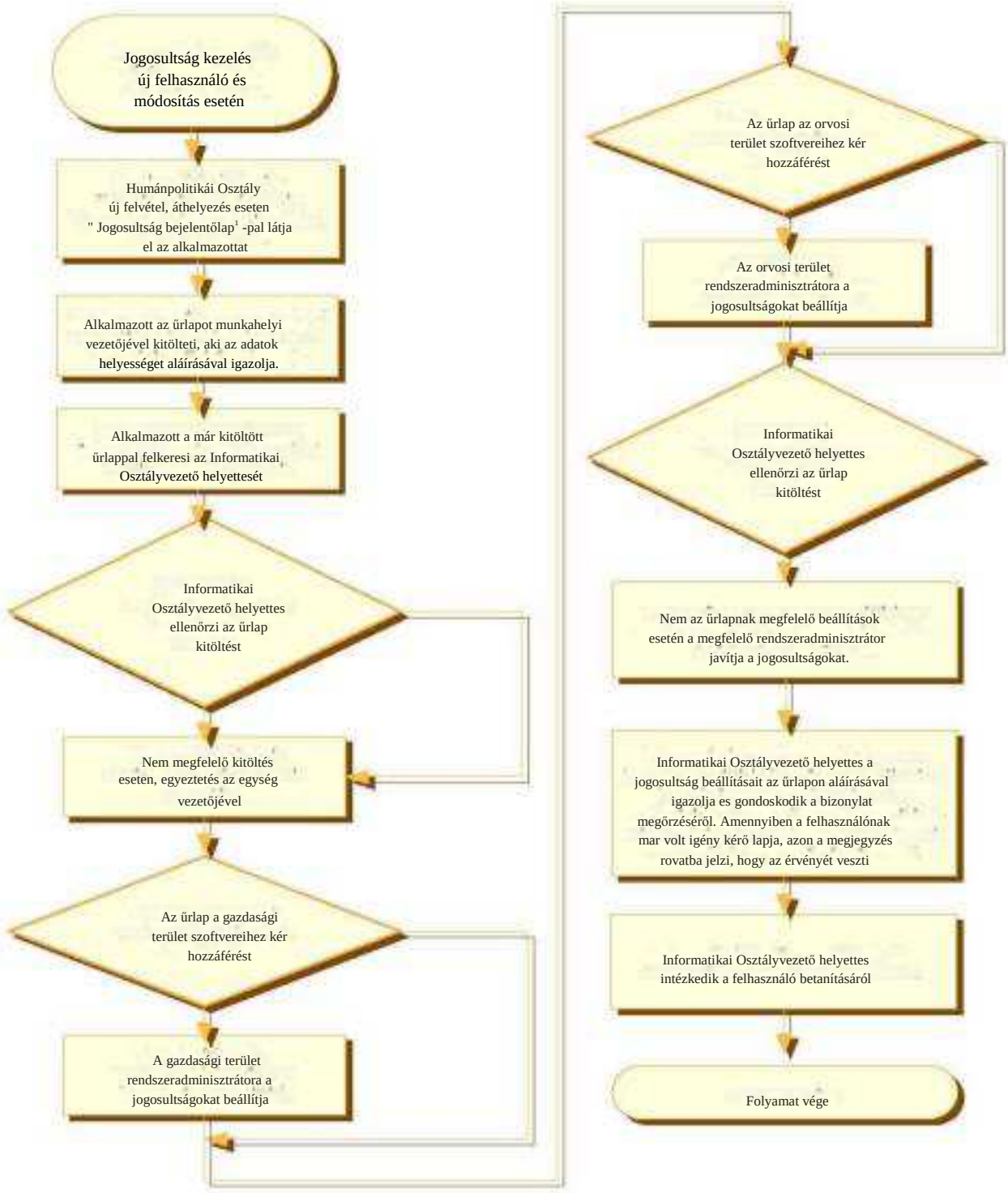
A felhasználó jogosultság változtatás (új felvétel, áthelyezés, kilépés, stb.) ügyvitelének folyamatábrája 1. ábrán látható.

Az ábrának megfelelően felhasználók jogosultságait a munkahelyi vezető határozzák meg, és ezt a „Jogosultság bejelentőlap”-on rögzíti, az Informatikai Osztály ez alapján végzi el a szükséges beállításokat.

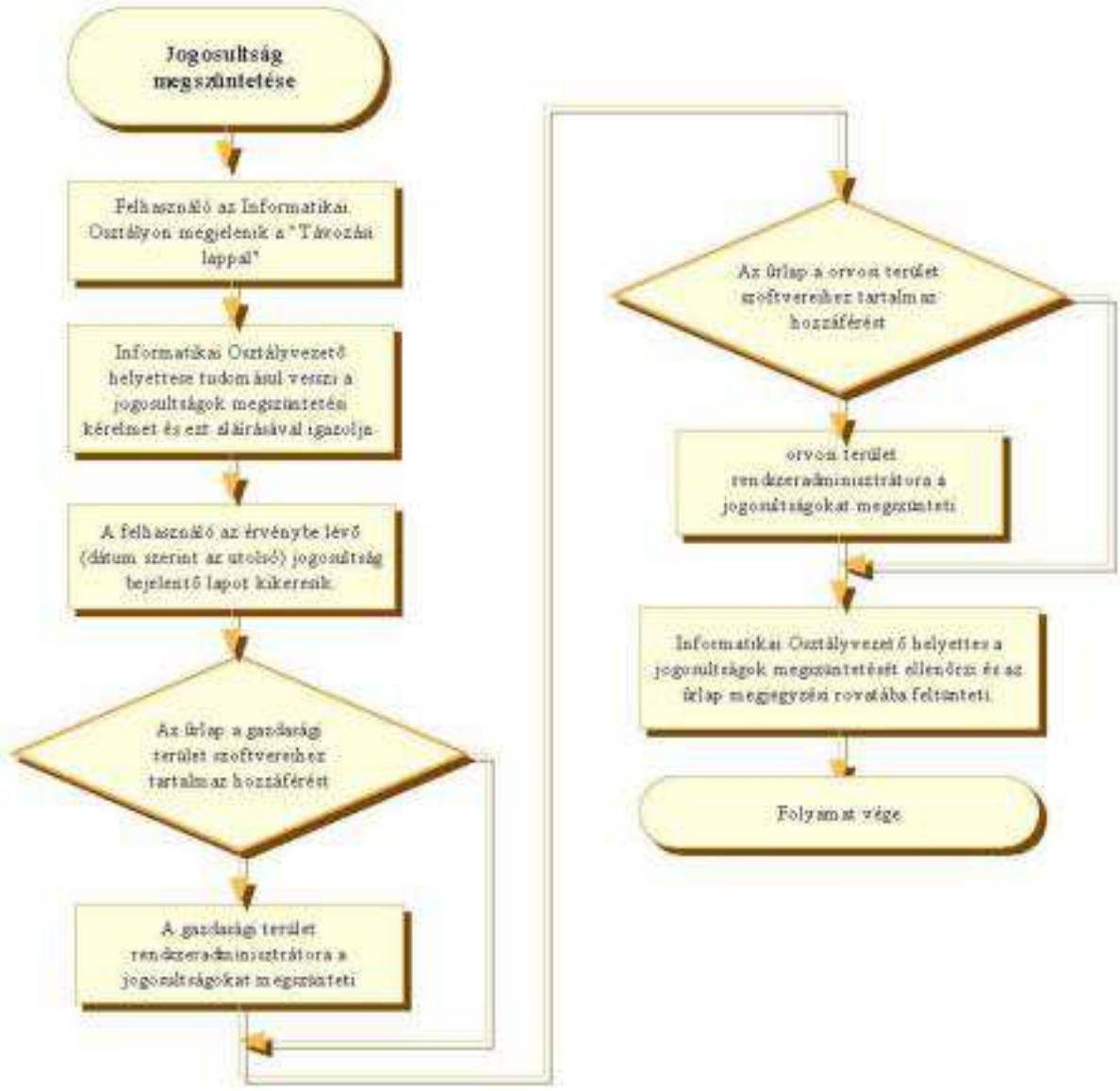
A bizonylaton kitöltendők: az illető személyes adatai, megjelölendők azon rendszerek, amelyhez hozzáférési jogot kell biztosítani, illetve kórházi rendszer esetén a mely egységekre terjedjenek ki a jogok.

Új felvételizőnél a Bér- és Munkaügyi Osztály a „Felvételi lap”-hoz automatikusan mellékel a „Jogosultság bejelentőlap”-ot, egyéb esetekben az Informatikai Osztálytól szerezhető be.

A kitöltött, munkahelyi vezető által aláírt űrlapot, az Informatikai Osztályra eljuttatják, ahol az Informatikai osztályvezető helyettese intézkedik az űrlapon kért jogosultságok adminisztrálásának elvégzéséről, majd annak elkészültét ellenőrzi. Intézkedik, a felhasználók betanításáról, gondoskodik az űrlapok felhasználónkénti megőrzéséről. A folyamat eredményes lezárását aláírásával igazolja.


Jogosultság kezelés
új felhasználó és
módosítás esetén
Humánpolitikai Osztály
új felvétel, áthelyezés eseten
" Jogosultság bejelentőlap[1] -pal látja
el az alkalmazottat
Alkalmazott az űrlapot munkahelyi
vezetőjével kitölteti, aki az adatok
helyességet aláírásával igazolja.
Alkalmazott a már kitöltött
űrlappal felkeresi az Informatikai
Osztályvezető helyettesét
Informatikai
Osztályvezető helyettes
ellenőrzi az űrlap
kitöltést
Nem megfelelő kitöltés
eseten, egyeztetés az egység
vezetőjével
Az űrlap a gazdasági
terület szoftvereihez kér
hozzáférést
A gazdasági terület
rendszeradminisztrátora a
jogosultságokat beállítja
Az űrlap az orvosi
terület szoftvereihez kér
hozzáférést
Az orvosi terület
rendszeradminisztrátora a
jogosultságokat beállítja
Informatikai
Osztályvezető helyettes
ellenőrzi az űrlap
kitöltést
Nem az űrlapnak megfelelő beállítások
esetén a megfelelő rendszeradminisztrátor
javítja a jogosultságokat.
Informatikai Osztályvezető helyettes a
jogosultság beállításait az űrlapon aláírásával
igazolja es gondoskodik a bizonylat
megőrzéséről. Amennyiben a felhasználónak
mar volt igény kérő lapja, azon a megjegyzés
rovatba jelzi, hogy az érvényét veszti
Informatikai Osztályvezető helyettes
intézkedik a felhasználó betanításáról
Folyamat vége

1. Ábra



2. Ábra

Kilépés esetén a felhasználó felkeresi „Távozási lap”-pal az Informatikai Osztályt, ahol az osztályvezető helyettes a bizonylatot aláírja, és intézkedik a felhasználó jogosultságainak megszüntetéséről. Megkeresi a felhasználó aktuális (dátum szerint az utolsó) „Jogosultság bejelentőlap” (3. ábra) űrlapját, annak értelmében a megfelelő szoftvereknél a rendszeradminisztrátorral visszavonatja a jogosultságot, majd aláírásával ezt igazolja a megjegyzés rovatban.

13. HIVATKOZÁSOK

E szabályzat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény, valamint az egészségügyi és hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII tv, illetve az egészségügyi és hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről szóló 62/1997. NM rendelet alapján készült.

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

14. MÓDOSÍTÁSI ELJÁRÁSOK

A szabályzat a ME 01 „Minőségirányítási Kézikönyv: Dokumentumok és feljegyzések kezelése, dokumentált információ” című eljárások szerint módosítható.

15. MELLÉKLETEK

1.sz. melléklet	Számítógépes hozzáférési jogosultságok kiadásának és nyilvántartásának rendje
2.sz. melléklet	Fertőző betegségek listája az érintett részéről történő kötelező adatszolgáltatás, valamint az egészségügyi államigazgatási szerv részére történő kötelező adattovábbítás esetén
3.sz. melléklet	Szűrő- és alkalmassági vizsgálatok
4.sz. melléklet	Nyilatkozat adatkezelés tiltásáról
5.sz. melléklet	Adatvédelmi felelős megbízás

1.sz. melléklet

SZÁMÍTÓGÉPES HOZZÁFÉRÉSI JOGOSULTSÁGOK KIADÁSÁNAK ÉS NYILVÁNTARTÁSÁNAK RENDJE

JOGOSULTSÁG BEJELENTŐLAP

Felhasználó neve: .....

Szervezeti egység ..... Rendszerfelhasználó név : .....

☐ Integrált gazdasági rendszer ☐ Főkönyv ☐ Pénzügy ☐ Raktár ☐ Munkalap ☐ Leltár ☐ Tárgyi eszköz ☐ Osztályos igénylés ☐ Intézeti elbírálás ☐ Letéti ☐ Cashflow ☐ Költségvetés tervező ☐ Kötelezettség vállalás ☐ Rendelés ☐ Élelmezés ☐ Ebédjegy ☐	☐ Orvosi rendszer moduljai ☐ Orvos ☐ Asszisztens ☐ Adminisztrátor ☐ Nővér ☐ Műtő ☐ Gyógytornász ☐ Betegfelvételi ☐ Vendég ☐ Ügyelet ☐ Rendszergazda ☐ Transzfúziológia rendszer ☐ Iktató rendszer ☐ Levelezés	Jogosultság igénylés az alábbi munkahely(ek)re: _____ _____ _____ _____ _____ _____ ☐ Bér nyilvántartó rendszer ☐ Munkaügyi rendszer ☐ Kontrolling ☐ Jogtár

Megjegyzés: .....

Érvényesség kezdete:

20..... ....

Igénylő egység vezetője Jogosultság kezelésért felelős

Megjelölt modul oktatásán részt vettem: .....

csak új felvétel esetén választható szabadon, ekkor is csak abban az esetben adható, ha még nem lett kiosztva a rendszerekbe. Egyébként a már érvényes felhasználó nevett kell megadni. **NEM LEHET BENNE SZÓKÖZ, ÉKEZETES- ÉS KÜLÖNLEGES KARAKTER.**

2. sz melléklet

Fertőző betegségek listája az érintett részéről történő kötelező adatszolgáltatás, valamint az egészségügyi államigazgatási szerv részére történő kötelező adattovábbítás esetén

A) Személyazonosító adatokkal együtt jelentendő:

1. Acut flaccid paralysis
2. Ancylostomiasis
3. Anthrax
4. Botulizmus
5. Brucellosis
6. Campylobacteriosis
7. Cholera
8. Congenitalis rubeola syndroma
9. Cryptosporidiosis
10. Diphtheria
11. Dysenteria (shigellosis és amoebiasis)
12. Dyspepsia coli
13. Egyéb E. coli által okozott megbetegedés
14. Echinococcosis
15. Encephalitis infectiosa (kullancsenc. és egyéb)
16. Enteritis infectiosa
17. Febris flava
18. Febris recurrens
19. Fertőző spongiform encephalopathiák:
    - Creutzfeldt-Jacob-betegség (CJB)
    - Variáns Creutzfeldt-Jacob-betegség (vCJB)
20. Giardiasis
21. Hepatitis infectiosa (fertőző májgyulladás)
22. Hepatitis A
23. Hepatitis B
24. Hepatitis C
25. Hepatitis E
26. Delta-hepatitis
27. Keratoconjunctivitis epidemica
28. Legionellosis
29. Lepra
30. Leptospirosis
31. Listeriosis
32. Lyme-kór (a kijelentés csak szövődmény előfordulása, valamint halálos kimenetel esetén kötelező)
33. Lyssa
34. Madárinfluenza

35. Malaria
36. Malleus
37. Meningitis purulenta
38. Meningitis serosa
39. Mononucleosis infectiosa
40. Morbilli
41. Multirezisztens kórokozók által okozott, egészségügyi ellátással összefüggő fertőzés
42. Nosocomialis véráramfertőzés (nosocomialis sepsis)
43. Ornithosis
44. Paratyphus
45. Parotitis epidemica
46. Pertussis
47. Pestis
48. Poliomyelitis anterior acuta
49. Q-láz
50. Rubeola
51. Salmonellosis
52. Scarlatina (a kijelentés csak szövődmény előfordulása, valamint halálos kimenetel esetén kötelező)
53. Súlyos akut légúti tünetegyüttes (SARS)
54. Schistosomiasis
55. Staphylococcosis
56. Strongyloidosis
57. Taeniasis
58. Tetanus
59. Toxoplasmosis
60. Trachoma
61. Trichinellosis
62. Tularemia
63. Typhus abdominalis
64. Typhus exanthematicus
65. Varicella (a kijelentés csak szövődmény előfordulása, valamint halálos kimenetel esetén kötelező)
66. Variola
67. Vírusos haemorrhagias lázak
68. Yersiniosis

B) Személyazonosító adatok nélkül jelentendő:

1. AIDS megbetegedés
2. HIV-fertőzés

3. sz melléklet

Szűrő- és alkalmassági vizsgálatok

1. Munkaköri, szakmai, egészségi alkalmassági orvosi vizsgálatok (előzetes, időszakos, soron kívüli, záró).

2. Szűrővizsgálatok - beleértve a biológiai monitorozási vizsgálatokat is - a foglalkozással összefüggő megbetegedések felderítésére.

3. A katonai egészségi alkalmasság, valamint az egyéb szolgálati viszony létesítéséhez szükséges egészségi alkalmasság megállapításához kapcsolódó szakorvosi vizsgálatok.

4. A közúti járművezetés engedélyezéséhez szükséges orvosi vizsgálatok.

5. A kézi lőfegyverek, lőszerek, gáz- és riasztófegyverek megszerzéséhez és tartásához szükséges orvosi vizsgálatok.

6. Az iskolai előkészítés, a tankötelezettség és képzési kötelezettség megállapításával kapcsolatban a látás-, hallás-, értelmi fejlődési, beszédfejlődési képességek, illetve más rendellenességek vizsgálata.

4.sz. melléklet

NYILATKOZAT ADATKEZELÉS TILTÁSÁRÓL

Alulírott:.....(szül.idő:
anyja neve: .....).

Az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. Törvényben foglalt adattovábbítással kapcsolatos jogaimról való tájékoztatást követően - cselekvőképességem teljes birtokában - megtiltom, hogy betegségemmel összefüggésbe hozható, gyógykezelésem érdekében fontos egészségügyi adataimat továbbítsák a kórházi egészségügyi hálózaton belül. Döntésemet annak egészségi állapotomra esetlegesen kiható következményei tudtában hoztam.
Tájékoztattak arról, hogy ezt a tiltó nyilatkozatot mindennemű alaki kötelezettség nélkül bármikor visszavonhatom, visszavonásomat azonban ezen nyilatkozaton írásban meg kell erősítenem.

Kelt:

aláírás

5.sz. melléklet

MEGBÍZÁS

Név:_____,osztály dolgozóját a mai naptól megbízom az_____

Egység **adatvédelmi felelős** feladatainak ellátásával.

Feladatai:

- Gondoskodik az egységen belül az adatvédelmi szabályok betartásáról, oktatást tart éves szinten az egységen belül az adatvédelmi kérdésekről.
- Minden év végén írásos beszámolót készít az előző év adatvédelméről.
- Nyilvántartja a kötelező és hivatalos adatszolgáltatási kötelezettségeket és gondoskodik azok előírásszerű teljesítéséről.
- Érvényesíti a betegek adatvédelmi jogaik megismerésének lehetőségét és gyakorlásának feltételeit.
- Kapcsolatot tart az ellátási területen dolgozó orvosokkal a korszerű és biztonságos adatcsere elősegítése céljából.
- Ellenőrzi az orvosi titok megtartását.
- Ellenőrzi a szabályzatok betartását, az aláírás minták vezetését.
- Figyelemmel kíséri az egység egységben történő valamennyi adatkezelést az adatvédelmi szabályzat betartásának szempontjából.
- Betartja és betartatja az eljárás- rendet adatvédelmi incidens esetén. Adatvédelmi vagy információbiztonsági incidensek esetén haladéktalanul jelzi azokat az Adatvédelmi Tisztviselőnek
- Javaslatot tesz az Adatvédelmi tisztviselőnek az adatvédelem betartása érdekében szükséges intézkedésekre.
- Joga van betekinteni az adatvédelemmel kapcsolatos minden szóba jöhető iratba és dokumentációba.
- Felméri és figyelemmel kíséri az osztályon történő valamennyi adatkezelési folyamatot az adatvédelmi szabályzat előírásainak megfelelően. Felméri és naprakészen tartja az osztályos adatvagyon leltárt. Az osztályon történő adatkezelés során az érintetteknek tájékoztatást ad az érvényes adatvédelmi szabályokról

Jelen megbízás visszavonásig érvényes.

Ajka, dátum: _____

_____
Adatvédelmi Tisztviselő

Az egyedi megbízásban foglaltakat megértettem és magamra nézve kötelezőnek elismerem.

_____

Adatvédelmi felelős

Kapják:
Címzett
Irattár