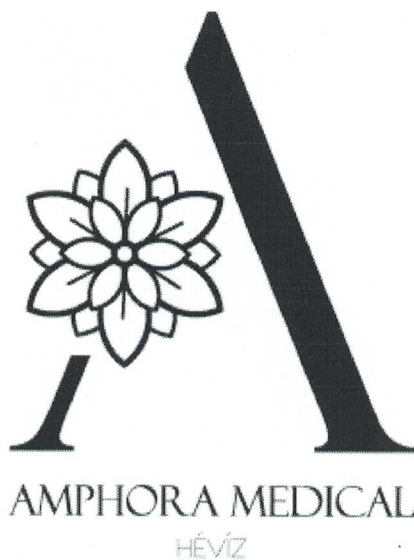


ADATKEZELÉSI SZABÁLYZAT

ARBELI Kft. – Amphora Medical Hévíz
Reuma- és Rehabilitációs Szakellátás



Érvényes: 2025. szeptember 26-tól visszavonásig
Készítette: ARBELI Kft. – Amphora Medical Hévíz egysége részére
Képviseli: Hódi György Zoltán, ügyvezető

Tartalomjegyzék

1. Általános rendelkezések	3
2. Jogszabályi háttér	3
3. Az adatkezelés célja és alapelvei	4
4. Az adatkezelés jogalapjai	4
5. Az adatkezelés részletes szabályai	5
6. Hozzáférési és jogosultsági szabályok	5
7. Az egészségügyi dokumentáció kezelése és megőrzése	6
8. Adatbiztonsági intézkedések	6
9. Adatvédelmi incidensek kezelése	7
10. Érintetti jogok és jogorvoslati lehetőségek	7
11. Felelősségi szabályok és adatvédelmi felelős	7
12. Záró rendelkezések	8
13. ARBELI Kft. szakmai program-specifikus adatkezelési szabályai	8
Melléklet-1: Adatvédelmi incidens-nyilvántartás	9
Melléklet-2: Páciensek hozzájáruló nyilatkozata	10
Melléklet-3: GDPR kérelmi minták	11
Melléklet-4: Adatvédelmi felelős kijelölése és feladatai	12

1. Általános rendelkezések

1.1. A szabályzat célja és hatálya

Jelen Adatkezelési Szabályzat (a továbbiakban: Szabályzat) célja, hogy részletesen meghatározza az ARBELI Kft. – Amphora Medical Hévíz által kezelt személyes és különleges (egészségügyi) adatok kezelésének elveit, módját, a kapcsolódó szervezeti és technikai intézkedéseket, valamint az érintettek jogainak gyakorlásához szükséges eljárásrendet. A Szabályzat hatálya kiterjed az intézmény valamennyi szervezeti egységére, minden alkalmazottra, továbbá mindazokra a külső szolgáltatókra és alvállalkozókra, akik a szolgáltató nevében (vagy annak érdekében) személyes adatokat kezelnek vagy hozzáférnek azokhoz.

1.2. Alapfogalmak

A Szabályzat alkalmazásában személyes adatnak minősül minden olyan információ, amely közvetve vagy közvetlenül természetes személyhez köthető, különleges adat pedig különösen az egészségi állapotra vonatkozó információ. Az adatkezelő az ARBELI Kft., adatfeldolgozó lehet az intézmény informatikai szolgáltatója, archiválással foglalkozó partnere, vagy más szerződött szolgáltató.

1.3. Elvek és felelősségmegosztás

Az adatkezelés szervezeti felelőssége az intézmény vezetését terheli: az intézményvezető felelős a szervezeti szabályok biztosításáért, az adatvédelmi felelős felügyeli a szabályzat végrehajtását. Minden munkavállaló köteles az adatvédelmi előírásokat betartani, és tudomására jutott incidenseket haladéktalanul jelenteni.

2. Jogszabályi háttér

2.1. Nemzeti jogszabályok

Az egészségügyi adatok kezelésével kapcsolatos főbb hazai jogszabályok az alábbiak: a 62/1997. (XII. 21.) NM rendelet, a 1997. évi XLVII. törvény az egészségügyi adatok kezeléséről, valamint a 1997. évi CLIV. törvény az egészségügyről. Ezek a jogszabályok részletesen szabályozzák az egészségügyi dokumentáció tartalmát, vezetését és megőrzését.

2.2. Infotv. és GDPR

Az Infotv. (2011. évi CXII. törvény) keretezi az információs önrendelkezési jogot és az adatvédelmi alapelveket, míg az EU által elfogadott GDPR (2016/679/EU) közös szabályrendszert biztosít az EU tagállamai részére. A GDPR vonatkozó cikkei (pl. 5., 6., 9., 15–22., 32–34. cikkek) meghatározzák az adatkezelés alapelveit, jogalapjait, az érintetti jogok gyakorlásának rendjét, valamint az adatbiztonsági követelményeket.

2.3. Hatósági előírások és nemzeti kiegészítések

A Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) iránymutatásai és határozatai, valamint az illetékes egészségügyi hatóságok (pl. ÁNTSZ/OKFŐ) útmutatásai szintén irányadóak az intézmény működtetése során. A Szabályzat készítésekor figyelembe vettük a hatályos jogértelmezéseket és gyakorlati követelményeket.

3. Az adatkezelés célja és alapelvei

3.1. Adatkezelési célok

Az adatkezelés elsődleges célja a betegellátás biztosítása: a klinikai döntéshozatal támogatása, a diagnosztikai és terápiás beavatkozások dokumentálása, a rehabilitációs folyamatok követése, valamint a jogszabályi kötelezettségek teljesítése (pl. statisztikai adatszolgáltatás). További célok lehetnek a belső minőségbiztosítás, oktatás és kutatás – azonban kutatás kizárólag az érintett tájékozott hozzájárulásával végezhető.

3.2. Alkalmazott elvek

A kezelések és az adatgyűjtés során az intézmény betartja a célhoz kötöttség, adattakarékosság és a pontosság elvét. Minden adatkezelési műveletre meg kell határozni a jogalapot, a célhoz szükséges adattartalmat és a megőrzési időt.

3.3. Különleges adatok kezelése

Az egészségügyi adatok különleges kategóriába tartoznak; kezelésük külön jogalapot igényel (pl. jogi kötelezettség, egészségügyi ellátás nyújtása, vagy kifejezett hozzájárulás). Az ilyen adatok hozzáférését és feldolgozását a Szabályzat szigorúan korlátozza.

4. Az adatkezelés jogalapjai

4.1. GDPR 6. cikk szerinti jogalapok

Az adatkezelés jogszerűségét a GDPR 6. cikkének (1) bekezdésében foglaltak alapján kell vizsgálni: a) hozzájárulás, b) szerződés teljesítése, c) jogi kötelezettség teljesítése, d) létfontosságú érdek, e) közérdekű feladat vagy közhatalmi jogosítvány, f) jogos érdek.

4.2. Különleges adatok – GDPR 9. cikk

Egészségügyi adatok kezelésének jogalapjai a GDPR 9. cikke szerint: kifejezett hozzájárulás, egészségügyi ellátás céljából történő kezelés jogi kötelezettség mellett, vagy vonatkozhat rá speciális nemzeti jogi szabályozás (pl. Eüak.).

4.3. Jogalap megfelelés dokumentálása

Minden adatkezelési műveletnél kötelező nyilvántartani a jogalapot és az arra vonatkozó indokolást. A nyilvántartás tartalmazza az adat típusa, célja, jogalapja, megőrzési ideje és az érintetti tájékoztatás módja.

5. Az adatkezelés részletes szabályai

5.1. Adatkezelési kategóriák

Az intézmény az adatokat a következő kategóriák szerint kezeli: azonosító adatok (név, születési adatok, lakcím, adószám, TAJ szám, személyazonosító igazolványok...), kontaktszemély adatai, egészségügyi adatok (anamnézis, vizsgálati eredmények, diagnózisok, terápiák), adminisztratív adatok (térítési információk, számlázás).

5.2. Adatgyűjtés és -beviteli szabályok

Az adatokat pontosan és teljes körűen kell rögzíteni. Betegfelvételnél mindig tájékoztatni kell az érintettet az adatkezelés céljáról és jogalapjáról, valamint a jogaik gyakorlásáról. Az adatbevitel során tilos felesleges vagy irreleváns adatok gyűjtése.

5.3. Adattovábbítás és adatfeldolgozók

Adattovábbítás harmadik fél részére kizárólag jogszabályi kötelezettség, az érintett hozzájárulása vagy szerződés teljesítése esetén történhet. Minden adatfeldolgozóval írásos szerződést kell kötni, amely tartalmazza az adatvédelemre vonatkozó kötelezettségeket.

6. Hozzáférési és jogosultsági szabályok

6.1. Jogosultságok megadása és nyilvántartása

A hozzáféréseket az intézmény vezetése és az informatikai felelős közösen határozzák meg, a legkisebb jogosultság elve szerint. Minden jogosultságot részletesen nyilvántartunk (ki, mikor, miért kapta).

6.2. Azonosítás és hitelesítés

Minden munkatársnak egyedi felhasználói azonosító és erős jelszó szükséges. Többlépcsős hitelesítés (MFA) alkalmazása ajánlott az adminisztratív és egészségügyi rendszerekhez való hozzáférésnél. A jelszókezelésre vonatkozó szabályokat a mindenkor szerződött rendszergazda határozza meg.

6.3. Hozzáférés-ellenőrzés és naplózás

Minden hozzáférést és adatmódosítást naplózni kell. A naplók rendszeres (legalább negyedéves) vizsgálata kötelező. Jogosulatlan hozzáférés gyanúja esetén azonnali intézkedést kell kezdeményezni.

7. Az egészségügyi dokumentáció kezelése és megőrzése

7.1. Dokumentáció tartalma

Az egészségügyi dokumentáció tartalmazza a betegazonosítókat, anamnézist, vizsgálati eredményeket (labor, képalkotó), diagnózisokat, beavatkozások leírását, gyógyszerelési adatokat, a beteg tájékoztatásának dokumentációját és zárójelentést. Az adatokat felhőtárhelyen a szerződött, akreditált egészségügyi szoftver üzemeltetője kezeli. A kezelt paciensek email, CD és igény szerint nyomtatott formában is megkapják a dokumentációt. Az intézmény nem tárol egészségügyi dokumentációt!

7.2. Megőrzési idő-kategóriák

A dokumentumokat az alkalmazandó jogszabályok szerint kell megőrizni, mely a szerződött egészségügyi szoftver üzemeltetőjének felelőssége: alapbetegkarton és zárójelentés minimum 30 év, képalkotó felvételek minimum 10 év, egyes speciális esetek hosszabb megőrzést igényelhetnek.

7.3. Archiválás és selejtezés

Az archiválás biztonságos, nyomon követhető módon történik. A selejtezés csak a jogszabályoknak megfelelő módon, dokumentált selejtezési jegyzőkönyv alapján lehetséges.

8. Adatbiztonsági intézkedések

8.1. Műszaki intézkedések

A műszaki intézkedések közé tartoznak a szerverek védelme, tűzfalak, behatolás-észlelő rendszerek, titkosítás az adattovábbításnál és adattárolásnál, rendszeres szoftverfrissítések és sebezhetőség-ellenőrzések, mely szerződött közreműködő partner bevonásával történik.

8.2. Szervezési intézkedések

Szervezési intézkedés például a hozzáférési politika, belső adatvédelmi eljárások, belső auditok, munkaköri leírásokba épített adatvédelmi kötelezettségek és rendszeres oktatások megtartása.

8.3. Mentési és helyreállítási tervek

Részletes adatmentési politika szerint napi inkrementális mentés és napi teljes mentés történik. Vészhelyzeti helyreállítási terv (Disaster Recovery Plan) és üzletmenet-folytonossági terv (BCP) áll rendelkezésre.

9. Adatvédelmi incidensek kezelése

9.1. Incidens meghatározása és osztályozása

Adatvédelmi incidens minden olyan esemény, amely adatvesztéshez, jogosulatlan hozzáféréshez vagy adattovábbításhoz vezet. Az incidenseket súlyosságuk szerint osztályozzuk: alacsony, közepes és súlyos kockázat.

9.2. Incidens-eljárás

Az észlelést követően azonnal értesíteni kell az adatvédelmi felelőst, aki elindítja a kivizsgálást, dokumentálja az eseményt, és szükség esetén értesíti a NAIH-ot a GDPR szerinti 72 órán belüli bejelentési kötelezettség szerint.

9.3. Kommunikáció és helyreállítás

Az érintettek értesítése a kockázat mértékétől függően történik. A helyreállítási intézkedések közé tartozik az érintett rendszerek izolálása, adat-helyreállítás, jogi és PR-egyeztetés.

10. Érintetti jogok és jogorvoslati lehetőségek

10.1. Tájékoztatáshoz való jog

Az érintetteket tájékoztatni kell arról, milyen adatokat kezel az intézmény, milyen célból, meddig, és ki az adatkezelő. A tájékoztatás történhet szóban, írásban vagy elektronikus úton.

10.2. Hozzáférés, helyesbítés, törlés

Az érintettek kérhetnek hozzáférést a róluk kezelt adatokhoz, kérhetik azok helyesbítését vagy törlését a GDPR-ban meghatározott feltételek szerint. A kérelmeket dokumentálni és 1 hónapon belül elbírálni kell.

10.3. Panasz és jogorvoslat

Az érintett panasszal fordulhat az intézmény adatvédelmi felelőséhez, illetve közvetlenül a NAIH-hoz. Jogviták esetén a polgári bíróság előtt is érvényesíthetők jogok.

11. Felelősségi szabályok és adatvédelmi felelős

11.1. Intézményi kötelezettségek

Az intézmény vezetése biztosítja a jogszabályi megfelelést, erőforrásokat biztosít az adatvédelemhez, és jóváhagyja a belső eljárásokat. A munkavállalókat rendszeresen képezni kell.

11.2. Adatvédelmi felelős (DPO)

Az intézmény kinevez egy adatvédelmi felelőt (DPO), akinek feladata a szabályzat betartásának ellenőrzése, kapcsolattartás a NAIH-val, incidenskezelés, és a dolgozók képzése.

11.3. Szerződéses és fegyelmi felelősség

Adatvédelmi kötelezettségek megszegése esetén fegyelmi és szerződéses jogi lépések hozhatók az érintett munkavállaló vagy partner ellen.

12. Záró rendelkezések

12.1. Hatálybalépés és felülvizsgálat

Ez a Szabályzat 2025. szeptember 26-án lép hatályba. A szabályzatot legalább háromévente felül kell vizsgálni, vagy haladéktalanul aktualizálni jogszabályváltozás esetén.

12.2. Aláírás és nyilvánosság

A Szabályzatot az intézmény vezetője hagyja jóvá. A munkavállalók számára hozzáférhetővé kell tenni, és a páciensek számára rövidített tájékoztató formában biztosítani kell.

12.3. Mellékletek és kapcsolódó dokumentumok

A Szabályzat mellékletei részletezik a gyakorlati űrlapokat és nyilvántartásokat, és részét képezik a szabályzatnak.

13. Az ARBELI Kft. szakmai program-specifikus adatkezelési szabályai

13.1. Reumatológiai ellátás

A reumatológiai szakrendelés során gyűjtött adatok (anamnézis, fizikális vizsgálat, labor- és képalkotó leletek, kezelési terv) részletes dokumentálást igényelnek. A vizsgálati leletekhez csak a kezelőorvosok és az ellátásban közreműködő szakemberek férhetnek hozzá.

13.2. Fizioerápia és rehabilitáció

A fizioerápiás kezelések naplóit, kezelési lapjait és a beteggel folytatott konzultációk feljegyzéseit elektronikus rendszerben kell vezetni, a kezelési protokollok és a beteggel egyeztetett célok egyértelmű rögzítésével.

13.3. Balneoterápia és speciális kezelések

A fürdő- és iszapkezelésekre vonatkozó adatokat (kezelési időpontok, indikációk, ellenjavallatok) külön kezelési lapokon kell rögzíteni és megőrizni.

13.4. Infekciókontroll dokumentáció

Fertőzés gyanú vagy bekövetkezett fertőzés esetén a fertőzések bejelentésére és nyilvántartására vonatkozó belső eljárásokat követni kell, különös tekintettel az adatvédelmi és járványügyi jelentési kötelezettségekre.

Hévíz, 2025.09.26.



ARBELI Kft.
2049 Dósd, Sajó u. 1/A.
Adószám: 24952554-2-13
HÉVÍZ: HUS8 10700268-71218427-51100005

Hódi György Zoltán

ügyvezető

Melléklet-4: Adatvédelmi felelős kijelölése és feladatai

Intézmény: ARBELI Kft. – Amphora Medical Hévíz

Adatvédelmi felelős neve: Hódi György Zoltán

Elérhetősége: gm@amphoramedical.hu

Feladatai:

- A Szabályzat végrehajtásának ellenőrzése és a munkatársak folyamatos tájékoztatása;
- Adatvédelmi incidensek nyilvántartása és kivizsgálása;
- Kapcsolattartás a NAIH-val és egyéb hatóságokkal;
- Rendszeres éves jelentések készítése az adatkezelési tevékenységről;

Kelt: Hévíz 2025.09.26.

Aláírás: 
ARBELI Kft.
2049 Dózsa Sándor u. 1/A.
Adószám: 24932584-2-13
Bszsz.: HU98 10700268-71218427-51100005

Jelen dokumentumot az ARBELI Kft. készítette. A tárolt és kezelt adatok védelméért az intézmény teljes felelősséget vállal.