A példány sorszáma:

SZ 04
ADATVÉDELMI ÉS ADATBIZTONSÁGI SZABÁLYZAT

Készítette:

VFK Data Pro. Kft.
dr. Vida András
Ügyvezető

Minőségügyi szempontból átvizsgálta:

Endrédi Ildikó
minőségügyi vezető

Jóváhagyta és a kiadást elrendelte:

Dr. Nagy András Csaba PhD
Főigazgató Főorvos

1. A Szabályzat célja

1.1 A Szabályzat elkészítésének célja

Az Adatvédelmi és Adatbiztonsági Szabályzat (továbbiakban: Szabályzat) a Zuglói Egészségügyi Szolgálat (a továbbiakban: Intézmény) egészségügyi és azokhoz kapcsolódó személyes adatok kezelésére vonatkozó egységes, fenntartható és folyamatosan fejleszthető elvrendszerének és gyakorlatának biztosítása érdekében készült.

A Szabályzat célja, hogy biztosítsa:

- az Intézmény mindennapi tevékenysége során végzett munkavégzés mellett a személyes adatok védelméhez fűződő információs önrendelkezési jog érvényesülését;
- az Intézmény által kezelt személyes adatok jogosulatlan felhasználásának megakadályozása érdekében meghatározza a személyes adatok kezelése során irányadó adatvédelmi és adatbiztonsági előírásokat.
- a személyes adatok védelméhez fűződő jog érvényesülését, a személyes adatok védelme elveinek érvényesülését,
- az Intézmény szervezeti egységeinél vezetett, személyes adatokat tartalmazó nyilvántartások vezetésének és működtetésének jogszerű rendjét,
- az adatbiztonsági követelmények (technikai és szervezési intézkedések) érvényesülését.

A Szabályzat meghatározza az Intézmény adatvédelmi tevékenysége irányításában és ellátásában résztvevő szervezeti egységeknek és személyeknek az adatkezelési tevékenységek ellátása során ellátandó feladatait.

A Szabályzat célja továbbá az Intézményen belüli egységes adatvédelmi és adatbiztonsági szemlélet, valamint olyan eljárások kialakítása és folyamatos működtetése, fenntartása, amelyekkel a személyes adatok biztonságos kezelése megvalósítható, a védelmi feladatok ellátása biztosítható, az adatvédelmi előírások megsértése megelőzhető, az adatvédelmi incidensek körülményei felderíthetők és indokolt esetben felelősségre vonási eljárás kezdeményezhető.

1.2 A Szabályzatban használatos kifejezések értelmezése

A Szabályzatban használatos kifejezések az egészségügyi és a hozzájuk kapcsolódó adatok kezeléséről és védelméről szóló mindenkori törvényi szabályozásban foglaltaknak megfelelően értelmezendők. Amennyiben ez a törvényi szabályozás nem tartalmazza az adott kifejezés értelmezését, úgy az információs önrendelkezési jogról szóló általános törvényi szabályozás definíciói, ilyenek hiányában a magyar nyelv és a köznapi szóhasználat alapján szükséges a Szabályzat kifejezéseit értelmezni.

Adatállomány: az egy nyilvántartásban kezelt adatok összessége[1];

Adatbiztonság: a személyes adatok jogosulatlan kezelése, így különösen jogosulatlan megszerzése, feldolgozása, megváltoztatása és megsemmisítése elleni szervezési, technikai megoldások, valamint eljárási szabályok összessége; az adatkezelés azon állapota, amelyben az adatok sérülésének, illetéktelen felhasználásának, megsemmisülésének kockázati tényezőit – és ezáltal a fenyegetettséget – a szervezési, műszaki megoldások és intézkedések a minimálisra csökkentik;

Adatkezelés: a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás,

[1] Infotv. 3. § 21. pont

terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés[2];

Adatkezelésért felelős szervezeti egység: az Intézmény azon szervezeti egysége, amelynek feladatkörébe tartozik az Intézmény kezelésében lévő valamely nyilvántartási rendszer létrehozása, fenntartása, illetve üzemeltetése;

Adatkezelő: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely a személyes adatok kezelésének céljait és eszközeit önállóan vagy másokkal együtt meghatározza; ha az adatkezelés céljait és eszközeit az uniós vagy a tagállami jog határozza meg, az adatkezelőt vagy az adatkezelő kijelölésére vonatkozó különös szempontokat az uniós vagy a tagállami jog is meghatározhatja;[3]

Adatkezelési Nyilvántartás: a GDPR 30. cikkében meghatározott adattartalmú, folyamatosan karbantartott nyilvántartás;

Adattovábbítás: az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele[4]

Adattörlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk többé nem lehetséges [5]

Néhány esetben (pl. bíróság döntés) lehet adatokat fizikailag is törölni egy rendszerből. Ilyen esetekben szükséges egy üres „place-holder” elemet tárolni a hierarchiának ezen pontján, hogy jelezze a törlést és azt, hogy az mikor és miért történt.

- Fizikai törlés: az adatok felismerhetetlenné tétele oly módon, hogy a helyreállításuk nem lehetséges.
- Logikai törlés: téves adatbevitel esetén lehetséges az adatokat logikailag törölni. A törlés ebben az esetben nem jelenti az adatok megsemmisülését. A törölt adatok, a törlés ténye, oka és az ehhez kapcsolódó adatok tárolásra kerülnek (ki, hol és miért). A törölt adatok, mint egy előző verzió az arra jogosultak számára elérhetőek.

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;

Adatvédelmi incidens: 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;

[2] GDPR 4. cikk 2. pont
[3] GDPR 4. cikk 7. pont
[4] Infotv. 3. § 11. pont
[5] Infotv. 3. § 13. pont

Adatmegsemmisítés*:* az adatokat tartalmazó adathordozó teljes fizikai megsemmisítése[6];

Adatfeldolgozás: az adatkezelő megbízásából vagy rendelkezése alapján eljáró adatfeldolgozó által végzett adatkezelési műveletek összessége;

Adatfeldolgozó: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely az adatkezelő nevében személyes adatokat kezel [7];

Adatkezelési megbízott: az adatkezelésért felelős szervezeti egység azon, e feladatkör ellátására kijelölt munkavállalója, aki a jelen utasításban, illetve az adatkezelést szabályozó más belső szabályozó dokumentumokban meghatározottak szerint az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó adatkezelések tekintetében, vagy adatkezeléseknek az adatkezelésért felelős szervezeti egység felelősségi körébe tartozó részében gondoskodik az adatkezelőt terhelő feladatok elvégzéséről,

Adatvédelem: az adatok valamilyen szintű, előre meghatározott csoportjára vonatkozó olyan előírások, amelyek adatkezelések, adathozzáférések és adatfelhasználások jogszerűségeit szabályozzák;

Adatvédelmi tisztviselő: a GDPR 39. cikkében meghatározott feladatokat az Intézmény jelen szabályzatában foglaltak szerint ellátó, az Intézménnyel jogviszonyban álló természetes- vagy jogi személy, aki elősegíti az Intézmény, mint Adatkezelő személyes adatok kezelésére vonatkozó jogszabályban meghatározott kötelezettségeinek teljesítését;

Álnevesítés (pszeudonimizálás): a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni[8];

Beteg: az egészségügyi szolgáltatásokat igénybe vevő vagy abban részesülő személy;[9]

Betegellátó: a kezelést végző orvos, az egészségügyi szakdolgozó, az érintett gyógykezelésével kapcsolatos tevékenységet végző egyéb személy, a gyógyszerész;[10]

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;[11]

Bűnügyi személyes adat*:* a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;[12]

Deperszonalizálás (anonimizálás): a nyilvántartási rendszerben tárolt személyes adatok közül a személyazonosításra alkalmas adatok eltávolítása olyan, visszafordíthatatlan módon, hogy a

[6] Infotv. 3. § 16. pont
[7] GDPR 4. cikk 8. pont
[8] GDPR 4. cikk 8. pont
[9] Eütv. 3. § a) pont
[10] Eüak. 3. § g) pont
[11] Infotv. 3. § 3b. pont
[12] Infotv. 3. § 4. pont

nyilvántartási rendszerben megmaradó adatok a továbbiakban semmilyen körülmények között nem teszik lehetővé egy természetes személy azonosítását;

Diagnosztikai vizsgálat: az egészségügyi szolgáltatóhoz forduló beteg panasza okának feltárására irányuló vizsgálat[13]

Dolgozói személyes adat: az Intézménnyel foglalkoztatási jogviszonyban álló személyek adata;

EGT állam: az Európai Unió tagállama és az Európai Gazdasági Térségről szóló megállapodásban részes más állam, továbbá az az állam, amelynek állampolgára az Európai Unió és tagállamai, valamint az Európai Gazdasági Térségről szóló megállapodásban nem részes állam között létrejött nemzetközi szerződés alapján az Európai Gazdasági Térségről szóló megállapodásban részes állam állampolgárával azonos jogállást élvez[14]

Egészségügyi adat: egy természetes személy testi vagy szellemi egészségi állapotára vonatkozó személyes adat, ideértve a természetes személy számára nyújtott egészségügyi szolgáltatásokra vonatkozó olyan adatot is, amely információt hordoz a természetes személy egészségi állapotáról;

Egészségügyi dokumentáció: a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés(ek), nyilvántartás(ok), vagy bármilyen más módon rögzített adat vagy multimédiás információ, függetlenül annak hordozójától vagy formájától[15];

Egészségügyi dolgozó*:* az orvos, a fogorvos, a gyógyszerész, az egyéb felsőfokú egészségügyi szakképesítéssel rendelkező személy, az egészségügyi szakképesítéssel rendelkező személy, továbbá az egészségügyi tevékenységben közreműködő egészségügyi szakképesítéssel nem rendelkező személy;[16]

Egészségügyi ellátás*:* a beteg adott egészségi állapotához kapcsolódó egészségügyi szolgáltatások összessége;[17]

Egészségügyi szolgáltató: a tulajdoni formától és a fenntartótól függetlenül minden, egészségügyi szolgáltatás nyújtására az egészségügyi hatóság által kiadott működési engedély alapján jogosult jogi személy, jogi személyiség nélküli szervezet és minden olyan természetes személy, aki a szolgáltatást saját nevében nyújtja;[18]

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;

Érintett: azonosított vagy azonosítható természetes személy; [19]

Genetikai adat: egy természetes személy örökölt vagy szerzett genetikai jellemzőire vonatkozó minden olyan személyes adat, amely az adott személy fiziológiájára vagy egészségi állapotára vonatkozó egyedi

[13] Eütv. 3. § kb) pont
[14] Infotv.3. § 23. pont
[15] Eütv. 3. § p) pont, és az Eüak. 3. § e) pont
[16] Eütv. 3. § d) pont
[17] Eütv. 3. § c) pont
[18] Eütv. 3. § f) pont
[19] GDPR 4. cikk 1. pont

információt hordoz, és amely elsősorban az adott természetes személyből vett biológiai minta elemzéséből ered;[20]

Gyógykezelés: minden olyan tevékenység, amely az egészség megőrzésére, továbbá a megbetegedések megelőzése, korai felismerése, megállapítása, gyógyítása, a megbetegedés következtében kialakult állapotromlás szinten tartása vagy javítása céljából az érintett közvetlen vizsgálatára, kezelésére, ápolására, orvosi rehabilitációjára, illetve mindezek érdekében az érintett vizsgálati anyagainak feldolgozására irányul, ideértve a gyógyszerek, gyógyászati segédeszközök, gyógyfürdőellátások kiszolgálását, a mentést és betegszállítást, valamint a szülészeti ellátást is;[21].

Harmadik fél: az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, 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 felhatalmazást kaptak**;**;[22]

Harmadik ország*:* minden olyan állam, amely nem EGT-állam;[23]

Hozzájárulás: az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez;[24]

Informatikai szakterület: az informatikai rendszerek üzemeltetéséért, az informatikai biztonság ellátásáért felelős szervezeti egység vagy egységek, ideértve az Intézmény információbiztonsági felelősét is;

Kezelést végző orvos: a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, valamint ezek keretében beavatkozásokat végző orvos, aki a beteg gyógykezeléséért felelősséggel tartozik vagy abban közreműködő orvos (pl.: konzílium, telemedicina, stb.);[25].

Kezelőorvos: a beteg adott betegségével, illetve egészségi állapotával kapcsolatos vizsgálati és terápiás tervet meghatározó, továbbá ezek keretében beavatkozásokat végző orvos, illetve orvosok, akik a beteg gyógykezeléséért felelősséggel tartoznak;[26]

Közeli hozzátartozó: a házastárs, az egyeneságbeli rokon, az örökbe fogadott, a mostoha- és nevelt gyermek, az örökbe fogadó, a mostoha- és nevelőszülő, valamint a testvér és az élettárs[27];

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

[20] Infotv. 3. § 3a pont
[21] Eüak. 3. § c) pont
[22] GDPR 4. cikk 10. pont

[23] Infotv. 3.§ 24. pont
[24] GDPR 4. cikk 11. pont
[25] Eüak. 3. § f) pont

[26] Eütv. 3. § b) pont
[27] Eütv. 3. § r) pont, Eüak.3. § j) pont

működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat[28];

Közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli[29];

Közvetett adattovábbítás: személyes adatnak valamely harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére továbbítása útján valamely más harmadik országban vagy nemzetközi szervezet keretében adatkezelést folytató adatkezelő vagy adatfeldolgozó részére történő továbbítása;

Különleges adat*:* a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;

Nemzetközi szervezet: a nemzetközi közjog hatálya alá tartozó szervezet és annak alárendelt szervei, továbbá olyan egyéb szerv, amelyet két vagy több állam közötti megállapodás hozott létre vagy amely ilyen megállapodás alapján jött létre,

Nyilvánosságra hozatal: az adat bárki számára történő hozzáférhetővé tétele[30];

Orvosi titok: a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat(ok), továbbá a szükséges, vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat.
Orvosi titok nem csak orvosnak juthat tudomására, illetve nem csak orvos kezelhet. Az orvosi titok megőrzése a jogszabály által előírt kivételektől eltekintve minden esetben kötelező[31];

Sürgős szükség: az egészségi állapotban hirtelen bekövetkezett olyan változás, amelynek bekövetkeztében azonnali egészségügyi ellátás hiányában az érintett közvetlen életveszélybe kerülne, illetve súlyos vagy maradandó egészségkárosodást szenvedne,[32]

Személyes adat: azonosított vagy azonosítható természetes személyre („érintett”) vonatkozó bármely információ; azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat, online azonosító vagy a természetes személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható;[33].

Személyazonosító adat (egészségügyi adat kezelése esetén): az olyan, az egészségügyi adat érintettjének azonosítására szolgáló személyes adat, amelyet az adatkezelő az egészségügyi adattal együtt, az egészségügyi adat kezelésével azonos vagy attól elválaszthatatlan céllal az egészségügyi dokumentáció részeként kezel;.

[28] Infotv. 3. § 5. pont
[29] l Infotv. 3. § 6. pont
[30] Infotv. 3. § 12. pont
[31] Eüak. 3. § d) pont
[32] Eütv. 3. § i) pont, Eüak. 3. § k) pont
[33] GDPR 1. cikk 1. pont

Teljes bizonyító erejű magánokirat:

- a kiállító az okiratot saját kezűleg írta és aláírta,
- vagy két tanú igazolja, hogy az okirat aláírója a részben vagy egészben nem általa írt okiratot előttük írta alá, vagy aláírását előttük saját kezű aláírásának ismerte el (az igazoláshoz az okiraton mindkét tanú elhelyezi az aláírását, továbbá saját kezűleg, olvashatóan feltünteti a nevét és lakóhelyét, ennek hiányában tartózkodási helyét),
- vagy az okirat aláírójának aláírását vagy kézjegyét az okiraton bíró vagy közjegyző hitelesíti,
- vagy ügyvéd vagy kamarai jogtanácsos az általa készített okirat szabályszerű ellenjegyzésével bizonyítja, hogy az okirat aláírója a más által írt okiratot előtte írta alá vagy aláírását előtte saját kezű aláírásának ismerte el,
- vagy az elektronikus okiraton az aláíró a minősített vagy minősített tanúsítványon alapuló fokozott biztonságú elektronikus aláírását vagy bélyegzőjét helyezte el, és – amennyiben jogszabály úgy rendelkezik – azon időbélyegzőt helyez el,
- vagy az elektronikus okiratot az aláíró a Kormány rendeletében meghatározott azonosításra visszavezetett dokumentumhitelesítés szolgáltatással hitelesíti, vagy olyan, törvényben vagy kormányrendeletben meghatározott szolgáltatás keretében jött létre, ahol a szolgáltató az okiratot a kiállító azonosításán keresztül a kiállító személyéhez rendeli és a személyhez rendelést a kiállító saját kezű aláírására egyértelműen visszavezethető adattal együtt vagy az alapján hitelesen igazolja; továbbá a szolgáltató az egyértelmű személyhez rendelésről kiállított igazolást elektronikus dokumentumba kapcsolt, elválaszthatatlan záradékba foglalja és azt az okirattal együtt legalább fokozott biztonságú elektronikus bélyegzővel és legalább fokozott biztonságú időbélyegzővel látja el.

Ha az okirat aláírója nem tud olvasni, illetve nem érti azt a nyelvet, amelyen az okirat készült, csak akkor jön létre teljes bizonyító erejű magánokirat, ha magából az okiratból kitűnik, hogy annak tartalmát a tanúk egyike vagy a hitelesítő személy az okirat aláírójának megmagyarázta.

Tiltakozás: az érintett nyilatkozata, amellyel személyes adatainak kezelését kifogásolja, és az adatkezelés megszüntetését, illetve a kezelt adatok törlését kéri;

Titkosítás: az adatok olyan átalakítása, melynek során az adat értelmezhetetlenné válik a megfelelő kulcs ismerete nélkül;

1.3 Az adatvédelemi alapelvek meghatározása

Az adatvédelmi alapelvek az Infotv.-ben és az EU általános adatvédelmi rendeletében meghatározott alapelvek szerint lettek meghatározva az alábbiak szerint:

- A személyes adatok védelméhez való jog és az önrendelkezés joga a természetes személyek Alaptörvényben biztosított alapjoga.
- Az információs önrendelkezési jog az érintettek beleegyezésének hiányában kizárólag törvényi felhatalmazás alapján korlátozható.
- Az információs önrendelkezési jog megvalósulása érdekében az Intézmény személyes adatokat csak a törvényben előírt esetekben (kötelező adatkezelés), illetve akkor kezel amennyiben ahhoz az érintett kifejezetten hozzájárult.
- Az Intézmény munkavállalói a feladatok ellátása kapcsán személyes és különleges adatot csak a vonatkozó jogszabályok előírásainak betartásával kezel.
- Az Intézmény munkavállalója fegyelmi, kártérítési, szabálysértési és büntetőjogi felelősséggel tartozik a feladat- és hatáskörének gyakorlása során tudomására jutott személyes adatok jogszerű kezeléséért.
- Az Intézmény munkavállalója felelős a rendszerekben és a dokumentumokban rendelkezésére álló adatok hozzáférési jogosultságok jogszerű használatáért.

- Az Intézmény személyes adatok kezelését csak a jogszabályokban meghatározott feladat- és hatáskörének gyakorlásához szükséges célból végez jog gyakorlása vagy kötelezettség teljesítése érdekében.
- A hozzájáruláson alapuló adatkezelésre csak az érintteti hozzájárulás birtokában van lehetőség.
- Törvényben elrendelt adatkezelés esetén kizárólag a felhatalmazást adó törvényben meghatározott célból valósulhat meg adatkezelés.
- Az Intézmény által kezelt – vagy az Intézmény feladatainak ellátásához más adatkezelő által rendelkezésre bocsátott – személyes adatok magáncélra való felhasználása tilos.
- Az adatkezelésnek mindenkor meg kell felelnie a célhoz kötöttség alapelvének.
- Személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető.
- Ha az adatkezelés célja megszűnt, vagy az adatok kezelése egyébként jogellenes, az adatokat törölni kell.
- A törlés az adatok oly módon történő felismerhetetlenné tétele, hogy helyreállításuk már nem lehetséges.
- Ha az Intézmény munkavállalója tudomást szerez arról, hogy az általa kezelt személyes adat hibás, hiányos, vagy elavult, köteles azt helyesbíteni, vagy helyesbítését az adat rögzítéséért felelős munkatársnál kezdeményezni.

1.4 Az egészségügyi és azokhoz kapcsolódó személyes adatok kezelésének célja

Az intézmény saját működésének és tevékenységének, minőségbiztosítási rendszerének fenntartása érdekében végzett adatkezelés az Európai Parlament és az Európai Tanács 2016/679. számú Általános Adatvédelmi Rendelet értelmében jogszabályi felhatalmazás, illetve jogos érdekre hivatkozás alapján történik.

Az egészségügyi adatkezelés célja:

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 érvényesítése,
f) az egyéni betegút követése.

Egészségügyi adatok továbbítása a gyógykezelés érdekében:

Az adatkezelés és adatfeldolgozás esetén az érintett betegségével kapcsolatba hozható minden olyan egészségügyi adat továbbítható, amely a kezelőorvos vagy a háziorvos döntése alapján a gyógykezelés érdekében fontos, kivéve, ha ezt az érintett írásban vagy önrendelkezési nyilvántartásba vett nyilatkozatában megtiltja. Ennek lehetőségéről a továbbítás előtt az érintettet tájékoztatni kell. Törvényben meghatározott közérdekből az érintett tiltása ellenére is továbbítani kell az egészségügyi és személyazonosító adatot.

Egészségügyi és személyazonosító adatot az a)-e) pontokban felsoroltakon kívül az alábbi célból lehet még kezelni:
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,
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 törvényben meghatározott feladatok ellátására kapott felhatalmazás körében bűnmegelőzés,
i) a nemzetbiztonsági szolgálatokról szóló 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 és közszolgálati jogviszony, hivatásos szolgálati viszony vagy egyéb jogviszony keretében történik,
p) közoktatás, felsőoktatás és szakképzés 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.

A fentiekben meghatározott céloktól eltérő célra is lehet az érintett, illetve törvényes vagy meghatalmazott képviselője (a továbbiakban együtt: **törvényes képviselő**) – megfelelő tájékoztatáson alapuló – írásbeli hozzájárulásával egészségügyi és személyazonosító adatot kezelni.
Az érintett a törvény értelmében a hozzájárulását bármikor visszavonhatja.
A hozzájárulással kapcsolatos bizonyítási kényszer a törvény értelmében az Adatkezelőnél van.

Egészségügyi, illetve személyazonosító adatot csak meghatározott célból, jog gyakorlása, és kötelezettség érdekében lehet kezelni. Csak annyi és olyan egészségügyi, illetve személyazonosító adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas, és csak a cél megvalósulásához szükséges mértékben és ideig.

Az egészségügyi, illetve személyazonosító adatok kezelésében érdekeltek lehetnek: az egészségügyi intézmény, a beteg, jogszabályban meghatározott körben a beteg, illetve az elhunyt beteg hozzátartozói, jogszabályban meghatározott, egészségügyi, illetve személyazonosító adatok kezelésére felhatalmazott szervezetek, hatóságok. Az érdekelt felek szükségletei és elvárásai az érintett pozíciójától függően eltérőek lehetnek, így

- az Intézmény vonatkozásában a pontos, az érintett egészségi állapotának követését elősegítő, egyértelmű és a gyógykezelés elvárható gondosságát alátámasztó dokumentáció vezetése, mely az egészség megőrzését, javítását, az eredményes és hatékony gyógykezelést szolgálja,
- a beteg és hozzátartozói vonatkozásában a pontos, az érintett egészségi állapotának követését elősegítő dokumentáció vezetése, mely lehetővé teszi az érintett számára a betegjogok gyakorlását, az egészsége megőrzése, javítása érdekében szükséges további lépések tervezését, esetleges utókezelését, rehabilitációját,
- más szervezetek, hatóságok vonatkozásában a feladat- és hatáskörükbe utalt tevékenység hatékony, a személyhez fűződő jogok tiszteletben tartása mellett történő ellátása.

Az egészségügyi, illetve személyazonosító adatok kezelésének és védelmének belső környezeti tényezői: az adatbiztonsági és adatvédelmi rendelkezések megismertetése a szervezeti egységekkel, alkalmazottakkal, a gyakorlati alkalmazásra vonatkozó belső tájékoztatók, megbeszélések, a szabályzat tartalmának folyamatos fejlesztése, a jogszabályi és minőségirányítási szabályozók változásaihoz igazítása.
A GDPR értelmében elvégzett érdekmérlegelési teszt, illetve szükség esetén hatásvizsgálat elvégzése a belső környezeti tényezőkhöz tartoznak.
A hatásvizsgálat minimális tartalmát a GDPR rendelet előírja. Javasolt a NAIH oldalán elérhető hatásvizsgálati szoftvert alkalmazni.
Az érdekmérlegelési tesztet szükség esetén az adatvédelmi tisztviselő végzi el, erről és a hatásvizsgálatokról nyilvántartást kell vezetni az Intézményben. A nyilvántartásban azoknak az érdekmérlegelési teszteknek is szerepelnie kell, amelyeknél nem született pozitív döntés.

Az egészségügyi, illetve személyazonosító adatok kezelésének és védelmének külső környezeti tényezői: az adatbiztonsági és adatvédelmi rendelkezések megismertetése a betegekkel (érintetti megkeresés), hozzátartozókkal, adatkérések és hatósági megkeresések fogadása, feldolgozása, megválaszolása.

Az Érintetti és a hatósági megkeresésekről nyilvántartást kell vezetni.

Az egészségügyi, illetve személyazonosító adatok kezelésével kapcsolatos lehetséges kockázatok és azok kezelése:

- adatvesztés, adatsérülés (kezelése: többszintű adatkezelés, papír alapon és elektronikusan is, a papír alapú dokumentáció tárolása, őrzése, irattározása, az elektronikus adatok védelme megfelelő eszközökkel, szoftverekkel, rendszergazdai intézkedésekkel, számítástechnikai rendszerek folyamatos karbantartása, frissítése, adatmentése, ld. a Szabályzat II.1. és 2. pontját),
- adathiba (kezelése: az egészségügyi dokumentációban történt elírás, leírási, gépelési hiba javítása protokoll szerint, a javítás időpontjának és elvégzője nevének feltüntetése mellett),
- illetéktelen hozzáférés az adatokhoz (kezelése: az adatbiztonsági és adatvédelmi rendelkezések megismertetése a szervezeti egységekkel, alkalmazottakkal, a gyakorlati alkalmazásra vonatkozó belső tájékoztatók, megbeszélések, az elektronikus adatok védelme megfelelő eszközökkel, szoftverekkel, rendszergazdai intézkedésekkel, személyhez kötött hozzáférési kóddal, a nem jogosulttól származó adatkérések esetén a kérelmező felhatalmazásának ellenőrzése. ld. a

Szabályzat II.1., II.2. és II.3. pontját).
A kockázatkezelési intézkedések tervezése és előkészítése az Intézmény Főigazgató Főorvosának a feladatkörébe tartozik, a gyakorlati megvalósításban az Intézmény informatikusa is közreműködik, akik kikérik az adatvédelmi tisztviselő véleményét. A tervezett intézkedéseket a Főigazgató Főorvos hagyja jóvá.

Az egészségügyi dokumentáció formái: elektronikus (informatikai alapú) és manuális (papír alapú). Az egyes formák létrehozására, tárolására, megőrzésére, megfelelőségére, felügyeletére és selejtezésére vonatkozó előírásokat a Szabályzat II.6., II.7. és II.8. pontja tartalmazza.

2. A szabályzat hatálya

A Szabályzat hatálya kiterjed az Intézménynél előforduló minden adatkezelésre és adatfeldolgozásra, amely

a) természetes személy személyes adataira
b) közérdekű adatokra

vonatkozik, beleértve az adatkezelés minden elemét, függetlenül attól, hogy az elektronikusan vagy papír alapon történik.

2.1. Területi hatály

A szabályzat területi hatálya kiterjed az Intézmény telephelyein lévő épületben lévő mindazon helyiségekre, amelyekben a szabályzat tárgyi hatálya alatt meghatározott eszközöket, szoftvereket használnak melyek segítségével elektronikus adatokat vagy dokumentumokat hoznak létre, tárolnak, használnak vagy továbbítanak.

2.2. Tárgyi hatály

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

- az egészségügyi ellátás nyújtásához kapcsolódó adatkezelést valósítanak meg a Szabályzat 4. pontjában felsorolt jogszabályok és az Intézmény belső szabályzatai szerint;
- 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);
- foglalkoztatási jogviszonyhoz kapcsolódó adatkezelést valósítanak meg (az Intézménnyel egészségügyi szolgálati jogviszonyban, munkaviszonyban vagy egyéb foglalkoztatási jogviszonyban (együtt: foglalkoztatási jogviszony) álló, állt, vagy foglalkoztatási jogviszonyba lépni szándékozó személyek) az adataira vonatkoznak.;
- az Intézménnyel szerződéses kapcsolatban álló társaságok képviselőinek, kapcsolattartóinak az adataira vonatkoznak.

2.3. Személyi hatály

Jelen Szabályzat személyi hatálya kiterjed az Intézmény irányítása alatt eljáró, a személyes adatokhoz hozzáféréssel rendelkező természetes személyekre (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 (adatfeldolgozók) esetén a GDPR 28. cikkének megfelelően.

2.4. Időbeli hatály

A Szabályzat rendelkezéseit szükség szerint, de legalább háromévenként felül kell vizsgálni.

3. A Szabályzat alkalmazása

A Szabályzatban foglaltakat a hatályos, az egészségügyi és a hozzájuk kapcsolódó személyes adatokról szóló, valamint az információs önrendelkezési jogról szóló általános jogszabályi rendelkezések alapul vételével kell alkalmazni, a jogszabályokban foglaltak elsőbbségének elvét szem előtt tartva.

Feladat és hatáskörök

Intézmény Főigazgató Főorvosának feladat és hatásköre

Az intézetben az egészségügyi és személyazonosító adatok védelméért, az alkalmazott adatkezelési rendszerek meghatározásáért, a nyilvántartás megőrzéséért az Intézmény Főigazgató Főorvosa felelős.

Tevékenysége során:

- gondoskodik az adatvédelmi szabályzatok elkészítéséről, kiadásáról, betartásáról és betartatásáról;
- kezdeményezi az adatvédelem, illetve az adatbiztonság területén kifejlesztett új technológiák és eszközök alkalmazását,
- biztosítja az adatkezeléssel foglalkozó személyek adatkezelési oktatását,
- kijelöli és megbízza az adatvédelmi tisztviselőt,
- tudományos kutatás esetén személyre szólóan, feladathoz és határidőhöz kötötten engedélyezi az orvosi dokumentációba való betekintést,
- gondoskodik az Intézet Adatvédelmi és Adatbiztonsági szabályzatának kiadásáról,
- dönt a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról
- vagy megsemmisítéséről,
- felelős az adatvédelmi szabályok megtartását biztosító személyi és tárgyi feltételek megteremtéséért.

Az Orvosigazgató feladat és hatásköre

A Főigazgató főorvost távollétében az orvosigazgató helyettesíti, adatvédelmi és adatbiztonsági felelősségi körében ellátja a Főigazgató Főorvos részére kijelölt feladatokat és tevékenységeket.

Adatvédelmi tisztviselő (=DPO) feladat és hatásköre

Az adatvédelmi tisztviselő a Főigazgató Főorvos, mint munkáltatói jog gyakorlója alá tartozó, vagy az Intézménnyel szerződéses jogviszonyban álló külső megbízottjaként láthatja el feladatait.
Az adatvédelmi tisztviselőt szakmai rátermettség és különösen az adatvédelmi jog és gyakorlat szakértői szintű ismerete, valamint a GDPR Rendeletben (39. cikk) említett feladatok ellátására való alkalmasság alapján kell kijelölni.
Az adatvédelmi tisztviselő közvetlenül az Intézmény, mint adatkezelő legfelső vezetésének tartozik felelősséggel.

Feladatai és tevékenységei:

- közreműködik, illetőleg segítséget nyújt az adatkezeléssel összefüggő döntések meghozatalában, valamint az érintettek jogainak biztosításában,
- tájékoztat és szakmai tanácsot ad az adatkezelő, továbbá az adatkezelést végző alkalmazottak részére az EU általános adatvédelmi rendelet, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban,
- ellenőrzi az adatkezelésre vonatkozó hazai és uniós jogszabályok, valamint a belső adatvédelmi és adatbiztonsági szabályzat rendelkezéseinek és az adatbiztonsági követelmények betartását, ideértve a feladatkörök kijelölését, az adatkezelési műveletekben vevő személyzet tudatosság-növelését és képzését, valamint a kapcsolódó auditokat is.
- kivizsgálja a hozzá érkezett bejelentéseket az érintettek, betegek részéről, és jogosulatlan adatkezelés észlelése esetén annak megszüntetésére hívja fel az adatkezelő személyt vagy az adatfeldolgozót,
- részt vesz a belső adatvédelmi és adatbiztonsági szabályzat elkészítésében;
- kérésre szakmai tanácsot ad az adatvédelmi hatásvizsgálatra vonatkozóan, valamint nyomon követi a hatásvizsgálat GDPR Rendelet (35. cikk) szerinti elvégzését,
- együttműködik a felügyeleti hatósággal,
- az adatkezeléssel összefüggő ügyekben – beleértve az előzetes konzultációt is (GDPR Rendelet 36. cikk) – kapcsolattartó pontként szolgál a felügyeleti hatóság felé, valamint adott esetben bármely egyéb kérdésben konzultációt folytat vele,
- kapcsolattartóként gondoskodik a kötelező adatbejelentésekről a felügyeleti hatóság felé, un. adatvédelmi tisztviselő regisztrálása (név, elérhetőség), továbbá az adatkezelőnél bekövetkezett incidens (biztonsági esemény) bejelentése,
- nyilvántartást vezet az adatvédelmi incidensekről,
- gondoskodik az adatvédelmi ismeretek oktatásáról.

Az adatvédelmi tisztviselő mellett az Intézmény adatvédelmi feladatainak felügyeletét a szervezeti egység vezetői biztosítják.

Az egészségügyi ellátást végző orvos feladat és hatásköre

Kezelést végző orvosnak kell tekinteni – a szakrendelés/részleg vezető főorvoson és a kezelő orvosán kívül – az adott járóbeteg szakrendelés/szakambulancia valamennyi orvosát, ügyeleti időben az ügyeletes orvost is.

A kezelést végző orvos feladatai különösen:

- a beteg adatkezeléssel kapcsolatos egyértelmű hozzájárulásának megszervezésére,
- a vezető főorvos egyidejű tájékoztatásával annak lehetővé tétele, hogy a beteg (törvényes képviselő) az egészségügyi dokumentációba előre egyeztetett időpontban az Intézet által rendszeresített kérelem alapján betekinthessen,
- a betegek egészségügyi adatainak kezelése és továbbítása a törvényben meghatározottak szerint,
- bűncselekmény elkövetésének alapos gyanúja esetén a Főigazgató Főorvos értesítése telefonon;
- ellátja mindazokat az adatkezeléshez kapcsolódó adatvédelmi feladatokat, melyekkel az osztályvezető főorvos megbízza.

Ápolási Igazgató feladat és hatásköre

Az érintett egészségügyi és személyazonosító adatait a Főigazgató Főorvos megbízása alapján megismerheti:

- az asszisztensi szakterületet érintő bejelentések, panaszok kivizsgálásakor;
- a szakrendelések/részlegek asszisztens által vezetett dokumentációjának ellenőrzése során;
- az egészségügyi szakdolgozók etikai magatartásának osztályon történő ellenőrzései alkalmával.

Gazdasági Igazgató feladat és hatásköre

A gazdasági igazgató jogosult megismerni és kezelni a beteg személyazonosító adatait, illetve indokolt és szükséges esetben szükséges mértékig egészségügyi adatot (pl. betegség ténye, stb.)

- az Intézményben kezelt nem magyar állampolgároknak, akik a hatályos jogszabályok értelmében betegellátási díj fizetésére kötelezettek.
- a biztosítottaknak, akik a külön jogszabályban meghatározottak szerint részleges, vagy teljes térítés mellet vehetik igénybe az egészségügyi szolgáltatásokat.
- Munkavállalókkal és alkalmazottakkal kapcsolatos személyes és különleges adatok, illetve dokumentumok.

Az Intézményi jogi képviselő feladatai és hatásköre

A panaszok kivizsgálása, a hatósági eljárások során, valamint az Intézmény ellen indult perekben jogosult:

- az érintett beteg egészségügyi dokumentációjába betekinteni,
- az egészségügyi dokumentációról másolatot készíteni,
- a kezelőorvostól, az egészségügyi szakdolgozóktól a beteg egészségi állapotáról, gyógykezeléséről, az érintett Intézeti tartózkodásának körülményiről tájékoztatást kérni,
- adatvédelmi incidens esetén a kivizsgálási anyagba betekinteni,
- a munkavállalókkal és alkalmazottakkal kapcsolatos személyes és különleges adatok, illetve dokumentumok.

Informatikai technikai személyzet feladatai és hatásköre

A napi üzemeltetési feladatok ellátása kapcsán jogosultak az egészségügyi személyzet munkáját segíteni.
Az üzemeltetés kapcsán a mentések, visszatöltések szoftver verziócserék és hibaelhárítás során jogosult az adatokba a szükséges mértékig betekinteni.

A finanszírozási referens feladat és hatásköre

A finanszírozási adatküldés és elszámolás kapcsán jogosult az egészségügyi ellátás teljes dokumentációjának a megismerésére, ellenőrzésére. Szükség esetén fénymásolat készítésére.

Adattovábbításra jogosultak köre

Az Intézetben egészségügyi és személyazonosító adatot továbbíthat:

- a Főigazgató Főorvos
- a gazdasági igazgató
- a kezelést végző orvos
- közegészségügyi és járványügyi célból:
  - a kezelést végző orvos
  - az egészségügyi szakdolgozó
  - az érintett gyógykezelésével kapcsolatos tevékenységeket végző egyéb személy.
- A hatóságok részére a jogszabályban meghatározottak szerint felhatalmazott személy, vagy az adatvédelmi tisztviselő továbbíthat adatot,
- mindazon személyek, akiket a Főigazgató Főorvos a munkaköre ellátása kapcsán a munkaköri leírásában ezzel megbízott.

4. Eltérés a Szabályzatban foglaltaktól

A Szabályzatban foglaltaktól eltérni csak az Intézmény Főigazgató Főorvosa jóváhagyásával lehetséges, s csak addig a mértékig, amíg azt a jogszabályok lehetővé teszik.

5. A Szabályzat módosítása

A Szabályzatot szükség szerint, de legalább három évenként felül kell vizsgálni. A jogszabályváltozásokat a Szabályzatban át kell vezetni, ennek megtörténtéig a módosuló jogszabályok folytán hatálytalanná váló rendelkezések nem alkalmazhatók.
A Szabályzat módosítása az intézeti adatvédelmi tisztviselő javaslata alapján a Főigazgató Főorvos jóváhagyásával történhet.

6. A Szabályzat megismerhetősége

A Szabályzat mindenkor hatályos állapota az Intézmény Intranet hálózatán kerül közzétételre a hatálybelépéssel egyidejűleg. Az Intézmény Intranet hálózata az Intézmény valamennyi szervezeti egysége, telephelye és dolgozója számára hozzáférhető. A 2.2. pontban hivatkozott az Intézmény által kezelt egészségügyi és azokhoz kapcsolódó személyes adatokhoz való hozzáféréssel járó munkát végzők vagy adatot kezelők számára az Intézmény egyedileg teszi a Szabályzatot megismerhetővé.
A Szabályzat eredeti példánya a Minőségügyi vezetőnél található, sorszámozott, nyomtatott példánya elérhető a Főigazgató Főorvosi Titkárságon, szkennelt példánya a ZESZ Intranetén keresztül megtekinthető.

7. A Szabályzat jogszabályi háttere

A Szabályzat alapjául a következő jogszabályok szolgálnak:

- 1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről
- 1997. évi CLIV. törvény az egészségügyről
- 1997. évi LXXXIII. törvény a kötelező egészségbiztosítás ellátásairól
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (Infotv)
- 117/1998. (XII. 1.) Korm. rendelet egyes egészségügyi ellátások visszautasításának részletes szabályairól
- 62/1997. (XII. 21.) NM rendelet az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezelésének egyes kérdéseiről
- 43/2003. (VII. 29.) ESzCsM rendelet a gyógyintézetek működési rendjéről, illetve szakmai vezető testületéről
- 60/2003. (X. 20.) ESzCsM rendelet az egészségügyi szolgáltatások nyújtásához szükséges szakmai minimumfeltételekről
- 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól
- Az egészségügyi dokumentációt kezelő jogutód nélküli megszűnése esetén az adatkezelési feladatokat ellátó szerv kijelöléséről szóló 44/2008 (II.29.) Korm.rendelet
- az Elektronikus Egészségügyi Szolgáltatási Térrel kapcsolatos részletes szabályokról szóló 39/2016.(XII. 21.) EMMI rendelet
- 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 rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR)

II. A Szabályzat különös rendelkezései

1. Általános biztonsági alapelvek, előírások

Az Intézményben az adatok kezelését – mind papíralapon, mind informatikai úton – az adatok megóvását biztosító módon kell végezni. 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.

Ennek érdekében papíralapú adatkezelés esetén:

- csak a vonatkozó biztonsági feltételeknek megfelelő zárható helyiségben, zárható szekrényben,
- a Zuglói Egészségügyi Szolgálat Iratkezelési Szabályzatában (SZ 05) foglaltaknak megfelelő rendben,

informatikai alapú adatkezelés esetén:

- folyamatos, a későbbiekben részletezendő időnkénti mentéssel,
- legalább két, külön helyiségben lévő szerveren kell megvalósítani az adatok tárolását.

Az adatkezelésre kizárólag a jogszabályok és e Szabályzat, illetve ahol a Szabályzat ettől eltérést enged, az Intézmény Főigazgató Főorvosa által feljogosított személyek jogosultak.
Az adatkezelési jogosultságnak mindig igazolhatónak és a jogszabályokból, illetve e Szabályzatból levezethetőnek kell lennie, annak ellenőrzésére az Intézmény Főigazgató Főorvosa, adott esetben az adatvédelmi tisztviselő bevonása mellett, mindenkor jogosult.
Minden, az Intézménnyel munkavégzésre irányuló jogviszonyt létesítő, vagy adatkezelést végző személynek, valamint az Intézménnyel szerződéses vagy egyéb kapcsolatba kerülő személynek meg kell ismernie e Szabályzat tartalmát a feladatellátás szükséges feltételeként és ezt ennek megismerését igazolnia szükséges.
Jog- vagy szabályzatellenes adatkezelés esetén az Intézmény Főigazgató Főorvosa haladéktalanul köteles megtenni a szükséges intézkedéseket.

2. Az adatkezelési rendszer biztonságának és kezelésének részletes szabályozása

Az adatforgalom a gyógyító-megelőző ellátás folyamatát követi. A rendszer működési megbízhatóságának elvei a következők:

- A rendelőkben, vizsgáló- és kezelőhelyiségekben semmilyen betegadatot tartalmazó iratot, adathordozót vagy munkaállomást nem lehet olyan helyre tenni, vagy olyan módon kezelni, ahol vagy ahogyan illetéktelen személy is hozzáférhet. Az ilyen iratok elzárásáról azokban az irodákban, illetve személyzeti helyiségekben is gondoskodni kell, ahol az iratkezelőn és az illetékes személyeken kívül más, illetéktelen személy is megfordulhat.
- A rendszer rugalmasságának és működési feltételeinek biztosítása, ami az intézetvezető feladata. A rugalmasság biztosításához elengedhetetlen az intézeti adatvédelmi tisztviselő és a szervezeti egység vezetőinek megfelelő jelzései a rendszer működésével kapcsolatban. A törvények és szakmai rendeletek előírásainak, szabályainak nyomon követése szükséges az intézkedések mihamarabbi megtételéhez.
- Az adatkezelési szabályok betartásának ellenőrzése, melyet a szervezeti egység vezetői rendszeresen, de legalább évente egy alkalommal valamennyi, a hatáskörükbe tartozó szervezeti egységben elvégeznek. Ennek módja az adatkezelés gyakorlatának szúrópróbaszerű ellenőrzése, a dokumentációk tárolásának ellenőrzése, az adatkezelőkkel készített interjú. Az ellenőrzés tapasztalatait éves beszámolóban rögzítik.

2.1. Az intézményi adatvédelmi tisztviselő (=DPO)

Az egészségügyi intézményen belül az egészségügyi és személyazonosító adatok védelméért, a nyilvántartás megőrzéséért az adatot kezelő intézmény vezetője a felelős, aki e tevékenység ellátásához adatvédelmi tisztviselőt vesz igénybe.

Az adatvédelmi tisztviselő jogosultságai:

- felvilágosítást kérhet bármely dolgozótól vagy az Intézménnyel szerződéses kapcsolatban álló külső személytől az e Szabályzat szerinti adatkezelés gyakorlatával kapcsolatban,
- javaslatot tehet az adatkezelést végzők tevékenységének ellenőrzésére,
- javaslatot tehet az intézményvezető Főigazgató Főorvos intézkedéséig bármely adatkezelés megtiltására,
- vitás kérdésekben, vagy ha a törvényi, illetve az Adatvédelmi- és Adatbiztonsági Szabályzatban előírt szempontok veszélyeztetését, be nem tartását észleli és közvetlen intézkedése nem járt eredménnyel, előterjesztési jog illeti meg a Főigazgató Főorvos felé,
- javaslatot tehet az intézményvezető főorvos felé az adatkezeléssel kapcsolatos szabályozás, illetve gyakorlat módosítására, fejlesztésére,
- tanácskozási joggal részt vehet minden olyan vezetői fórumon, értekezleten, amelynek napirendjén a hatáskörébe tartozó témák szerepelnek.

Az adatvédelmi tisztviselő kötelezettségei:

- javaslatot tesz az adatvédelmi szabályok betartása és betartatása érdekében,
- gondoskodik a dolgozók adatvédelmi ismereteinek fejlesztéséről, ennek keretében a Szabályzatban foglaltak tudomásul vételének igazolásáról, szükség esetén adatvédelmi kérdések megválaszolásáról, a vonatkozó jogszabályok ismeretanyagának átadásáról, Oktatási segédanyagot állít össze,
- folyamatosan figyelemmel kíséri az adatkezelés intézményi rendjét és javaslatot annak megszervezésére,
- az adatbiztonsági, adatvédelmi feladatokról, adatvédelemmel kapcsolatos problémákról szükség esetén tájékoztatást nyújt az intézmény vezetői felé,
- kezdeményezheti az adatvédelem területén kifejlesztett új technológiák és eszközök alkalmazását,
- segítséget nyújt a szervezeti egység vezetőinek adatvédelmi munkájához,
- javaslatot tesz a Főigazgató Főorvosnak az adat-nyilvántartási időtartamokról,
- javaslatot tesz a Főigazgató Főorvosnak a kötelező nyilvántartási időt követően a nyilvántartott adatok további tárolásáról, megsemmisítéséről (iratkezelési, selejtezési szabályzat szerint),
- segíti a Főigazgató Főorvost az adatkezelési kérdésekben meghozandó döntések előkészítésében (pl. az orvosi dokumentációba történő betekintéssel, az egészségügyi adatok megismerésével, másolatkéréssel kapcsolatos kérelmek elbírálásában, az EESZT-vel kapcsolatos hatósági megkeresések megválaszolásában),
- szervezi az adatvédelmi képzéseket,
- közreműködik az intézmény adatvédelmi és adatbiztonsági szabályzatának elkészítésében,
- ellátja az e Szabályzat vagy jogszabály által részére megállapított további feladatokat.

2.2. Szervezeti egység (osztály) adatvédelmi feladatai

Az adott szervezeti egység (osztály) vezetője, vagy az általa megbízott személy:

- figyelemmel kíséri az osztályon történő valamennyi adatkezelést, hogy az Adatvédelmi és Adatbiztonsági Szabályzat előírásai teljesülnek-e,
- figyelemmel kíséri az osztály dolgozóinak továbbképzését az Adatvédelmi és Adatbiztonsági Szabályzat végrehajtásáról,
- ellenőrzi az orvosi titok megtartását,
- észrevételeit továbbítja az intézményi adatvédelmi tisztviselőnek.

2.3. Az adatkezelési rendszer környezetének védelme

A papíralapú dokumentációt előfordulási helyén el kell zárni, vagy folyamatos felügyeletet kell biztosítani. Olyan helyiségek esetében, ahol gyakori a helyiség elhagyása a napi munkafolyamatok miatt (pl. rendelő), a helyiségek zárására kiemelt figyelmet kell fordítani.

Nagyobb mennyiségű dokumentációs anyag tárolási helyein a tűzvédelmi előírások, csőtörés miatti dokumentum megsemmisülés megelőzése és óvó rendszabályok betartása kötelező.

Elektronikus dokumentáció kizárólag személyes jelszóval védett munkaállomásokon tehető hozzáférhetővé, az arra jogosultak számára. Biztosítani kell, hogy az elektronikusan tárolt adatokkal kapcsolatos minden beavatkozás (módosítás, továbbítás, törlés stb.) csak az arra feljogosított által, visszakereshető módon történhessen.

2.4. Az adatok sérülésének, illetve elvesztésének megelőzésére, a következmények felszámolására tervezett intézkedések

Valamennyi adat mentése két szerverre történik, ami nagyban kiküszöböli az adatsérülés és adatvesztés lehetőségét.
Ezen kívül a papíralapú dokumentumok zárható helyiségekben, zárható szekrényekben történő tárolása további biztonsági garanciát nyújt az adatok integritása szempontjából.
Az informatikai rendszer lehetővé teszi, hogy a papíralapon esetlegesen károsodott adatok eredete, létrehozásának időpontja bizonyítható legyen kétség esetén, illetve az ilyen adatok rekonstruálhatóak legyenek.
Az Intézményi audit kapcsán GDPR értelmében végzett adatvédelmi vizsgálatok is elvégzésre kerülnek rendszeres időközönként.

2.5. Az adatkezelési rendszer sérülése, illetve károsodása esetére tervezett intézkedések

A két szerveren történő adattárolás nagyban kiküszöböli az adatkezelési rendszer károsodásával kapcsolatos veszélyeket a tárolt adatokra nézve. A rendszer fizikai, informatikai vagy egyéb károsodása esetén haladéktalanul megtörténik az adattárolásra szolgáló szerverek biztonságba helyezése, szükség esetén az adatok migrálásának intézése.
A rendszer helyreállításáig az adatokat manuálisan kell rögzíteni, majd az így felvitt adatokat, amint az lehetségessé válik, informatikailag fel kell dolgozni.
A papíralapú adatkezelésre vonatkozóan a tároló hely sérülése esetén a még használható dokumentumokat biztonságos helyre kell szállítani.
Mindennemű adatkezelés esetén az adatok hozzáférésének biztonságát veszélyeztető állapot felszámolását azonnal meg kell kezdeni, és az elhárítás idejére folyamatos felügyeletet, illetéktelenek hozzáférésének kiküszöbölését kell biztosítani.
Az elhárítást követően a történteket egy kivizsgálási jegyzőkönyvben kell rögzíteni. A jegyzőkönyvnek részét kell, hogy képezze egy olyan vizsgálatnak, amely alapján megvizsgálásra kell, hogy kerüljön az, hogy az informatikai rendszer bizalmasság, sértetlenség és rendelkezésre állás szempontjából

sérülhetett-e.
Amennyiben bármely szempont szerint sérülés állapítható meg azonnali hatállyal intézkedni kell a sérülés elhárításáról és az eredeti állapot helyreállításáról.
Amennyiben személyes adatok is sérülhettek abban az esetben incidensvizsgálatot is le kell folytatni.

2.6. Az Incidenskezelés

A GDPR (85) preambuluma szerint:
„Az adatvédelmi incidens megfelelő és kellő idejű intézkedés hiányában fizikai, vagyoni vagy nem vagyoni károkat okozhat a természetes személyeknek, többek között a személyes adataik feletti rendelkezés elvesztését vagy a jogaik korlátozását, a hátrányos megkülönböztetést, a személyazonosság-lopást vagy a személyazonossággal való visszaélést, a pénzügyi veszteséget, az álnevesítés engedély nélküli feloldását, a jó hírnév sérelmét, a szakmai titoktartási kötelezettség által védett személyes adatok bizalmas jellegének sérülését, illetve a szóban forgótermészetes személyeket sújtó egyéb jelentős gazdasági vagy szociális hátrányt.”

Az incidenskezelés célja

- Az adatkezelő kellő sebességgel és eredményességgel végrehajthassa azokat az intézkedéseket, amelyek révén a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehessen állítani,
- Magas kockázatú incidens esetén az érintett tájékoztatásra kerüljön, és ehhez a kellő információk rendelkezésre álljanak,
- Adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, kellő adattartalommal bejelenthesse az illetékes felügyeleti hatóságnak,
- Az incidenssel kapcsolat jogellenes tevékenységek a jogszabályok szerinti módon és mértékben felderítésre és a hatósági eljárások részére felhasználásra kerülhessenek.

Az incidenskezelés folyamata és felelősei

Az incidenskezelési folyamat megfelelőségét a ZESZ adatvédelmi tisztviselője felügyeli.

Az incidenskezelés fő lépései az alábbiak:

- A ZESZ szervezeti egységeihez, illetve a Főigazgató Főorvoshoz érkező incidens-bejelentések az adatvédelmi tisztviselőhöz kerülnek továbbításra,
- Az adatvédelmi tisztviselő értékeli a bejelentést és szükség esetén kiegészítő információkat vagy részletes kivizsgálást kezdeményez a bejelentésben szereplő adatkezelési folyamatért felelős szervezeti egységnél. Az értékelés szerint bejelentést lehet nem tekinteni incidensnek vagy kis kockázatúnak, vagy nagy kockázatúnak besorolni.
- Valós incidens esetén az adatvédelmi tisztviselő tájékoztatja a ZESZ Főigazgató Főorvosát az incidens ismert körülményeiről és a bejelentés tartalmáról.
- Amennyiben az Intézmény vezetője a kapott tájékoztatás alapján úgy ítéli meg, hogy az adatvédelmi incidens valószínűsíthetően kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatvédelmi tisztviselő adatvédelmi tisztviselő ajánlásai szerint a Hatóság honlapjáról letölthető formanyomtatvány alkalmazásával és a GDPR 33. cikk (3) bekezdése szerinti tartalommal bejelenti azt a Hatóság felé.
- Nyilvánvalóan magas kockázatot vagy súlyos következményt eredményező helyzetben az adatvédelmi tisztviselő az incidens – lehetőleg a tudomására jutást követő 72 órán belül – illetékes felügyeleti hatóságnak történő bejelentésében közreműködik (az ekkor rendelkezésre álló adatokkal),

- Amennyiben a rendelkezésre álló adatok alapján egyértelműen megállapítható, hogy az azt észlelő önálló szervezeti egység tevékenységével összefüggésben, vagy azt érintően következett be az adatvédelmi incidens, soron kívül megkezdi az incidens érintettekre nézve megjelenő hatásainak csökkentését és arról haladéktalanul írásban értesíti az adatvédelmi tisztviselőt.
- A részletes kivizsgálás alapján meghatározott helyzet- és kockázatértékelés segítségével az adatvédelmi tisztviselő szükség esetén haladéktalanul a következmények mérséklése érdekében bevonja az informatikai és az érintett szakmai egységek vezetőit és azok véleményének figyelembevételével meghatározza a szükséges további kivizsgálás irányait és a helyesbítő intézkedéseket,
- Az informatika és az érintett szakmai egységek végrehajtják a következmények mérséklésére irányuló intézkedéseket,
- A megfelelő feltételek fennállása esetén az adatvédelmi tisztviselő a lehető legrövidebb időn belül közreműködik abban, hogy az Intézmény az érintett természetes személyt megfelelő tájékoztatásában, részesítse az őket ért adatvédelmi incidensről.
- Az adatvédelmi tisztviselő megvizsgálja az felé beérkező jelzésben foglaltakat, és az adatvédelmi incidens lehetséges hatásainak felmérése és megállapítása érdekében szükség szerint bevonja az Intézmény informatikai biztonságért felelős vezetőjét, az önálló szervezeti egység vezetőjét vagy az adatvédelmi incidenssel érintett szakterület tekintetében szakértelemmel rendelkező személyeket is.
- Az adatvédelmi tisztviselő az IT és az érintett szakmai egységek vezetőinek bevonásával megvizsgálja, és szükség esetén kezdeményezi az incidensben szerepet játszó folyamatok és azok szabályozásának módosítását.
- Az adatvédelmi tisztviselő gondoskodik az incidens adatainak és a kapcsolódó dokumentumoknak teljes körű rögzítéséről az incidenskezelési nyilvántartásban.

Az adatvédelmi incidens bejelentésének folyamata a felügyeleti hatóságnak

A jogszabályok (GDPR 33. cikk (1) pont) szerint az adatvédelmi incidenst a ZESZ indokolatlan késedelem nélkül, és ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomására jutott, bejelenti az illetékes felügyeleti hatóságnak.
Az illetékes hatóság felé a bejelentést az ZESZ adatvédelmi tisztviselője kezdeményezi, aki

- mérlegeli, hogy az adatvédelmi incidens valószínűsíthetően jár-e számottevő kockázattal a természetes személyek jogaira és szabadságaira nézve, és ennek függvényében indítja meg a bejelentési eljárást,
- mielőbb, lehetőleg még a bejelentést megelőzően tájékoztatja a ZESZ főigazgató főorvosát az incidens ismert körülményeiről és a bejelentés tartalmáról,
- köteles a bejelentés adatait rögzíteni az incidenskezelési nyilvántartásban, a bejelentéssel kapcsolatos iratokat az incidenskezelési nyilvántartáshoz tartozóan másolatban archiválja,
- nyomon követi az esetleges hatósági eljárás lépéseit és kezdeményezi a hatósági intézkedések megvalósulását.

Azt, hogy az bejelentésre indokolatlan késedelem nélkül került-e sor, különösen az adatvédelmi incidens jellegére és súlyosságára, valamint annak az érintettre gyakorolt következményeire, illetve hátrányos hatásaira figyelemmel kell megállapítani.
Ha a bejelentés nem történik meg 72 órán belül, akkor annak megtörténtekor mellékelni kell hozzá a késedelem igazolására szolgáló indokokat is. A 72 órás határidő betartása érdekében a bejelentés akár még hiányos adattartalommal (pl. az érintett adatkör teljes körű tisztázása előtt) is meg kell, hogy történjen. Ilyen esetben a bejelentést – a hiányzó adatok rendelkezésre állását követően haladéktalanul – utólag ki kell egészíteni.
Amennyiben az adatkezelési incidens az ZESZ adatfeldolgozói kapcsolatban levő más szereplőnél következik be, akkor a GDPR 33. cikk (2) pont szerint az adatfeldolgozó az adatvédelmi incidenst, az

arról való tudomásszerzését követően indokolatlan késedelem nélkül bejelenti a ZESZ. Ez esetben a ZESZ – a fentiek szerinti, a kockázat mértékére irányuló mérlegelést követően, annak eredményétől függően – a fenti eljárásban hajtja végre a bejelentést.

A bejelentés tartalma

A GDPR 33. cikk (3) szerint az illetékes hatóság felé történő bejelentésben legalább

- ismertetni kell az adatvédelmi incidens jellegét, beleértve – ha lehetséges – az érintettek kategóriáit és hozzávetőleges számát, valamint az incidenssel érintett adatok kategóriáit és hozzávetőleges számát;
- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell a ZESZ által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

Az érintett tájékoztatása az adatvédelmi incidensről

A jogszabályok (GDPR 34. cikk (1) pont) szerint, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelőnek indokolatlan késedelem nélkül tájékoztatnia kell az érintettet az adatvédelmi incidensről.

Az érintettet nem kell tájékoztatni, ha az alábbiak bármelyike teljesül:

- ha az adatvédelmi incidens, az addig rendelkezésre álló adatok mérlegelése alapján valószínűsíthetően nem járt magas kockázattal az érintett természetes személy(ek) jogaira és szabadságaira nézve,
- a ZESZ korábban olyan megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás (pl. kulcsos titkosítás, anonimizálás, pszeudonimizálás) alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az incidensben érintett személyes adatokat
- a ZESZ az adatvédelmi incidenst követően olyan további intézkedéseket tett, amelyek biztosítják, hogy az érintett jogaira és szabadságaira jelentett magas kockázat a továbbiakban valószínűsíthetően nem valósul meg
- a tájékoztatás aránytalan erőfeszítést tenne szükségessé. Ilyen esetekben az érintetteket nyilvánosan közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.

A fenti feltételek fennállását az adatvédelmi tisztviselő köteles értékelni és a tájékoztatási kötelem fennállásáról a döntés meghozatalát kezdeményezni.
A tájékoztatási kötelmet – fenti mérlegeléstől függetlenül – megalapozza, ha a felügyeleti hatóság vizsgálati hatáskörében eljárva utasítja a ZESZ, hogy tájékoztassa az érintettet az adatvédelmi incidensről.
Amennyiben fennáll a tájékoztatás kötelme, akkor az érintett tájékoztatását a ZESZ adatvédelmi tisztviselője kezdeményezi, aki meghatározza

- az érintettek és tájékoztatandók körét,
- a tájékoztatás tartalmát,
- a tájékoztatás formáját,

- a ZESZ főigazgatóját mielőbb, lehetőleg még a tájékoztatást megelőzően informálja a tervezett tájékoztatás körülményeiről, érintettjeiről és tartalmáról,
- a tájékoztatás tényét, annak adatait, esetleges elmaradásának indoklását rögzíti az incidenskezelési nyilvántartásban, a tájékoztatással kapcsolatos iratokat az incidenskezelési nyilvántartáshoz tartozóan másolatban archiválja.

A tájékoztatás tartalma

Az érintett részére adott tájékoztatásban világosan és közérthetően ismertetni kell az adatvédelmi incidens jellegét, és közölni kell legalább az alábbi információkat és intézkedéseket.

- közölni kell az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit;
- ismertetni kell az adatvédelmi incidensből eredő, valószínűsíthető következményeket;
- ismertetni kell a ZESZ által az adatvédelmi incidens orvoslására tett vagy tervezett intézkedéseket, beleértve adott esetben az adatvédelmi incidensből eredő esetleges hátrányos következmények enyhítését célzó intézkedéseket.

A tájékoztatás formája

A tájékoztatás formájának meghatározásáért a ZESZ főigazgató főorvosa a felelős, aki e körben kikéri az adatvédelmi tisztviselő tanácsát. A ZESZ főigazgató főorvosának ezen döntése során figyelembe kell vennie a tájékoztatáshoz kapcsolódó erőfeszítések (költségek) mennyiségét, valamint az incidens kapcsán felmerült kockázatok, veszélyek és károk mértékét.
Ha mérlegelés nem eredményezi az erőfeszítések aránytalan szükségességét, akkor az érintetteket írásban, illetve – a kellő feltételek fennállása esetén – elektronikus levél útján kell tájékoztatni.
Az erőfeszítések aránytalan szükségessége esetén az érintetteket nyilvánosan (pl. sajtóban, a ZESZ internetes felületén) közzétett információk útján kell tájékoztatni, vagy olyan hasonló intézkedést kell hozni, amely biztosítja az érintettek hasonlóan hatékony tájékoztatását.
Amennyiben az incidens egyidejűleg több egészségügyi ellátót is érint, akkor a ZESZ összehangolja tájékoztatási tevékenységét a fenntartójával, illetve a többi érintett egészségügyi ellátóval.

Az incidenskezelési nyilvántartás

Az adatvédelemmel kapcsolatos incidensek kezelése, ellenőrzése, valamint a hatóságok és az érintettek tájékoztatása érdekében a ZESZ nyilvántartást vezet az incidensekkel kapcsolatos adatokról. A nyilvántartásba rögzíteni kell minden olyan eseményt, amely megfelel a GDPR rendelet szerinti definíciónak.

A nyilvántartás tartalma

A nyilvántartás az alábbi adatokat tartalmazza az adott incidenssel kapcsolatban:

- az incidens egyedi azonosítóját,
- az érintett személyes adatok körét,
- az érintett személyek körét és számát,
- az incidens időpontját,
- az incidens típusát, körülményeit,
- az incidens hatásait,
- az incidens negatív következményeinek és megismétlődésének elhárítására megtett intézkedéseket,
- a felügyeleti hatósági bejelentés szükségességét, a bejelentés adatait (időpont, forma, tartalom)
- az incidens érintettjeinek tájékoztatásának tényét, annak adatait, esetleges elmaradásának indoklását,

- a jogszabályban előírt egyéb feladatokat.

A nyilvántartás részeként, fizikai elkülönülés esetén azzal logikailag egységben kezelve, központilag tárolni kell az egyes adatvédelmi incidensekhez kapcsolódó,

- az adatvédelmi incidens felügyeleti hatósági bejelentésével kapcsolatban keletkezett adatokat és dokumentumokat,
- az érintettek tájékoztatásához kapcsolódóan keletkezett adatokat és dokumentumokat.

Felelős

Az incidenskezelési nyilvántartás jogszabályoknak és jelen Szabályzatnak megfelelő vezetéséért a ZESZ főigazgató főorvosa a felelős, aki ezen tevékenységét az adatvédelmi tisztviselője bevonásával látja el.

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 a tervezett adatkezelésért felelős szervezeti egység vezetője végzi el, az adatvédelmi tisztviselő iránymutatásai alapján. Az érdekmérlegelési tesztet írásban kell elvégezni. Az elkészült dokumentumot az adatvédelmi tisztviselőnek kell megküldeni, aki azt szakmai szempontból véleményezi. A jogos érdeken alapuló adatkezelés kizárólag az érdekmérlegelési teszt elvégzését és az adatvédelmi tisztviselő véleményének beszerzését követően kezdhető meg.

Az érdekmérlegelési teszt módszertanát, a megválaszolandó kérdéseket minden esetben a tervezett adatkezelés figyelembevételével kell megválasztani, az alábbi kérdések köre csak orientáló, a tervezett adatkezelés szempontjából releváns egyéb kérdésekkel bővíthető. Abból kell kiindulni, hogy bármilyen adatkezelés beavatkozás az érintett magánszférájába és e beavatkozás jogosságát, szükségességét és arányosságát kell bizonyítani.

Az érdekmérlegelési teszt részei:

- a tervezett adatkezelés leírása és az annak keretében kezelni tervezett személyes adatok meghatározása,
- az adatkezelő vagy azon harmadik fél jogos érdekének azonosítása, akinek az adatkezelés érdekében áll (Miért szükséges az adatkezelés?),
- az érintett érdekeinek, jogainak azonosítása (Arányban van-e az adatkezelés az érintett magánszférájának korlátozásával?),
- az adatkezelő (vagy harmadik fél) és az érintettek érdekeinek összevetése,
- az adatkezelés biztosítékainak leírása,
- 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.

A hatásvizsgálat elvégzését a tervezett adatkezelésért felelős szervezeti egység vezetője koordinálja. A hatásvizsgálat megállapításait írásban kell rögzíteni. Az elkészült hatásvizsgálati dokumentációt az adatvédelmi tisztviselőnek kell megküldeni, amely azt 8 munkanapon belül szakmai szempontból véleményezi és beszerzi az információbiztonsági szakterület véleményét is. Ha az adatkezelési megbízott 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 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.

A hatásvizsgálat első részében összefoglalóan le kell írni a tervezett adatkezelést, különösen:

- az adatkezelésért felelős szervezeti egységet és a tervezett adatfeldolgozó megjelölését;
- az adatkezelés jogalapját, célját (az adatkezeléstől várt előnyöket, az adatkezelés szükségességét), terjedelmét (időben és a kezelt adatok volumenében);
- az adatkezeléssel érintettek körét, a kezelendő adatok körét, az adatok megőrzésének tervezett idejét,
- azon adatkezelők megjelölését, akiknek az adatot továbbítani tervezik, és különösen, ha harmadik országba vagy nemzetközi szervezet felé tervezik az adattovábbítást;
- az adatkezelésre vonatkozó követelmények (jogszabályi követelmények vagy magatartási kódexből, szabványból eredő követelmények);
- az adatkezelés folyamatának a leírását.

A hatásvizsgálat második részében ki kell fejteni és meg kell indokolni az adatkezelés szükségességének és arányosságának garanciáit, az érintett jogait biztosító garanciák érvényesülését.

A hatásvizsgálat harmadik részében azonosítani és értékelni kell az adatkezelés potenciális kockázatait, és a kockázatok enyhítésére tervezett, elfogadott intézkedéseket, megoldásokat.

A hatásvizsgálat negyedik része tartalmazza a tervezett adatkezelés értékelését:
a szempontok értékelését a tekintetben, hogy azok egyenként megfelelőek, további intézkedésekkel megfelelőek lehetnek, illetve nem megfelelőek;
a tervezett kiegészítő intézkedések végrehajtásának ütemtervét;
annak egyértelmű rögzítését, hogy a tervezett adatkezelés valószínűsíthetően magas kockázattal jár-e a természetes személyek jogaira nézve, és ennek alapján az adatkezelés megkezdhető-e, illetve szükség van-e az adatvédelmi felügyeleti hatósággal való konzultációra.

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

A nyilvántartás kezelése

Bizalmasság

A nyilvántartás egésze bizalmasan kezelendő, annak tartalmának megismerésére az alábbiak jogosultak:

- a ZESZ Főigazgató Főorvosa és annak esetleges megbízottja(i),
- az adatvédelmi tisztviselő és annak esetleges megbízottja(i),
- a jogszabályok szerinti hatóságok meghatalmazottjai.

Az adatvédelmi tisztviselő köteles a jogosultakat kérésükre az incidensek jellemzőiről tájékoztatni.

Megőrzés

Az incidenskezelési nyilvántartásban szereplő adatok megőrzési ideje a Polgári Törvénykönyv által a követelésekre meghatározott elévülési idejével (2024-ben 5 év) egyezik meg. A megőrzési idő lejártát követően a nyilvántartás érintett elemeit elektronikus forma esetén visszavonhatatlanul törölni kell, a papíralapú dokumentumokat pedig meg kell semmisíteni.
Az iratmegőrzési kötelezettség az iratok eredeti példányára, vagy eredeti példány hiányában, annak külön jogszabályban előírt módon, elektronikus úton előállított hiteles másolatára vonatkozik.
A megőrzésre és megsemmisítésre vonatkozó előírások betartásáért a ZESZ adatvédelmi tisztviselője felel, aki egyben meghatározza az őrzés helyszínét is.

2.7. Az adatok eltulajdonítása elleni védekezés szabályai

Az egészségügyi dokumentációval az egészségügyi szolgáltató, az abban szereplő adattal a beteg rendelkezik. Az egészségügyi dokumentáció védelme az Intézmény alapvető kötelezettségei közé tartozik.

A dokumentálást követően a betegdokumentációt el kell zárni, illetve folyamatos felügyelet mellett kell őrizni. A dokumentáció csak arra igazoltan jogosult személynek adható át.

Egészségügyi vagy ahhoz kapcsolódó személyes adat eltulajdonításának gyanúja esetén az intézeti adatvédelmi tisztviselőt haladéktalanul értesíteni kell, és jegyzőkönyvet kell felvenni. Az adatvédelmi tisztviselő köteles megtenni a szükséges jogi lépéseket, valamint intézkedni az eltulajdonított adat lehetőség szerinti reprodukálása, pótlása iránt.

Az informatikai úton tárolt adatok biztonságát az Informatikai Szolgáltatási Szabályzatban (SZ 17) foglaltak szerint biztosítja az Intézmény.

3. Jogosultságok szabályozása

3.1. Az adatkezelő azonosítása, az adatkezelési rendszerbe történő belépés, illetve kilépés

Az adatkezeléssel foglalkozó dolgozók aláírás mintáját rögzíteni kell. Az aláírás mintákat a szervezeti egység vezetője nyilvántartja és őrzi.
Elektronikus adatkezelés esetén az aláírást felhasználónév és jelszó helyettesíti. A jelszó titkosan történő kezeléséért a jelszó tulajdonosa felel. Tilos a jelszó megadása más személy számára, és tartózkodni kell annak mások által beazonosítható módon való feltüntetésétől.
A jelszó tulajdonosa felelős továbbá a munkaállomása elhagyásakor a rendszerből való szabályszerű kilépésért.
Az informatika vezetője felelős a jelszóhasználatot rögzítő adatállományok folyamatos naplózásáért és a napló állományok rendszeres mentéséért.

Az adatokhoz csak személyazonosítást követően férhetnek hozzá az arra feljogosítottak. A személyesen megjelenő, ily módon az adatot hozzáférhetővé tevő számára azonosítható dolgozótól aláírás kérése nem kötelező.
Külső személy (pl. hozzátartozó) számára történő adathozzáférés lehetővé tétele esetén kötelező a személyazonosítás, a jogszabály által biztosított hozzáférés alapjául szolgáló kapcsolat (meghatalmazotti minőség, hozzátartozói kapcsolat) hitelt érdemlő igazolása. Nem engedélyezhető a "bemondás" alapján történő feljogosítás a hozzáférésre.

3.2. Az adatkörök csoportosítása adatkezelők szerint

Az adatoknak nyilvántartási idejük, elhelyezésük szerint három szintjét különböztetjük meg. A különböző szintek és a hozzájuk kapcsolódó tárolási feltételek a következők:

- **„A" szint**nek nevezzük a mindennapi kezelésre szoruló dokumentációkat: ezek azok a dokumentációk, melyek a jelenleg is vizsgálaton lévő, kezelés, gondozás alatt álló érintettek iratait tartalmazzák. Papíralapú dokumentáció esetén az illetékes szervezeti egységben tárolják olyan helyen, hogy biztosítva legyen a szakorvos bármikori hozzáférhetősége, de védve legyen az érintett kezelésében részt nem vevők (pl. kísérők, fizikai dolgozók stb.) hozzáférhetősége ellen. Informatikai rendszerben tárolt dokumentum esetén a jogosultsági szintek meghatározása biztosítja a hozzáférést, illetve annak kizárását.
- **„B" szint**nek nevezzük azokat a dokumentációkat, melyek többnyire öt irattári éven belüliek. Tárolásuk dokumentumtárolási alapfunkciót szolgáló helyiségben történik (pl. központi irattár vagy valamely szervezeti egységtől fizikailag elkülönített, de a szervezeti egység kijelölt munkatársa által kezelt irattárolók). A tárolók kialakításánál biztosítani kell a dokumentációk védelmét és hozzáférésük rendszerét.
  A dokumentációkat rendszerezetten, visszakereshető módon kell raktározni biztonsági zárral ellátott tároló szekrényekben vagy biztonsági zárral ellátott helyiségben.
- **„C" szint**nek nevezzük azokat a dokumentációkat, melyek többnyire öt irattári éven túliak, nem rendszeresen, hanem esetlegesen kezeljük, megőrzési kötelezettség miatt tároljuk. Ezeket a dokumentációkat az „Archívum"-ban kell elhelyezni.

Valamennyi adatkörre azonos módon alkalmazandók a jogszabályokban és e Szabályzatban foglalt rendelkezések a hozzáférési jogosultságokat illetően.

Az egyes ellátási folyamatokhoz, betegutakhoz kapcsolódó konkrét hozzáférési jogosultságokat az informatikai rendszer algoritmusa tartalmazza a feladat- és hatáskörök, valamint a szakmai kompetenciák alapján.

3.3. Az adatkezelők jogosultságának nyilvántartása

Az informatikai algoritmus alapján az egyes dolgozók konkrét hozzáférési jogosultsága munkakör szerint kerül meghatározásra, és az informatikai rendszerben kerül nyilvántartásra.
Az ettől való eltérésre, módosításokra az intézeti adatvédelmi tisztviselő javaslatot tehet az adatbiztonság és az adatkezelési szabályok betartásának szem előtt tartásával, azt a Főigazgató Főorvos engedélyezheti.

Az Intézményen belül az egészségügyi és személyazonosító adat kezelésére jogosult – az adatkezelés egyéb feltételeinek teljesülése esetén:

- a Főigazgató Főorvos,
- az Orvosigazgató
- a Gazdasági igazgató,
- Ápolási igazgató és helyettese,
- Humánerőforrás Igazgató
- minőségügyi vezető
- finanszírozási referens,

- alapellátási koordinátor
- az informatikai osztály munkatársai,
- központi betegirányítás dolgozói,
- a szervezeti egységek vezető főorvosai,
- szakorvosok,
- védőnők,
- gyógytornászok,
- pszichológusok,
- a betegellátásban résztvevő egészségügyi szakdolgozók,
- az intézeti adatvédelmi tisztviselő,
- az otthoni szakápolás dolgozói,
- adminisztrátorok, titkárnők,
- ügyiratkezelő irattáros,
- pénzügyi osztály ezzel a feladattal megbízott munkatársai.

Fent nevezettek „Munkavégzésre irányuló jogviszonyban foglalkoztatott személy adatvédelmi és titoktartási nyilatkozata” (FNY 189) tételére kötelezettek. A nyilatkozatot a Munkaügyi és bérgazdálkodási Osztályon a személyi anyagban őrizzük.

Az Intézményből egészségügyi és személyazonosító adatot az alábbi személyek továbbíthatnak – az adattovábbítás további feltételeinek teljesülése esetén:

- a Főigazgató Főorvos és helyettesei,
- a szakorvos,
- fertőző betegség észlelése esetén a betegellátó a törvényben meghatározott esetekben,
- védőnők,
- a Főigazgató Főorvos által a NEAK, illetve egyéb külső intézmény felé küldött elektronikus adatszolgáltatással megbízott szervezeti egységek.

Népegészségügyi célból történő adattovábbítás

A daganatos eredetű betegség észlelése esetén a betegellátó továbbítja az érintett egészségügyi és személyazonosító adatait a 49/2018. (XII. 28.) EMMI rendelet alapján vezetett Nemzeti Rákregiszternek.

4. Az egészségügyi dokumentáció ellenőrizhetősége

4. 1. Az adatkezelési rendszer adminisztrálásának szabályozása

A Főigazgató Főorvos szakmai koordinációja és az adatvédelmi tisztviselő tanácsadása mellett a szervezeti egységek vezetői az adott szervezeti egység napi szintű adatkezelési tevékenységét támogatják.

A beteg, illetve a beteg hozzátartozója vagy meghatalmazottja által a ***Betegdokumentációról kért másolat kiadás nyilvántartása*** tartalmazza:

- a kérő nevét (ha hozzátartozó, akkor rokoni fokát is),
- a kérő lakcímét,
- a kért dokumentáció nevét,
- keletkezési dátumát vagy időintervallumát,
- a másolatok oldalszámát,
- a dokumentáció kiadójának nevét.
- a kiadás dátumát,
- az átvevő aláírását vagy a továbbítás módját.

A listát a Főigazgató Főorvosi által megbízott személy-, illetve röntgen film vagy adathordozó kiadása esetén a kiadó szervezeti egység vezeti.

Esemény-, rendkívüli esemény jelentések tételes nyilvántartása tartalmazza:
- az esemény, rendkívüli esemény megnevezését,
- az esemény, rendkívüli esemény idejét,
- az egység nevét,
- a jelentés címzettjének nevét, címét.

Az archiválási rend dokumentációja az intézmény Iratkezelési Szabályzata (SZ 05) alapján történik, az archivált iratok nyilvántartását a szabályzatnak megfelelően kell végezni.

4.2. Az adatok eredetének azonosíthatósága

Az érintettek személyes adatainak eredetiségét az érintett személyi igazolványának, TAJ kártyájának, útlevelének, lakcím kártyájának, EU-s biztosítási kártyájának, illetve egyéb a térítés-mentességet igazoló okiratának elkérésével lehet azonosítani.
A betegellátók azonosítása a dokumentáción lévő aláírás és pecsét (orvosi, intézményi) alapján történik.
Amennyiben számítógépes rendszeren készült a dokumentáció, az azonosításnak két lehetséges módja van. Az egyik a fokozott biztonságú elektronikus aláírás és pecsét, a másik a kinyomtatott dokumentáción a felülhitelesítés.

4.3. Az adatok pontosságának, valódiságának mérése

Az adatok pontosságáért az adatokat rögzítő, illetve azokat származtató munkatárs felelős. Az egészségügyi adatok pontossága, valódisága természetüknél fogva csak korlátozottan rekonstruálható a későbbiekben. Az adatok pontosságát és valódiságát a lehetőségekhez mérten biztosító tényezők a következők:
- elektronikus adatrögzítés esetén a rögzítés időpontjának visszakereshető módon történő regisztrációja,
- adatmódosítás tényének felismerhetősége,
- jogszabály által megkívánt esetekben a beteg (törvényes képviselő) aláírása a dokumentáción a megfelelőség elismeréseként

Kétség, illetve panasz esetén a szervezeti egység vezetője jogosult az adatok összevetésével megvizsgálni a hibás, pontatlan adatok előfordulását. Amennyiben megállapításra kerül, hogy valamely adat valótlan, téves, erről feljegyzést kell készíteni, és az adatnál is jelölni kell annak ilyen minőségét, továbbá lehetőség szerint rekonstruálni kell a helyes adatot, és azt javítottként feltüntetni a dokumentációban. Ilyen esetekben a hibás adatot tartalmazó dokumentációt esetleg használó érintetteket is tájékoztatni kell az adathiba észleléséről.
Az egészségügyi dokumentációban szereplő hibás adatot úgy kel kijavítani vagy törölni, hogy az eredetileg felvett adat megállapítható legyen.

Az Érintett jogai

Az Intézmény vezetője biztosítja, hogy az érintett – aki lehet az Intézmény munkavállalója, illetve a Intézményen kívüli harmadik természetes személy (pl. beteg), akinek az adatát az Intézmény kezeli – az Intézmény által kezelt adataihoz az alábbiak szerint tájékozódjon a személyhez kapcsolódó adatkezelésről.
Az érintett az Infotv. és az EU általános adatvédelmi rendeletében foglaltak szerint tájékoztatást kérhet az Intézménytől mint Adatkezelőtől a személyes adatainak kezeléséről, és kérheti személyes adatainak helyesbítését, illetve – a jogszabályban elrendelt adatkezelések kivételével – azok törlését, más adatkezelő vagy adatfeldolgozó általi hozzáférésének korlátozhatóságát, kérheti adatainak hordozhatóságát, tiltakozhat személyes adatainak kezelése ellen.

A tájékoztatás ingyenes, ha a tájékoztatást kérő az adott naptári évben azonos adatkezelésre vonatkozó tájékoztatási kérelmet még nem nyújtott be. Egyéb esetekben költségtérítés állapítható meg, amelynek fedeznie kell a tájékoztatással kapcsolatban felmerült közvetlen költségeket. A már megfizetett költségtérítést vissza kell téríteni, ha az adatokat jogellenesen kezelték, vagy ha a tájékoztatás kérése a személyes adat helyesbítését eredményezte.
Amennyiben törvény alapján az érintett tájékoztatása nem tagadható meg, a tájékoztatás többek között kiterjed a kezelt adatok megjelölésére, az adatkezelés céljára, jogalapjára, időtartamára, továbbítására, az adatfeldolgozó nevére, címére és az adatkezeléssel összefüggő tevékenységére, továbbá arra, hogy kik és milyen célból kapják vagy kapták meg az adatokat.

Az érintett által benyújtott, az őt megillető jogosultságok érvényesítésére irányuló kérelmet annak benyújtásától számított legrövidebb idő alatt, de legfeljebb 30 napon belül elbírálja és döntéséről az érintettet írásban, vagy ha az érintett a kérelmet elektronikus úton nyújtotta be, elektronikus úton értesíti[34].

Az adatkezelő indokolatlan késedelem nélkül, de mindenféleképpen a kérelem beérkezésétől számított egy hónapon belül tájékoztatja az érintettet a GDPR 15–22. cikk szerinti kérelem nyomán hozott intézkedésekről. Szükség esetén, figyelembe véve a kérelem összetettségét és a kérelmek számát, ez a határidő további két hónappal meghosszabbítható. A határidő meghosszabbításáról az adatkezelő a késedelem okainak megjelölésével a kérelem kézhezvételétől számított egy hónapon belül tájékoztatja az érintettet. Ha az érintett elektronikus úton nyújtotta be a kérelmet, a tájékoztatást lehetőség szerint elektronikus úton kell megadni, kivéve, ha az érintett azt másként kéri.[35]

A valóságnak nem megfelelő adatot az Intézet – amennyiben a szükséges adatok rendelkezésre állnak – köteles helyesbíteni.
A kezelt adatot törölni kell, ha:

- az adat kezelése jogellenes;
- az érintett azt – törvényben előírt kötelező adatkezelést kivéve – kéri;
- az adat hiányos vagy téves, és ez az állapot jogszerűen nem orvosolható, feltéve, hogy a törlést törvény nem zárja ki;
- az adatkezelés célja megszűnt, vagy az adatok tárolásának törvényben meghatározott határideje lejárt;
- azt a bíróság vagy a Hatóság elrendelte.

Az adat helyesbítéséről vagy törléséről az érintetten kívül mindazokat tájékoztatni kell, akiknek az adatot továbbították, kivéve, ha a tájékoztatás elmaradása az adatkezelés céljára tekintettel az érintett jogos érdekeit nem sérti.
Abban az esetben, ha az érintett önként fordul az egészségügyi ellátóhálózathoz, 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 egészségügyről szóló 1997. évi CLIV. törvény 15 §(4) bekezdése alapján a beteg a (3) bekezdésben foglalt beleegyezését szóban, írásban vagy ráutaló magatartással megadhatja, kivéve, ha e törvény eltérően nem rendelkezik.

Az érintettet az adatkezelés megkezdése előtt tájékoztatni kell az adatkezeléssel összefüggő tényekről az Infotv. 14. §-ában foglaltak szerint. Ezt a tájékoztatást az Intézet területén és honlapján elhelyezett az „Adatkezelési kérdésekkel kapcsolatos tájékoztató betegeink számára” c. tájékoztatóban tesszük közzé.

[34] Infotv. 15. § (1) b)
[35] GDPR 12 cikk (3)

Az érintett tiltakozhat személyes adatának kezelése ellen, ha

- a személyes adatok kezelése (továbbítása) kizárólag az adatkezelő vagy az adatátvevő jogának vagy jogos érdekének érvényesítéséhez szükséges, kivéve, ha az adatkezelést törvény rendelte el;
- a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik;
- a tiltakozás jogának gyakorlását törvény lehetővé teszi.

Amennyiben a tiltakozás indokolt, az adatkezelő köteles az adatkezelést (további adatfelvételt, adattovábbítást) megszüntetni és az adatokat zárolni, valamint a tiltakozásról, és az annak alapján tett intézkedésekről értesíteni mindazokat, akik részére a tiltakozással érintett személyes adatot korábban továbbította.

Ha az érintett nem ért egyet a tiltakozásának elbírálása eredményeként hozott adatkezelői döntéssel, a döntés ellen a közléstől számított harminc napon belül – az Infotv. 22. §-ában foglalt módon – bírósághoz fordulhat.

Jogorvoslati lehetőségek

Az Érintett – amennyiben álláspontja szerint az adatkezelés nem felel meg a jogszabályi követelményeknek, illetőleg az Intézmény megsértette személyes adataihoz fűződő jogait – a

Nemzeti Adatvédelmi és Információszabadság Hatósághoz (=NAIH)
(székhely: 1055 Budapest, Falk Miksa utca 9-11.;
postacím: 1363 Budapest, Pf. 9,
telefon: +36 (1) 391-1400,
e-mail: dpo@naih.hu
web: http://www.naih.hu/
online ügyintézés elérhetősége: https://naih.hu/online-ugyinditas)

fordulhat, vagy a Bíróság előtt érvényesítheti jogait.

A jogérvényesítés az Infotv., valamint a Ptk. alapján lehetséges.
A Nemzeti Adatvédelmi és Információszabadság Hatóságnál bejelentéssel bárki vizsgálatot kezdeményezhet arra hivatkozással, hogy személyes adatok kezelésével kapcsolatban jogsérelem következett be vagy annak közvetlen veszélye fennáll.
Az érintett adatvédelmi hatósági eljárás megindítása iránti kérelmet nyújthat be a Nemzeti Adatvédelmi és Információszabadság Hatósághoz, ha megítélése szerint a rá vonatkozó személyes adatok kezelése megsérti e rendeletet.

A bírósági jogérvényesítés esetén az ügyben soron kívül jár el. A per elbírálása az Adatkezelő székhelye szerinti, azaz a

Fővárosi Törvényszék
(1055 Budapest, Markó u. 27,
levelezési cím: 1363 Pf. 16.,
tel.: +36-1-354-6000)

hatáskörébe tartozik, de a per - az Érintett választása szerint - az Érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.
Az Érintett a jogainak megsértése esetén közvetlenül az Intézmény adatvédelmi tisztviselőjéhez is fordulhat.

5. Az adatkezelési rendszerből, illetve az abba irányuló adatforgalom szabályozása

Az érintettről felvett, a gyógykezelés érdekében szükséges egészségügyi és személyazonosító adatok külső (Intézményből kikerülő) továbbítását nyilván kell tartani.

A külső adattovábbításról nyilvántartást vagy kísérő iratot kell készíteni, melynek tartalmi elemei:
- adattovábbítás címzettje,
- adattovábbítás időpontja,
- továbbított adatok köre,
- adattovábbítás célja,
- adattovábbító neve, beosztása, aláírása.

Az adatkezelést végző az általa vagy az egyéb betegellátó által felvett egészségügyi adatokról, a saját tevékenységéről és intézkedéseiről feljegyzést készít, mely a nyilvántartás részét képezi.

6. Az adatkezelési rendszer műszaki megbízhatósága, a fenntartás és a karbantartás, a dokumentációs előírások szabályozása, átmeneti rendelkezések a műszaki változtatás és fejlesztés időszakára

Az adatkezelési rendszer megváltoztatása az intézeti adatvédelmi tisztviselő javaslata alapján a Főigazgató Főorvos jóváhagyása alapján történhet meg. Minden, az adatkezelési rendszer megváltozásával járó változtatási, fejlesztési elképzelést az intézeti adatvédelmi tisztviselő elé kell terjeszteni, aki véleményével segíti a Főigazgató Főorvos jóváhagyással kapcsolatos döntését.

Az adatvédelmi rendszer fejlesztésének előkészítése során a következőket kell bemutatni, a várható időtartamok, időpontok megjelölésével
- hozzáférés lehetőségének változásai,
- adatbiztonságot érintő változások,
- az adatrögzítés módját, részleteit érintő változások,
- minden egyéb, az adatkezelést érintő változás.

Harmadik országba irányuló adattovábbítás különös 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 az intézményi jogász és az informatikai osztályvezető véleményének kikérése után – javaslatot tesz az adattovábbítás módjára, az adatátadás során alkalmazandó biztosítékok körére.

6.1. Elektronikus (informatikai alapú) adatkezelés

A számítástechnikai adatok mentésének szabályozása.
Az informatikai hálózat szerverein tárolt központi adatbázisok rendszeres mentéséért az Informatikai Osztály (a továbbiakban: **informatika**) vezetője a felelős.

A szerverek központi adatbázisainak mentését minden nap el kell végezni, részletes „***Mentési és megőrzési terv***” alapján.

A mentések metodikája:

- A mentéseknek automatikusan, dokumentáltan, megfelelő hibakezeléssel és hibajelzéssel kell megtörténnie.
- Az adatbázisok napi mentését, a rendelési időn kívül kell elkészíteni.
- A mentésekről automatikusan másolatot kell készíteni, a telephelyen lévő valamely másik adatbázis szerverre is.
- Egy heti (napi-napi) mentést kell megőrizni.

A mentés további részleteit az Informatikai Szolgáltatási Szabályzata (SZ 17) tartalmazza.

A számítógépes munkaállomásokon és a nem hálózati számítógépeken tárolt adatállományok mentéséről az adatok tulajdonosa (létrehozója, vagy módosítója) köteles gondoskodni.
A munkaállomások és a nem hálózati gépek mentéséhez szükséges adathordozókat az informatika biztosítja.
A mentéseket hibaellenőrzéssel kell végrehajtani, hiba észlelése esetén meg kell ismételni.
A központi adatbázisokról készült mentések megfelelő tárolásáért az informatika vezetője a felelős.
Az egyedi számítógépek és hálózati munkaállomások mentett adatainak megfelelő tárolása a felhasználó feladata és felelőssége.

Amennyiben karbantartási vagy rendszerfejlesztési célból az adatok hozzáférése időlegesen korlátozott, úgy erről előzetesen értesíteni kell az érintetteket a korlátozottság várható időtartamának megadásával, illetve lehetővé kell tenni a napi szinten használt adatok alternatív hozzáférését. Amennyiben az elektronikus adatrögzítés lehetősége átmenetileg korlátozott, alternatív elektronikus úton vagy manuális adatrögzítéssel kell azt pótolni. Az informatikai rendszer üzemzavarának megszüntetése után az üzemzavar alatt történt adatfelvételeket az informatikai rendszerben rögzíteni kell.
Egyebekben az elektronikus adatkezelési rendszerre vonatkozó szabályokat az Informatikai Szolgáltatási Szabályzat (SZ 17) tartalmazza.

6.2. Az Elektronikus Egészségügyi Szolgáltatási Térrel (EESZT) kapcsolatos rendelkezések

Az Intézmény, mint működési engedéllyel rendelkező egészségügyi szolgáltató köteles informatikai rendszere útján csatlakozni az Elektronikus egészségügyi szolgáltatási térhez, mely az egészségügyi ellátórendszer informatikai rendszereinek együttműködését biztosítja. Az EESZT-t a Kormány által rendeletben kijelölt Állami Egészségügyi Ellátó Központ (a továbbiakban: működtető) működteti.

Az Intézmény az EESZT-hez történő csatlakozást követően csatlakozott adatkezelőként jogosult és köteles a rendszert az adatbiztonsági és adatvédelmi előírások maradéktalan betartásával használni. Az EESZT rendszerében történő adatkezelés és adattovábbítás jogszabályon alapul, a megjelölt célhoz kötötten. Az Intézmény az EESZT szolgáltatásait a működtető által biztosított csatlakozással saját informatikai rendszerén keresztül is igénybe veheti.
Az EESZT szolgáltatásait az Intézmény azon dolgozója veheti igénybe, aki a működtető által vezetett egységes azonosítási és jogosultságkezelési nyilvántartásban szerepel.
Az EESZT működtetője által kinevezett adatvédelmi tisztviselő megkeresésre az Intézmény köteles az adatkezeléssel kapcsolatos adatot, dokumentumot vagy tájékoztatást soron kívül, de legkésőbb 5 (öt) munkanapon belül rendelkezésre bocsátani.

Az Intézmény csatlakozott adatkezelőként az EESZT útján a működtető rendelkezésére bocsátja, a **központi eseménykatalógus**ban rögzíti a kezelt személlyel kapcsolatos alábbi adatokat:

a) az érintett TAJ száma, családi és utóneve, születési ideje, neme, az EESZT útján továbbított vény és beutaló esetében a vényben és beutalóban foglalt egyéb személyazonosító adatok, az érintett EESZT-ben képzett azonosítója,
b) az ellátási esemény megjelölése, típusa, időpontja és időtartama, valamint miniszteri rendeletben meghatározott egyéb adatai és dokumentumai, valamint

c) az ellátási eseményt nyújtó egészségügyi szolgáltató megjelölése, EESZT-ben képzett azonosítója, valamint az ellátást végző vagy abban közreműködő személy EESZT azonosítója.

Az adatrögzítés törvényben meghatározott célja:

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.

A működtető az EESZT útján nyújtott szolgáltatásokon keresztül, az adatok kezelésére jogosult EESZT felhasználó, így az Intézmény számára is rendszerezett módon hozzáférést biztosít az alábbi adatokhoz (központi eseménykatalógus):

a) az érintett TAJ száma, családi és utóneve, születési ideje, neme, az EESZT útján továbbított vény és beutaló esetében a vényben és beutalóban foglalt egyéb személyazonosító adatok, az érintett EESZT-ben képzett azonosítója,
b) az ellátási esemény megjelölése, típusa, időpontja és időtartama, valamint miniszteri rendeletben meghatározott egyéb adatai és dokumentumai, valamint
c) az ellátási eseményt nyújtó egészségügyi szolgáltató megjelölése, EESZT-ben képzett azonosítója, valamint az ellátást végző vagy abban közreműködő személy EESZT azonosítója,
d) az érintettre vonatkozó, a csatlakozott adatkezelők informatikai rendszereiben tárolt és hozzáférhetővé tett további adatok.

A működtető ezen adatokat az érintett halálát követő 5 évig, az egészségügyi dokumentációra vonatkozó jogszabályok szerint őrzi meg.

Az érintett bejelentheti az egészségügyi és hozzájuk kapcsolódó személyes adatai kezeléséhez hozzájáruló vagy azt korlátozó nyilatkozatát (**önrendelkezési nyilatkozat**). Az érintett az önrendelkezési nyilatkozatát megteheti:

- az EESZT útján a Kormány által rendeletben kijelölt, az önrendelkezési nyilvántartást vezető szerv által rendszeresített elektronikus formanyomtatványon,
- a Kormány által kötelezően nyújtott azonosítási szolgáltatás útján történő azonosítását követően elektronikusan, vagy
- a Kormány által kijelölt szervnél vagy a kormányablaknál személyesen, vagy meghatalmazottja útján írásban.

Az érintett nyilatkozata és az alapján vezetett önrendelkezési nyilvántartás tartalmazza:

a) az önrendelkezési nyilatkozatot tevő családi és utónevét,
b) az önrendelkezési nyilatkozatot tevő TAJ számát,
c) azoknak az egészségügyi adatoknak a megjelölését, amelyekre az önrendelkezési nyilatkozat vonatkozik és az ezen egészségügyi adatokra vonatkozó önrendelkezési nyilatkozatot, valamint
d) a nem elektronikus úton megtett önrendelkezési nyilatkozat esetében a bejelentés megtételének helyét.

Az érintett önrendelkezési nyilatkozatában jogosult megtiltani, hogy az Intézmény vagy más csatlakozott adatkezelő vagy EESZT felhasználó a központi eseménykatalógusban rögzített adatait megismerhesse.

Az EESZT felhasználó nem hivatkozhat arra, hogy az önrendelkezési nyilvántartásba bejegyzett önrendelkezési nyilatkozatot nem ismeri.
Az érintett a kezelőorvosa előtt írásban jogosult olyan nyilatkozatot tenni, amelyben az önrendelkezési nyilvántartásba bejegyzett korlátozás alól a kezelőorvos számára esetileg felmentést ad. Ilyen esetben a kezelőorvos az EESZT-ben rögzíti a nyilatkozat megtételének tényét, időpontját és tartalmát.

Az érintett kezelőorvosa, ennek hiányában háziorvosa az arra jogosult személyek részére történő hozzáférhetővé tétel érdekében az EESZT útján rögzíti az általa kezelt érintettel kapcsolatban az érintett TAJ számát, születési idejét, nemét, továbbá az érintett egészségi állapotával, kórelőzményével, egyes beavatkozásaival kapcsolatos egészségügyi adatokat (**egészségügyi profil**).
Az adatrögzítés törvényben meghatározott célja:

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.

Az egészségügyi profilban rögzített adatokat az érintett halála után 5 évvel helyreállíthatatlanul törölni kell.
Az egészségügyi profil nyilvántartásból az adat megismerésére jogosult EESZT felhasználó számára kizárólag egyedileg – TAJ számmal, ennek hiányában természetes személyazonosító adatokkal – azonosított érintettre vonatkozó adat továbbítható.

Az érintett jogosult megtiltani, hogy az egészségügyi profil adatait az érintett kezelőorvosa vagy háziorvosa rögzítse. Az érintett írásban kérheti az egészségügyi profil nyilvántartásba bejegyzett adatának javítását az azt bejegyző orvosától, illetve a működtetőtől.

Az Intézmény, mint csatlakozott adatkezelő köteles az EESZT útján a működtető részére megküldeni az egészségügyi ellátás során keletkezett, az EESZT-vel kapcsolatos jogszabályokban előírt adatokat.

Az EESZT keretein belül **digitális képtovábbítás** keretében lehetőség van egyedileg, TAJ számmal azonosított érintettre vonatkozóan az érintettről képalkotó diagnosztikai eljárással készített felvétel vagy más digitális képi információ elérésére és EESZT felhasználók egymás közötti továbbítására. A működtető ennek érdekében nyilvántartást vezet, amely az érintett TAJ számához kapcsoltan tartalmazza, hogy az érintettről képalkotó diagnosztikai eljárással felvételt készítettek és a felvétel elérési útját. A működtető a nyilvántartásban az érintettre vonatkozó adatot az érintett halálát követő 5 év elteltével törli.
A digitális képtovábbítás törvényben meghatározott célja:

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.

A működtető biztosítja az EESZT útján elektronikus konzílium lefolytatását, ha a konzíliumra felkért orvos az elektronikus konzílium lefolytatását biztosítja, a konzílium kérést elfogadja, és az érintettre vonatkozó adatokat jogosult megismerni.
A működtető a digitális képtovábbítás során továbbított adatokat nem őrzi meg, az elektronikus konzultáció során a továbbított digitális képi információt és leleteket a továbbítást követően a konzultáció lefolytatása érdekében 30 napig megőrzi, majd törli.

6.3. Manuális (papíralapú) adatkezelés

Az Intézményen belül központi iktatás révén az iratok nyilvántartása a Központi Iktatóban történik, az Intézmény Iratkezelési Szabályzatában (SZ 05) részletezett módon.
Az iratok Intézményen belüli átadásához kézbesítőkönyvet (C 5230-29), vagy elosztási jegyzéket (FNY 001), Intézményen kívüli átadásához kézbesítőkönyvet, iratmásolatot használnak. (Részletezve az Intézmény Iratkezelési Szabályzatában SZ 05)
Az adatok tárolására szalagos irományfedelet, kötegelést vagy archiváló dobozokat kell használni.
A szervezeti egységeken, részlegeken a különféle betegdokumentációk nyilvántartására regisztereket használhatnak.
Az érintettek tájékoztatására, nyilatkoztatására azokat a rendszeresített nyomtatványokat használhatják, melyek az intézeti nyomtatványalbumban szerepelnek.
A különféle egészségügyi dokumentációk nyilvántartásával, megőrzésével, archiválásával, selejtezhetőségével kapcsolatosan az Intézmény Iratkezelési Szabályzatában (SZ 05) részletezett

szabályok az irányadóak.
Az Irattár kialakítására mindenképpen olyan helyiséget kell használni, ahol az iratok fizikai megóvása biztosított. Az irattárat stabil vagy mobil, vasból vagy acélból készült állványokkal, vagy szekrényekkel kell berendezni úgy, hogy a hozzáférhetőség és a munkavédelmi szempontok biztosítva legyenek. A dokumentációk nyilvántartására szolgáló jegyzékeket elkülönítetten kell tárolni.

A dokumentációkat fűzős iratfedélben, vagy kötegelve, vagy archiváló dobozokban kell tárolni, melyeket a tartalmuk (évkör, egység, megőrzési idő) nyilvántartására szolgáló címkével, felirattal kell ellátni. A nem papíralapú iratokat az időtállóságot biztosító paramétereknek megfelelően kell tárolni. Az elektronikus adathordozók irattározásánál legfontosabb szempont a biztonsági másolatok készítése, melyet az eredetiektől elkülönített, de azzal azonos biztonsági feltételekkel kell tárolni. A központi irattárból, archívumból iratot csak az intézet felső vezetésének tagjai és a szervezeti egységek vezetői kölcsönözhetnek ki, kizárólag a munkavégzéséhez kapcsolódóan. A kölcsönzést az irattári napló és az iratpótló lap megfelelő vezetésével kell dokumentálni.

7. Az adatkezelőkre vonatkozó szabályok

7.1. A munkavégzésre irányuló jogviszonnyal összefüggő adatvédelmi vonatkozású kérdések

A Szabályzatot az Intézménnyel munkavégzésre irányuló jogviszonyt létesítőknek, valamint bármilyen jogviszony alapján az Intézmény által kezelt egészségügyi és azokhoz kapcsolódó személyes adatokhoz való hozzáféréssel járó munkát végzőknek a jogviszony létesítésekor aláírásukkal igazolva tudomásul kell venniük (Javaslat foglalkoztatásra - FNY 049, Oktatási bizonylat – FNY 050).
A Szabályzat hatálybalépésekor már az Intézménnyel jogviszonyban állóknak a hatálybalépést követő 15 napon belül kell a tudomásul vételről nyilatkozniuk. A Szabályzatban foglaltak tudomásul vétele az Intézménnyel létrejövő jogviszony alapján történő feladatellátás szükséges feltétele.
A Szabályzat tudomásul vételéről szóló „Munkavégzésre irányuló jogviszonyban foglalkoztatott személy adatvédelmi és titoktartási nyilatkozata” (FNY 189) a munkaügyi anyagban meg kell őrizni.

7.2. Az adatot kezelő és az adatkezelési rendszert fenntartó, illetve fejlesztő feladatkörök elválasztása

Az Intézményben adatkezelésre jogosultak köre e Szabályzatban foglaltak szerint meghatározott.
Az adatkezelési rendszer folyamatosan megfelelő működését és fejlesztéseit a Főigazgató Főorvos az intézeti adatvédelmi tisztviselő segítségével irányítja.

Az egyes szervezeti egységekben a szervezeti egység vezetői segítik elő az adatkezelési elvek mindennapi érvényesülését, szükség esetén tájékoztatva az intézeti adatvédelmi tisztviselőt a tapasztalt rendellenességekről, javasolt változtatásokról.

7.3. Az adatvédelmi képzés szabályozása

Minden, az Intézménnyel munkavégzésre irányuló jogviszonyt létesítő személy adatvédelmi képzésben részesül, melynek kötelező elemei a Szabályzat és a vonatkozó jogszabályok megismerése. A képzést az adatvédelmi tisztviselő szervezi meg, megtörténtét az adatvédelmi tisztviselő és az érintett, képzésben részesült személy is aláírásával igazolja.
Legalább háromévente szinten tartó képzésben kell részesülniük az Intézménnyel munkavégzésre irányuló jogviszonyban állóknak. A képzés kötelező elemei a Szabályzat hatályos állapotának és a vonatkozó jogszabályok megismerése.
A képzések történhetnek csoportos előadás vagy írásos anyag egyéni megismerése formájában is, illetve ezek kombinációjaként.
Az érintettnek a szinten tartó képzés megtörténtét is aláírásával kell igazolnia.

8. Az egészségügyi dokumentáció, illetve a zárójelentés tárolásának, megsemmisítésének, archiválásának rendje

A dokumentációk selejtezése:
A dokumentációk selejtezésére az irattáros tesz javaslatot (amennyiben ez szükséges kikéri az adatvédelmi tisztviselő véleményét) az Intézmény Iratkezelési Szabályzatában (SZ 05) meghatározott kötelező őrzési idő letelte után. Az irattáros és az illetékes levéltár közreműködésével jegyzőkönyvben rögzítik a selejtezhető dokumentációkat, majd hitelesített megsemmisítő berendezéssel megtörténhet a megsemmisítés.
A tárolás, megsemmisítés, archiválás rendjéről bővebben az Iratkezelési Szabályzat (SZ 05) rendelkezik.

9. Az egyes adatkezelési célok megvalósításának helyi sajátosságai

9.1. Adatkezelés gyógykezelés, egészségi állapot nyomon követése céljából

Az adatkezelés az érintett gyógykezeléséhez kapcsolódóan, a betegfelvétel során a személyes adatok rögzítésével kezdődik meg. Az egészségügyi adatok felvétele a gyógykezelés részét képezi. A kezelést végző orvos dönti el, hogy a szakmai, finanszírozási 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 adatok rögzítése az Intézmény orvos-informatikai rendszerében történik.

Amennyiben az ellátásban részt vevő szakember adathiányt észlel, úgy köteles annak lehetőség szerinti, valós idejű pótlása iránt intézkedni.

Az érintett az ellátásáról minden esetben (kivéve, ha a kezelőorvos megítélése szerint ez a beteg állapotának esetleges romlását eredményezheti) a kezelést végző orvos által aláírt és lepecsételt dokumentumot kap kézhez, melyen szerepel személyes adatain túl (amennyiben az ellátás jellege alapján alkalmazható)

- a beutaló diagnózis
- panaszok leírása
- a betegvizsgálat eredménye
- a megállapított kórkép
- az elvégzett beavatkozások
- további teendők (kontroll, gyógyszerszedés stb.).

Cselekvőképtelen, illetve korlátozottan cselekvőképes érintett esetén a fenti adatok törvényes képviselőhöz való eljuttatásáról is gondoskodni kell.

9.2. A betegdokumentációba való betekintés és betegdokumentációról történő másolat készítésének rendje

Az érintett, vagy annak törvényes képviselője jogosult a gyógykezeléssel összefüggésben történő adatkezelésről tájékoztatást kapni, a rá vonatkozó egészségügyi és személyazonosító adatokat megismerni, az orvosi dokumentációba betekinteni**, valamint arról másolatot kapni**.
A betegdokumentációba történő betekintés- és ***az első másolat kiadása térítésmentes***, minden további másolat kiadása térítésköteles:

7§ (3) Az érintettnek az (EU) 2016/679 európai parlamenti és tanácsi rendelet (a továbbiakban: általános adatvédelmi rendelet) 15. cikk (3) bekezdésében meghatározott, az adatkezelés tárgyát

képező személyes adatok ***minden további másolatért*** miniszteri rendeletben meghatározott költségelemek alapján ***díjat kell fizetni.***

A mindenkor aktuális térítési díjak külön Főigazgató Főorvosi utasításban meghatározottak.

Ez a jog megilleti az érintett ellátásának időtartama alatt az általa írásban felhatalmazott személyt, az érintett ellátásának befejezését követően az általa teljes bizonyító erejű magánokiratban felhatalmazott személyt is.

A érintett életében, illetőleg halálát követően az érintett házastársa, egyeneságbeli rokona, testvére, valamint élettársa – írásbeli kérelme alapján – jogosult a fenti jogok gyakorlására, ha az egészségügyi adatra a házastárs, az egyeneságbeli rokon, a testvér, illetve az élettárs, valamint leszármazóik életét, egészségét befolyásoló ok feltárása, illetve ezen személyek egészségügyi ellátása céljából van szükség, és az egészségügyi adat más módon való megismerése, illetve az arra való következtetés nem lehetséges.

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.
Az egészségügyi és személyazonosító adatok megismerésének, az orvosi dokumentációba történő betekintés és másolat készítés lehetővé tételét megelőzően a kérelmező jogosultságát körültekintően vizsgálni kell.

Az érintett beteg, vagy hozzátartozója, vagy szabályszerű meghatalmazással rendelkező megbízottja az egészségügyi dokumentációba az érvényes jogszabályok betartása mellett betekinthet, vagy arról másolatot kérhet az alábbi módon:
A Főigazgató Főorvosi Titkárságra írásban, előzetesen kérelem benyújtása szükséges. Ez iktatásra, elbírálásra kerül. A kérelmet az alábbi formanyomtatványok kitöltésével tudja kezdeményezni a kérelmező: FNY 079A saját dokumentum esetén, FNY 079B elhunyt hozzátartozó esetén.
Igazolni kell a kérelmező személyazonosságát és a kért adatokhoz való jogosultságát (beteg, meghatalmazott, hozzátartozó stb.). Mindenképpen szükséges a keresett dokumentáció pontos azonosítása, az ügyben nem érintett adatok illetéktelen hozzáférését elkerülendő.
Megtekintési kérelem esetén a dokumentum „A” és „B” szintű engedélyezése után a szervezeti egység megtekinthető, hatékony „C” szintű, előkeresése után csak meg kell állni, a megtekintés megtörtént a kérelmező aláírásával igazolja.
Másolat kérelme esetén a Titkárság (vagy a Főigazgató Főorvos által megbízott ügyintéző) az írásbeli kérelem alapján kikéri a dokumentációt a kiállító egységtől, vagy irattárból, archívumból és a fénymásolatok elkészítése után darabonként hitelesíti, valamint az „eredetivel megegyező másolat” felirattal látja el. Ez az eredeti dokumentáció a számítógépes nyilvántartásban található, úgy azt a dokumentációt készítő szervezeti egység nyomtatja ki, hitelesíti és ellátja az „eredetivel megegyező másolat” felirattal. Ezt követően kiadásra eljuttatja a Titkárságra. A térítésköteles másolatok kiadása csak a kérelmező által befizetett összegről szóló elismervény felmutatásával lehetséges. A fizetés az intézet pénztárában történik. A másolatok átvételét dokumentálni kell. Az átvételt a kérelmező a betegdokumentációról kért másolatok nyilvántartásában (FNY 079C) aláírásával igazolja.

RTG film, adathordozó kiadás a készítő szervezeti egységnél történik a fentiekben előírt nyilvántartási kötelezettség mellett.
Eredeti képalkotó diagnosztikai felvétel az érintett vagy nevében a törvényben erre feljogosított képviselője számára csak teljes bizonyító erejű magánokiratban foglalt, a cél megjelölését tartalmazó kérelem elbírálása nyomán, a felvétel lehetőség szerinti reprodukálását és a másolat megőrzéséről való gondoskodást követően adható ki.

9.3. Adatkezelés a betegjogok érvényesítése céljából

Az érintett vagy a nevében törvény által erre feljogosított képviselőjének írásbeli kérelme esetén a panaszban, bejelentésben (a továbbiakban együtt: **panasz**) foglaltak kivizsgálása során az Adatok kezelhetők, és azok a panaszra adott válaszban feltüntethetők, valamint a belső vizsgálat eredményeként esetlegesen szükségessé váló további eljárások céljából a megfelelő szervek irányában továbbíthatók. A panaszkezelés folyamatát ld. SZ 12 Panaszkezelési Szabályzat.

9.4. Adatkezelés egészségügyi szakemberképzés céljából

A gyógykezelés során az érintett (törvényes képviselője) hozzájárulásával lehet jelen szakképzésben, továbbképzésben részt vevő egészségügyi dolgozó, hallgató vagy tanuló.

Mind az egészségügyi dokumentációba történő betekintés, másolatkérés, mind a panaszkezelés során lehetőséget kell adni az érintetteknek arra, hogy az Intézmény adatbiztonsági, adatvédelmi tevékenységével kapcsolatos észrevételeiket, javaslataikat megtehessék (az Intézményben és az Intézmény honlapján közzétett nyilvános elérhetőségi csatornákon, pl. telefonon, e-mailben, levélben).

9.5. Adattovábbítás az egészségügyi ellátórendszeren kívüli szerv megkeresésére

Az alábbi szervek írásbeli megkeresésére a kezelést végző orvos az érintett egészségügyi és a megkereső szerv által törvény alapján kezelhető, az azonosításhoz szükséges személyazonosító adatait átadja a megkereső szervnek:

a) büntetőügyben a nyomozó hatóság, az ügyészség, a bíróság, az igazságügyi szakértő, polgári peres és nemperes, valamint közigazgatási hatósági ügyben a közigazgatási hatóság, az ügyészség, a bíróság, az igazságügyi szakértő,
b) szabálysértési eljárás során az eljárást lefolytató szervek,
c) potenciális hadköteles és hadköteles személy esetén a fővárosi és megyei kormányhivatal járási (fővárosi kerületi) hivatala, a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szerve, valamint 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,
e) a Magyar Honvédség katonai igazgatási és központi adatfeldolgozó szerve, a kiképzett tartalékosok békeidőszakban történő hadi beosztásra történő kiírása és a kiképzett tartalékosok gyors és differenciált behívása érdekében, a honvédelemről és a Magyar Honvédségről szóló törvényben meghatározott körben,
f) az egészségügyi dolgozóval szemben folyamatban lévő etikai eljárás során az eljárás lefolytatása hatáskörrel és illetékességgel rendelkező kamarai szerv,
g) a rendőrségről szóló törvényben meghatározott belső bűnmegelőzési és bűnfelderítési feladatokat ellátó, valamint a terrorizmust elhárító szervek a törvényben meghatározott feladatok ellátása érdekében, az abban kapott felhatalmazás körében,
h) halottvizsgálat során a halottvizsgálatot végző orvos,
i) i)a légi-, a vasúti és a víziközlekedési balesetek és egyéb közlekedési események szakmai vizsgálatáról szóló törvényben, valamint a polgári légiközlekedési balesetek és repülőesemények vizsgálatáról és megelőzéséről és a 94/56/EK irányelv hatályon kívül helyezéséről szóló, 2010. október 20-i 996/2010/EU európai parlamenti és tanácsi rendeletben meghatározott szakmai vizsgálat során a közlekedésbiztonsági szerv.

A megkeresésben az adatkezelés pontos célját és a kért adatok körét meg kell jelölni.

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. Ezen adattovábbításhoz az érintett, illetve az adattal

kapcsolatosan egyébként rendelkezésre jogosult beleegyezése nem szükséges.

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 Intézmény telephelye szerint illetékes gyermekjóléti szolgálatot haladéktalanul értesíteni kell, 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.

Ezen adattovábbításhoz az érintett, illetve az adattal kapcsolatosan egyébként rendelkezésre jogosult beleegyezése nem szükséges.

Egészségügyi és személyazonosító adatot közigazgatási hatósági eljárás, illetve az érintettnek intézményi elhelyezése, gondozása céljából akkor lehet továbbítani, ha arra az érintett jogai érvényesítéséhez vagy kötelezettségei teljesítéséhez van szükség.

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. Nincs szükség a hozzájárulásra az alábbi esetekben:

a) ha valószínűsíthető vagy beigazolódott, hogy az érintett az Eüak. 1. számú mellékletében felsorolt valamely betegség kórokozója által fertőződött, vagy fertőzéses eredetű mérgezésben, illetve fertőző betegségben szenved, kivéve a 15. § (6) bekezdése szerinti esetet,
b) ha az adattovábbításra az Eüak. 2. számú mellékletében felsorolt szűrő- és alkalmassági vizsgálatok elvégzéséhez van szükség,
c) heveny mérgezés esetén,
d) ha valószínűsíthető, hogy az érintett az Eüaktv. a 3. számú melléklete szerinti foglalkozási eredetű megbetegedésben szenved,
e) ha az adatszolgáltatásra a magzat, illetve a kiskorú gyermek gyógykezelése, egészségi állapotának megőrzése vagy védelme érdekében van szükség,
f) ha bűnüldözés, bűnmegelőzés céljából, továbbá ügyészségi, bírósági eljárás, illetve szabálysértési vagy közigazgatási hatósági eljárás során az illetékes szerv a vizsgálatot elrendelte,
g) ha az adatszolgáltatásra a nemzetbiztonsági szolgálatokról szóló törvény szerinti ellenőrzés céljából van szükség,
h) ha az adatszolgáltatás büntetőügyben a nyomozó hatóság, az ügyészség, a bíróság, az igazságügyi szakértő, polgári peres és nemperes, valamint közigazgatási hatósági ügyben a közigazgatási hatóság, az ügyészség, a bíróság, az igazságügyi szakértő megkeresése alapján történik – azzal, hogy polgári peres eljárás során a harmadik személyt érintő - szexuális úton terjedő fertőző betegségre vonatkozó - egészségügyi adat nem adható ki,
i) élveszületés és halálozás esetén a születés, illetve halálozás helye szerint illetékes anyakönyvvezető útján a Központi Statisztikai Hivatal részére az élveszületett, illetve elhalálozott személy egészségügyi és személyazonosító adatait át kell adni. A születéssel, illetve halálozással kapcsolatos események anyakönyvezése céljából teljesítendő bejelentési kötelezettsége során a betegellátó megismerheti és továbbíthatja élveszületés esetén a gyermek szülei, halálozás esetén az életben lévő házastárs, bejegyzett élettárs személyi azonosító adatait.

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

III. Kamerarendszer üzemeltetése

1. A kamerarendszerrel szemben támasztott követelmények

1.1. A zárt rendszerű műszaki megoldással kiépített kamrarendszernek meg kell felelnie a mindenkori legmagasabb adatbiztonsági szint és a felvételek automatikus rögzítése követelményeinek.

1.2. A közönség számára nyilvános magánterület védelme esetén – jól látható helyen, jól olvashatóan, a területen megjelenni kívánó harmadik személyek tájékozódását elősegítő módon – figyelemfelhívó jelzést, ismertetést kell elhelyezni

a) arról a tényről, hogy az adott területen elektronikus megfigyelőrendszert alkalmaznak (térfigyelés);
b) az elektronikai vagyonvédelmi rendszer által folytatott megfigyelés, valamint a rendszer által rögzített, személyes adatokat tartalmazó kép- és hangfelvétel készítésének, tárolásának céljáról, az adatkezelés jogalapjáról, a felvétel tárolásának helyéről, a tárolás időtartamáról, a rendszert alkalmazó (üzemeltető) személyéről és elérhetőségéről, az adatok megismerésére jogosult személyek köréről, továbbá az információs önrendelkezési jogról és az információszabadságról szóló törvénynek az érintettek jogaira és érvényesítésük rendjére vonatkozó rendelkezéseiről.

1.3. Az Mt. 11/A. §-a és az Infotv. 14. § a) pontja alapján a munkáltatónak előzetesen tájékoztatnia kell a munkavállalót az elektronikus megfigyelő rendszer alkalmazásával együtt járó adatkezelés lényeges körülményeiről.

A munkavállalónak adott írásbeli tájékoztatásnak legalább ki kell terjednie:

- az adatkezelés jogalapjára,
- az egyes kamerák elhelyezésére és a vonatkozásukban fennálló célra, az általuk megfigyelt területre, tárgyra, illetőleg arra, hogy az adott kamerával közvetlen vagy rögzített megfigyelést végez-e a munkáltató,
- az elektronikus megfigyelő rendszert üzemeltető (jogi vagy természetes) személy meghatározására,
- a felvétel tárolásának helyére és időtartamára,
- a felvételek tárolásával kapcsolatos adatbiztonsági intézkedésekre,
- az adatok megismerésére jogosult személyek körére, illetőleg arra, hogy a felvételeket mely személyek, szervek részére, milyen esetben továbbíthatja,
- a felvételek visszanézésére vonatkozó szabályokra, illetőleg arra, hogy a felvételeket milyen célból használhatja fel a munkáltató,
- arra, hogy a munkavállalókat milyen jogok illetik meg az elektronikus megfigyelő rendszerrel összefüggésben és milyen módon tudják gyakorolni a jogaikat,
- arra, hogy az információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe.

Nem alkalmazható elektronikus megfigyelőrendszer olyan helyen, ahol a megfigyelés az emberi méltóságot sértheti, így különösen öltözőben, próbafülkében, mosdóban, illemhelyen.

2. A kamerarendszer üzemeltetője

2.1. A kamerarendszer üzemeltetésére a Zuglói Egészségügyi Szolgálat szerződést köt a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység részletes szabályairól szóló 2005. évi CXXXIII. törvény hatálya alá tartozó Zuglói Közbiztonsági non-profit Kft.-vel (székhelye: 1145 Budapest, Laky Adolf utca 36.) – továbbiakban: **Üzemeltető**.

3. Az adatkezelés

3.1. A kamerarendszer által rögzített felvételek (adatok) jogszabályoknak megfelelő kezelése az Üzemeltető feladata és felelőssége.

3.2. Az Üzemeltető az elektronikus megfigyelőrendszer működése útján kép-, hang-, valamint kép- és hangfelvételt a kötelezettségeit meghatározó szerződés keretei között, a szerződésből fakadó kötelezettségei teljesítése céljából, az információs önrendelkezési jogról és az információszabadságról szóló törvény szerinti adatvédelmi jogok érvényesítése mellett, illetve e törvényben meghatározott korlátozó rendelkezések betartásával készíthet, illetve kezelhet. E tevékenysége során vagyonőrzési feladatokat ellátó személy adatkezelőnek minősül.

3.3. Az elektronikus megfigyelőrendszer az egyéb törvényi feltételek megléte esetén is kizárólag akkor alkalmazható, ha ehhez a természetes személy kifejezetten hozzájárul. A hozzájárulás ráutaló magatartással is megadható. Ráutaló magatartás különösen, ha az ott tartózkodó természetes személy a magánterület közönség számára nyilvános részén az e fejezet 1.2. pontjában meghatározottaknak megfelelően elhelyezett ismertetés ellenére a területre bemegy, kivéve, ha a körülményekből egyértelműen más következik.

3.4. A felvételeket az Üzemeltetőnek a rögzítést követő 3 napon keresztül kell tárolnia. A rögzített kép-, hang-, valamint kép- és hangfelvételt felhasználás hiányában legfeljebb a rögzítéstől számított három munkanap elteltével meg kell semmisíteni, illetve törölni kell úgy, hogy azok többé ne legyenek helyreállíthatóak. Felhasználásnak az minősül, ha a rögzített kép-, hang-, vagy kép- és hangfelvételt, valamint más személyes adatot bírósági vagy más hatósági eljárásban bizonyítékként felhasználják.

3.5. A kamerarendszer által rögzített felvételekhez – az e fejezet 4. pontban foglaltak kivételével - kizárólag a rendszer üzemeltetője férhet hozzá, azokat csak a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen esetben jogosult megismerni, és a felvételeket csak a bíróság, a szabálysértési vagy más hatóság részére továbbíthatja, egyéb harmadik személy számára nem teheti hozzáférhetővé. A továbbításra kizárólag törvényben meghatározott esetekben és a felvételre igényt tartó adatkezelési jogalapjának megfelelő igazolása után kerülhet sor. A felvételeket a továbbítás megtörténte után haladéktalanul törölni kell.

4. Az adatok felhasználása, adatigénylés

4.1. A kamerarendszer által rögzített felvételek bizonyítékul használhatóak fel a rögzítés helyszínén elkövetett bűncselekmény vagy szabálysértés miatt indult büntető-, szabálysértési vagy más hatósági, bírósági eljárásban – ideértve az érintett személy által, jogainak érvényesítése céljából indított eljárásokat, akár a polgári peres eljárást is.

4.2. Az, akinek jogát vagy jogos érdekét a kép-, hang-, vagy a kép- és hangfelvétel, illetve más személyes adatának rögzítése érinti, a kép-, hang-, valamint kép- és hangfelvétel, illetve más személyes adat rögzítésétől számított három munkanapon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adatot annak kezelője ne semmisítse meg, illetve ne törölje.

4.3. Bíróság vagy más hatóság megkeresésére a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre attól számított harminc napon belül, hogy a megsemmisítés mellőzését kérték, nem kerül sor, a rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

4.4. A rögzített kép-, hang-, valamint kép- és hangfelvételt, valamint más személyes adatot csak az a személy- és vagyonvédelmi tevékenységet végző személy jogosult megismerni, akinek ez a szerződésből fakadó kötelezettségei érvényesítéséhez szükséges, és a jogsértő cselekmény megelőzése vagy megszakítása érdekében mellőzhetetlen.

4.5. A felvételek megismeréséről az Üzemeltető jegyzőkönyvet készít, amelynek tartalmaznia kell a rögzített felvétel adatait, az annak megismerésére jogosult személy nevét, továbbá az adatok megismerésének okát és idejét.

5. Az érintettek jogai és érvényesítésük

5.1. A felvételen szereplő természetes személy érintett számára biztosítani kell valamennyi, az információs önrendelkezési jogról és az információszabadságról szóló törvényben felsorolt jognak az ott meghatározott korlátozások figyelembevételével történő gyakorlását.

5.2. Az érintett kérelmére az adatkezelő tájékoztatást ad az érintett általa kezelt adatairól, az adatkezeléssel összefüggő tevékenységéről, továbbá – az érintett személyes adatainak továbbítása esetén – az adattovábbítás jogalapjáról és címzettjéről. Az érintett kérelmezheti az adatkezelőnél

a) tájékoztatását személyes adatai kezeléséről,
b) személyes adatainak – a felvételnek – a törlését vagy zárolását (8 nap elteltével a felvételek automatikusan törlődnek).

5.3. Az adatkezelő az adattovábbítás jogszerűségének ellenőrzése, valamint az érintett tájékoztatása céljából adattovábbítási nyilvántartást vezet, amely tartalmazza az általa kezelt személyes adatok továbbításának időpontját, az adattovábbítás jogalapját és címzettjét.

5.4. Az adatkezelő köteles a kérelem benyújtásától számított legrövidebb idő alatt, legfeljebb azonban 30 napon belül, írásban megadni a tájékoztatást. Ha az adatkezelő az érintett tájékoztatás, törlés vagy zárolás iránti kérelmét nem teljesíti, írásban közli a kérelem elutasításának ténybeli és jogi indokait.

5.5. A tájékoztatás, törlés vagy zárolás iránti kérelem elutasítása esetén az adatkezelő tájékoztatja az érintettet a bírósági jogorvoslat, továbbá a Nemzeti Adatvédelmi és Információszabadság Hatósághoz fordulás lehetőségéről. Az elutasított kérelmekről az adatkezelő a Nemzeti Adatvédelmi és Információszabadság Hatóságot évente a tárgyévet követő év január 31-éig értesíti.

5.6. Az érintett a jogainak megsértése esetén bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. A per elbírálása a törvényszék hatáskörébe tartozik. A per - az érintett választása szerint - az érintett lakóhelye vagy tartózkodási helye szerinti törvényszék előtt is megindítható.

6. Egyéb rendelkezések

6.1. „A Kamerarendszer üzemeltetése” című fejezet hatályos jogszabályoknak megfelelő aktualizálását Üzemeltető folyamatosan elvégzi.

6.2. Az e fejezetben nem szabályozott kérdésekben a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, , vonatkozó részeit kell alkalmazni.

IV. Hatálybalépés

Ez a szabályzat 2024.06.03. napján lép hatályba és egyidejűleg hatályát veszti az Intézet 2022.11.18. napján kiadott Adatvédelmi Szabályzat (10. kiadás)

V. Feljegyzések, nyomtatványok (Dokumentált információk):

Azonosító:	***Megnevezés:***
–	Irattári napló
–	Iratpótló lap
–	Selejtezhető dokumentumok jegyzőkönyve
–	Szervezeti egység adatvédelmi reszortfelelősök regisztrációs listája
–	Betegdokumentációról (beteg által) kért másolatok nyilvántartása
–	Esemény, rendkívüli esemény jelentésének tételes nyilvántartása
–	Egészségügyi és személyazonosító adatok külső továbbításának nyilvántartása
–	Aláírás minták
–	Éves adatvédelmi jelentés
–	Oktatási segédanyag
FNY 001	Elosztási jegyzék
FNY 004	Eltérésjelentés
FNY 049	Javaslat foglalkoztatásra
FNY 050	Oktatási bizonylat
FNY 079A	Kérelem egészségügyi dokumentációba való betekintésre és/vagy másolat készítésére (érintett saját adatairól)
FNY 079B	Kérelem egészségügyi dokumentációba való betekintésreés/vagy másolat készítésére (elhunyt páciens esetén)
FNY 079C	Betegdokumentumokról kért másolatok nyilvántartása
FNY 186	Adatvédelmi ellenőrzési nyilvántartás
FNY 189	Munkavégzésre irányuló jogviszonyban foglalkoztatott személy adatvédelmi és titoktartási nyilatkozata
C 5230-29.	Kézbesítőkönyv
C 5230/170a	Iktatókönyv (8 alszámos)
–	Hatásvizsgálat
–	Érdekmérlegelési teszt
–	Incidenskezelési nyilvántartás
–	„Az elektronikus megfigyelő rendszer alkalmazásával együtt járó adatkezelés lényeges körülményeiről” c. tájékoztató munkavállalók részére