



KOMLÓI EGÉSZSÉGCENTRUM, Bányászati Utókezelő és
Éjjeli Szanatórium Egészségügyi Központ
H-7300 KOMLÓ, MAJÁLIS TÉR 1.
TEL.: (36 72) 582 340
FAX: (36 72) 482 045



INFORMATIKAI BIZTONSÁGI SZABÁLYZAT

Érvényes: 2018. május 25-től

Készítette:


Fejes Éva

Gazdasági igazgató

Jóváhagyta:



Dr. Tanczos Frigyes Attila
főigazgató

1. Az Informatikai Biztonsági Szabályzat célja

A szabályzat alapvető célja, hogy az informatikai rendszer alkalmazása során biztosítsa az adatvédelem elveinek, az adatbiztonság követelményeinek érvényesülését, s megakadályozza a jogosulatlan hozzáférést, az adatok megváltoztatását és jogosulatlan nyilvánosságra hozatalát.

Az IBSZ célja továbbá:

- a titok-, vagyon- és tűzvédelemre vonatkozó védelmi intézkedések betartása,
- az üzemeltetett informatikai rendszerek rendeltetésszerű használata,
- az üzembiztonságot szolgáló karbantartás és fenntartás,
- az adatok informatikai feldolgozása és azok további hasznosítása során az illetéktelen felhasználásból származó hátrányos következmények megszüntetése, illetve minimális mértékre való csökkentése,
- az adatállományok tartalmi és formai épségének megőrzése,
- az alkalmazott programok és adatállományok dokumentációinak nyilvántartása,
- a munkaállomásokon lekérdezhető adatok körének meghatározása,
- az adatállományok biztonságos mentése,
- az informatikai rendszerek zavartalan üzemeltetése,
- a feldolgozás folyamatát fenyegető veszélyek megelőzése, elhárítása,
- az adatvédelem és adatbiztonság feltételeinek megteremtése
- GDPR alapelveinek érvényesítése

A szabályzatban meghatározott védelemnek működni kell a rendszerek fennállásának egész időtartama alatt a megtervezésüktől kezdve az üzembe helyezésen keresztül az üzemeltetésig. A jelen IBSZ az adatvédelem általános érvényű előírását tartalmazza, meghatározza az adatvédelem és adatbiztonság feltételrendszerét.

2. Az Informatikai Biztonsági Szabályzat hatálya

2.1. Személyi hatálya

Az IBSZ személyi hatálya kiterjed a Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ (továbbiakban: intézmény) egész területére.

2.2. Tárgyi hatálya

- kiterjed a védelmet élvező elektronikus adatok teljes körére, felmerülésük és feldolgozási helyüktől, idejüktől és az adatok fizikai megjelenési formájuktól függetlenül,
- kiterjed az intézmény tulajdonában lévő, illetve az általa bérelt valamennyi informatikai berendezésre,
- valamint az informatikai eszközök műszaki dokumentációira,
- kiterjed az informatikai folyamatban szereplő összes dokumentációra (fejlesztési, szervezési, programozási, üzemeltetési),
- kiterjed a rendszer- és felhasználói programokra,
- kiterjed az adatok felhasználására vonatkozó utasításokra,

- kiterjed az adathordozók tárolására, felhasználására.

3. Az adatkezelés során használt fontosabb fogalmak

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 - valamint az adatból levonható, az érintettre vonatkozó következtetés

Adatkezelés: az alkalmazott eljárástól függetlenül az adatok gyűjtése, felvétele és tárolása, feldolgozása, hasznosítása (ideértve a továbbítást és a nyilvánosságra hozatalt) és törlése. Adatkezelésnek számít az adatok megváltoztatása és további felhasználásuk megakadályozása is;

Adatfeldolgozás: az adatkezelési műveletek, technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől.

Adat továbbítás: ha az adatot meghatározott harmadik fél számára hozzáférhetővé teszik.

Adatkezelő: az a természetes vagy jogi személy, aki vagy amely az adatok kezelésének célját meghatározza, az adatkezelésre vonatkozó döntéseket meghozza és végrehajtja, illetőleg a végrehajtással adatfeldolgozót bízhat meg.

Adatfeldolgozó: az a természetes vagy jogi személy, aki vagy amely az adatkezelő megbízásából adatok feldolgozását végzi.

Nyilvánosságra hozatal: ha az adatot bárki számára hozzáférhetővé teszik;

Adatbiztonság: az adatkezelő, illetőleg tevékenységi körében az adatfeldolgozó köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek az adat- és titokvédelmi szabályok érvényre juttatásához szükségesek.

Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg sérülés vagy a megsemmisülés ellen.

Adatvédelmi incidens: Az adatbiztonság olyan sérülése, mely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.

4. Az IBSZ biztonsági fokozata

Az intézmény adatai különböző biztonsági fokozatba tartozhatnak. (üzleti titkok, pénzügyi adatok, illetve az intézmény belső szabályozásában hozzáférés-korlátozás alá eső (pl. egyes feladatok végrehajtása érdekében bizalmas) és a nyílt adatok feldolgozására, tárolására alkalmas adatok)

5. Kapcsolódó szabályozások

Az IBSZ előírásai összhangban vannak:

- Leltározási és értékelési szabályzattal,
- Számviteli politikával
- Adatvédelmi és adatbiztonsági szabályzattal

1. A személyes adatok kezelésére vonatkozó elvek

A Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ a vele kapcsolatba kerülő természetes személyek adatait az alábbi elvek betartása mentén tartja nyilván:

- jogszerűség, tisztességes eljárás és átláthatóság
- célhoz kötöttség
- adattakarékosság
- pontosság
- korlátozott tárolhatóság
- integritás és bizalmas jelleg
- elszámoltathatóság

2. Az adatkezelés jogalapjai

A Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ a vele kapcsolatba kerülő természetes személyek adatait az alábbi elvek betartása mentén tartja nyilván:

- az érintett hozzájárulása;
- szerződéskötés
- jogi kötelezettség teljesítése
- létfontosságú érdek
- közérdekű adatkezelés
- jog, jogos érdek, érdekmérlegelés

Ha az adatkezelés hozzájáruláson alapul, az adatkezelőnek képesnek kell lennie annak igazolására, hogy az érintett személyes adatainak kezeléséhez hozzájárult

Az érintett személyes adatainak jogos érdek alapján történő kezelése esetén érdekmérlegelést végzünk, melynek során:

- beazonosítjuk és rögzítjük a jogos érdeket
- beazonosítjuk és rögzítjük az érintett érdekeit és jogait
- szükségesség és arányosság, a célhoz kötöttség, adattakarékosság, korlátozott tárolhatóság elve alapján mérlegelés
- tájékoztatjuk az érintettet az érdekmérlegelésről

Az érintettnek tiltakozási joga van, mely alapján a személyes adatot nem kezeljük tovább, kivéve, ha az adatkezelést kényszerítő ok indokolja *(pl. munkaviszonnyal összefüggésben szükségszerűen kezelendő adatok esetén)*

3. Az adatkezelés célja

Az intézmény az alábbi célokból végez adatkezelést a jogszabályokkal összhangban:

1997. évi XLVII. törvény alapján az alaptevékenység: betegellátás nyújtásához kapcsolódóan a betegek adatait kezeljük;
- munkavállalók adatainak kezelése;
- szerződéses partnerek kapcsolattartói adatainak kezelése a szerződés teljesítése céljából;
- vagyonvédelem, személyi biztonság;
- törvényben meghatározott kötelezettség teljesítése céljából.

Az egészségügyi dokumentáció tartalmazza:

- a betegről felvett személyi adatokat (név, születési dátum, lakhely, stb.)
- a gyógykezelés során rögzített egészségügyi adatokat (az érintett testi, értelmi és lelki állapotára, kóros szenvedélyére, valamint a megbetegedés, illetve az elhalálozás körülményeire, a halál okára vonatkozó adatok)
- mindazt, amit a beteg elmondott megbetegedése körülményeiről, tüneteiről, korábbi betegségeiről
- a vizsgálati eredményeket, a betegség megnevezését, az elvégzett beavatkozásokat, a gyógyszeres terápiákat.

Az egészségügyi dokumentációt a kezelőorvos a kezelés során folyamatosan vezeti, abba a beteg vizsgálatával és gyógykezelésével kapcsolatos minden adatot köteles rögzíteni.

4. Az adatkezelés időtartama:

A Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ az adatok megőrzésének időtartamáról tájékoztatja az érintetteket.

- A számlákat jogi kötelezettség miatt legalább 8 évig megőrizzük. A számlakiállítás alapjául szolgáló iratok megőrzési ideje 8 év.
- A munkaviszony, közalkalmazotti jogviszony, közreműködői jogviszony alapjául szolgáló iratok megőrzési ideje: 50 év.
- Szerződés teljesítéséhez kapcsolódó adatok megőrzése: 5 év.
- Pályázati projektek elszámolásához kapcsolódó adatok megőrzése a támogatási szerződésben meghatározott időtartam.
- Zárójelentés megőrzési ideje 50 év
- Egészségügyi dokumentáció megőrzési ideje 30 év
- Képkötő diagnosztikai eljárással készített felvétel megőrzési ideje 10 év, a felvételtől készített lelet megőrzési ideje 30 év

5. Az érintettek jogai

A személyes adataihoz kapcsolódóan az érintettnek a jogszabályban meghatározott jogai vannak.

- a) hozzáférés joga
- b) a helyesbítés joga
- c) a törléshez való joga
- d) az adat kezelésének korlátozásához való joga
- e) a személyes adatok helyesbítéséhez vagy törléséhez, illetve az adatkezelés korlátozásához kapcsolódó értesítési kötelezettség
- f) az adathordozhatósághoz való joga
- g) tiltakozáshoz való joga

6. Az érintettek tájékoztatásának folyamata

A Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ, mint adatkezelő megfelelő intézkedéseket hoz annak érdekében, hogy az érintett részére a személyes adatok kezelésére vonatkozó valamennyi információt és minden egyes tájékoztatást tömör, átlátható, érthető és könnyen hozzáférhető formában, világosan és közérthetően megfogalmazva nyújtsa, különösen a gyermekeknek címzett bármely információ esetében. Az információkat írásban vagy más megfelelő módon - ideértve adott esetben az elektronikus utat is – adja meg. Az érintett kérésére szóbeli tájékoztatás is adható, feltéve, hogy más módon igazolták az érintett személyazonosságát.

- Személyes adatok gyűjtése közvetlenül az érintettektől:

Ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtjük, akkor a személyes adatok megszerzésének időpontjában az alábbi információkról tájékoztatjuk az érintetteket:

- a) az adatkezelőnek és az adatkezelő képviselőjének megnevezése és elérhetőségei:

Adatkezelő neve: Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ
 Elérhetőségei: 7300 Komló, Majális tér 1., Pf.: 82., Tel: 06 – 72 / 582 340

- b) a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja;
- c) ha az adatkezelés egy harmadik fél jogos érdekeinek érvényesítéséhez szükséges, a harmadik fél jogos érdekei;

A tisztességes és átlátható adatkezelést biztosítsa, az érintettet a következő kiegészítő információkról tájékoztatja:

- a) a személyes adatok tárolásának időtartamáról,
- b) az érintett azon jogáról, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen, valamint az érintett adathordozhatósághoz való jogáról;

- c) a hozzájárulás bármely időpontban történő visszavonásához való jog, amely nem érinti a visszavonás előtt a hozzájárulás alapján végrehajtott adatkezelés jogszerűségét;
- d) a felügyeleti hatósághoz címzett panasz benyújtásának jogáról;
- e) arról, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményekkel járhat az adatszolgáltatás elmaradása;

Ha az adatkezelő a személyes adatokon a gyűjtésük céljától eltérő célból további adatkezelést kíván végezni, a további adatkezelést megelőzően tájékoztatja az érintettet erről az eltérő célról és minden releváns kiegészítő információról.

- Személyes adatok gyűjtése egyéb forrásból

Ha a személyes adatokat nem az érintettől szereztük meg, akkor az előbb felsorolt információkon kívül a következőkről tájékoztatjuk még az érintetteket.

- a) az érintett személyes adatok kategóriái
- b) a személyes adatok forrása és adott esetben az, hogy az adatok nyilvánosan hozzáférhető forrásokból származnak-e.

7. Az adatfeldolgozás folyamata

Az adatfeldolgozás során nem veszünk igénybe adatfeldolgozót.

8. Védelmet igénylő, az informatikai rendszerre ható elemek

Az informatikai rendszer egymással szervesen együttműködő és kölcsönhatásban lévő elemei határozzák meg a biztonsági szempontokat és védelmi intézkedéseket.

Az informatikai rendszerre az alábbi tényezők hatnak:

- a környezeti infrastruktúra,
- a hardver elemek,
- az adathordozók,
- a dokumentumok,
- a szoftver elemek,
- az adatok,
- a rendszerelemekkel kapcsolatba kerülő személyek.

8.1. A védelem tárgya

- A védelmi intézkedések kiterjednek:
- az alkalmazott hardver eszközökre és azok működési biztonságára,
- az informatikai eszközök üzemeltetéséhez szükséges okmányokra és dokumentációkra,
- az adatokra és adathordozókra, a megsemmisítésükig, illetve a törlésre szánt adatok felhasználásáig,

- az adatfeldolgozó programrendszerekre, valamint a feldolgozást támogató rendszer szoftverek tartalmi és logikai egységére, előírászerű felhasználására, reprodukálhatóságára,

8.2. A védelem eszközei

A mindenkori technikai fejlettségnek megfelelő műszaki, szervezeti, programozási, jogi intézkedések azok az eszközök, amelyek a védelem tárgyának különböző veszélyforrásokból származó kárt okozó hatásokkal, szándékokkal szembeni megóvását elősegítik, illetve biztosítják.

9. Elektronikus térfigyelő rendszerrel kapcsolatos adatkezelés

A Komlói Egészségközpont, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ (7300 Komló, Majális tér 1.) területén, az épületen belüli, illetve az épületen kívüli mozgást elektronikus megfigyelő rendszerrel (továbbiakban: kamerákkal) figyeljük, mely során személyes adatokat tartalmazó képfelvételek készülnek. Az adatkezeléshez történő hozzájárulás önkéntes, ráutaló magatartással történik. Ön az intézmény területére történő belépéssel és az itt tartózkodással hozzájárulását adja a képfelvétellel kapcsolatos adatkezeléshez

9.1. Adatkezelés célja

A megfigyelés és a képfelvételek rögzítésének célja az intézmény területén tartózkodó személyek életének, testi épségének valamint a kollégium vagyontárgyainak védelme. További cél a jogsértések megelőzése és észlelése, az elkövető tettenérése, illetve a felvételek bizonyítékként történő felhasználása a hatósági eljárások keretében.

9.2. Az adatkezelés jogalapja

Az intézmény dolgozói, betegek, látogatói az elektronikus térfigyelő rendszerrel végzett adatkezelésről tájékoztatást kapnak. Az elektronikus térfigyelő rendszer alkalmazásáról a területen megjelenni kívánó további személyek részére jól látható helyen, jól olvashatóan, tájékozódást elősegítő módon, ismertetőt kell kihelyezni. Az ismertető szövegét a szabályzat 3. melléklete tartalmazza. Az elektronikus térfigyelő rendszer alkalmazásához a közalkalmazotti vagy egyéb munkavégzés ellátására irányuló jogviszonyban nem álló személyek hozzájárulása önkéntes, ráutaló magatartással történik, akik az épületbe lépésükkel elfogadják, hogy róluk felvételek készülhetnek, és azok a szabályzatban meghatározottak szerint felhasználhatók.

9.3. Az adatkezelés időtartama

A képfelvételeket 3 napig tároljuk.

9.4. Az adatkezelés jogosultsági köre

A kamerákkal folyamatosan sugárzott képek megtekintésére kizárólag a szabályzat 2. mellékletében felsorolt személyek jogosultak. A kamerák által készített és tárolásra került

felvételeket kizárólag a rendszergazda, főigazgató, illetve a főigazgató által megbízott vezető nézheti vissza. A kamerák által készített és tárolásra került felvételekről mentést kizárólag informatikusok készíthetnek.

9.5. Az adatbiztonsági intézkedések

A képfelvételek megtekintésére és visszanezésére szolgáló monitor úgy kerül elhelyezésre, hogy a képfelvételek sugárzása alatt azokat a jogosultsági körön kívül más személy ne láthassa. A megfigyelést és a tárolt képfelvételek visszanezését kizárólag a jogsértő cselekmények kiszűrése, az azok megszüntetéséhez szükséges intézkedések kezdeményezése céljából tehetik. A kamerák által sugárzott képekről a központi felvevő egységen kívül más eszközzel felvételt készíteni nem lehet. A tárolt képfelvételekhez történő hozzáférés csak biztonságos módon, és csak úgy történhet, hogy az adatkezelő személye azonosítható legyen. A tárolt képfelvételek visszanezését és a képfelvételekről készített mentést dokumentálni kell. A jogosultság indokának megszűnése esetén a tárolt képfelvételekhez történő hozzáférést haladéktalanul meg kell szüntetni. A rögzítő készülékben elkülönített merevlemezező fut az operációs rendszer, és a rögzítésre került felvételeket is csak ezen a merevlemezen tárolják. A felvételekről külön biztonsági másolat nem készül. Jogsértő cselekmény észlelését követően a szükséges hatósági eljárás haladéktalan megkezdéséről és a cselekményről készült felvételek tárolásáról intézkedni kell, egyben tájékoztatni kell a hatóságot, hogy a cselekményről képfelvétel készült.

9.6. Kamerák elhelyezése

Az intézmény épületén belül 9 darab, a főépület bejáratánál 3 darab kamera található. A kamerák pontos helye és az általuk megfigyelt területek az alábbiak:

- főépület DNY-i sarkán elhelyezett kamerák 2 db: főbejárat és D-i bejárat.
- főépület NY-i oldalán 1 db: hátsó és élelmezés bejárat.
- sebészeti osztály 5 db belső kamera
- betegfelvétel 2 db belső kamera
- sürgősségi betegfogadó 1 db belső kamera

9.7. Az érintettek jogai

Érintett: bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy (az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény 3. § 1. pont).

Akinek jogát vagy jogos érdekét a képfelvétel, illetve más személyes adatának rögzítése érinti, a képfelvétel, illetve más személyes adat rögzítésétől számított három napon belül jogának vagy jogos érdekének igazolásával kérheti, hogy az adat ne kerüljön megsemmisítésre, illetve törlésre. Bíróság vagy más hatóság megkeresésére a rögzített képfelvételt, valamint más személyes adatot a bíróságnak vagy a hatóságnak haladéktalanul meg kell küldeni. Amennyiben megkeresésre a megsemmisítés mellőzésének kérésétől számított harminc napon belül nem kerül sor, a rögzített képfelvételt, valamint más személyes adatot meg kell semmisíteni, illetve törölni kell.

Az érintett kérelmezheti a tájékoztatását személyes adatai kezeléséről, a személyes adatainak helyesbítését, valamint a személyes adatainak – a kötelező adatkezelés kivételével – törlését vagy zárolását.

Az érintett tiltakozhat személyes adatának kezelése ellen,

- a) ha a személyes adatok kezelése vagy továbbítása kizárólag az adatkezelőre vonatkozó jogi kötelezettség teljesítéséhez vagy az adatkezelő, adatátvevő vagy harmadik személy jogos érdekének érvényesítéséhez szükséges, kivéve kötelező adatkezelés esetén,
- b) ha a személyes adat felhasználása vagy továbbítása közvetlen üzletszerzés, közvélemény-kutatás vagy tudományos kutatás céljára történik, valamint
- c) törvényben meghatározott egyéb esetben. A tiltakozást a kérelem benyújtásától számított legrövidebb időn belül, de legfeljebb 15 napon belül a kollégiumvezető megvizsgálja, annak megalapozottsága kérdésében döntést hoz, és döntéséről a kérelmezőt írásban tájékoztatja.

Az érintett a jogainak megsértése esetén az adatkezelő ellen bírósághoz fordulhat. A bíróság az ügyben soron kívül jár el. Azt, hogy az adatkezelés a jogszabályban foglaltaknak megfelel, az adatkezelő köteles bizonyítani.

10. A védelem felelőse

A védelem felelőse a mindenkori informatikai vezető és rendszergazdák.

A jelen szabályzatban foglaltak szakszerű végrehajtásáról az intézmény vezetőinek kell gondoskodnia.

10.1. Adatvédelmi felelősök feladatai

- Informatikai vezető feladatai:
- az IBSZ kezelése, naprakészen tartása, módosítások átvezetése,
- javaslatot tesz a rendszer szűk keresztmetszeteinek felszámolására.
- meghatározza a védett adatok körét,
- ellátja az adatkezelés és adatfeldolgozás felügyeletét,
- ellenőrzi a védelmi előírások betartását,
- az adatvédelmi tevékenységet segítő nyilvántartási rendszer kialakítása,
- az adatvédelmi feladatok ismertetése,
- ellenőri tevékenységét adminisztrálja.
- ellenőrzi a szoftverek használatának jogszerűségét

b) Rendszergazda feladatai:

a rendszergazda a saját feladatkörébe tartozó rendszert felügyeli, felelős az informatikai rendszerek üzembiztonságáért, szerverek adatairól biztonsági másolatok

készítéséért és karbantartásáért,
 gondoskodik a rendszer kritikus részeinek újra indíthatóságáról, illetve az újra indításhoz szükséges paraméterek reprodukálhatóságáról,
 feladata a védelmi eszközök működésének folyamatos ellenőrzése,
 felelős az intézmény informatikai rendszer hardver eszközeinek karbantartásáért,
 nyilvántartja a beszerzett, illetve üzemeltetett hardver és szoftver eszközöket,
 gondoskodik a folyamatos vírusvédelemről
 a vírusfertőzés gyanúja esetén gondoskodik a fertőzött rendszerek vírusmentesítéséről,

folyamatosan figyelemmel kíséri és vizsgálja a rendszer működésére és biztonságára szempontjából a lényeges paraméterek alakulását, ellenőrzi a rendszer adminisztrációját,

10.2. Az informatikai vezető ellenőri feladatai

évente egy alkalommal részletesen ellenőrzi az IBSZ előírásainak betartását, rendszeresen ellenőrzi a védelmi eszközökkel való ellátottságot, előzetes bejelentési kötelezettség nélkül ellenőrzi az informatikai munkafolyamat bármely részét.

10.3. Az informatikai vezető jogai

- az előírások ellen vétőkkel szemben felelősségre vonási eljárást kezdeményezhet az intézmény vezetőjénél,
- bármely érintett szervezeti egységnél jogosult ellenőrzésre,
- betekinthez valamennyi iratba, ami az informatikai feldolgozásokkal kapcsolatos,
- javaslatot tesz az új védelmi, biztonsági eszközök és technológiák beszerzésére illetve bevezetésére,
- adatvédelmi szempontból az informatikai beruházásokat véleményezi.

11. Az Informatikai Biztonsági Szabályzat alkalmazásának módja

Az IBSZ megismerését az érintett dolgozók részére a vezetők és a rendszergazdák oktatás formájában biztosítják. Erről nyilvántartást kötelesek vezetni.

Az Informatikai Biztonsági Szabályzatban érintett munkakörökben az egyes munkaköri leírásokat ki kell egészíteni az IBSZ előírásainak megfelelően.

12.1. Az Informatikai Biztonsági Szabályzat karbantartása

Az IBSZ-t az informatikában - valamint az intézménynél - a fejlődés során bekövetkező változások miatt időközönként aktualizálni kell. Az IBSZ folyamatos karbantartása az informatikai vezető feladata.

13.2. A védelmet igénylő adatok és információk osztályozása, minősítése, hozzáférési jogosultság

Az adatokat és információkat jelentőségük és bizalmassági fokozatuk szerint osztályozzuk: közlésre szánt, bárki által megismerhető adatok, minősített, titkos adatok.

Az informatikai feldolgozás során keletkező adatok minősítője annak a szervezeti egységnek a vezetője, amelynek védelme az érdekkörébe tartozik.

Az adatok feldolgozásakor meg kell határozni írásban és névre szólóan a hozzáférési jogosultságot. A kijelölt dolgozók előtt az adatvédelmi és egyéb szabályokat, a betekintési jogosultság terjedelmét, gyakorlati módját és időtartamát ismertetni kell.

Alapelve, hogy mindenki csak ahhoz az adathoz juthasson el, amire a munkájához szüksége van.

Az információhoz való hozzáférést lehetőség szerint a tevékenység naplózásával dokumentálni kell, ezáltal bármely számítógépen végzett tevékenység – adatbázisokhoz való

hozzáférés, a fájlba vagy mágneslemezre történő mentés, a rendszer védett részeibe történő illetéktelen behatolási kísérlet – utólag visszakereshető.

A naplófájlokat rendszeresen át kell tekinteni, s a jogosulatlan hozzáférést vagy annak a kísérletét az intézmény vezetőjének jelenteni kell.

A naplófájlok áttekintéséért, értékeléséért az informatikai vezető és a rendszergazdák a felelősek.

Az adatok védelmét, a feldolgozás – az adattovábbítás, a tárolás - során az operációs rendszerben és a felhasználói programban alkalmazott logikai matematikai, illetve a hardver berendezésekben kiépített technikai megoldásokkal is biztosítani kell (szoftver, hardver adatvédelem).

14. Az informatikai eszközbázist veszélyeztető helyzetek

Az információk előállítására, feldolgozására, tárolására, továbbítására, megjelenítésére alkalmas informatikai eszközök fizikai károsodását okozó veszélyforrások ismerete azért fontos, hogy felkészülten megelőző intézkedésekkel a veszélyhelyzetek elháríthatók legyenek.

14.1. Környezeti infrastruktúra okozta ártalmak

- elemi csapás:
- földrengés,
- árvíz,
- tűz,
- villámcsapás, stb.
- környezeti kár:
- légszennyezettség,
- nagy teljesítményű elektromágneses térerő,
- elektrosztatikus feltöltődés,
- a levegő nedvességtartalmának felszökése vagy leesése,
- piszkolódás (pl. por).
- közüzemi szolgáltatásba bekövetkező zavarok:
- feszültség-kimaradás,
- feszültség-ingadozás,
- elektromos zárlat,
- csőtörés.

14.2. Emberi tényezőre visszavezethető veszélyek

Szándékos károkozás:

- behatolás az informatikai rendszerek környezetébe,
- illetéktelen hozzáférés (adat, eszköz),
- adatok- eszközök eltulajdonítása,
- rongálás (gép, adathordozó),
- megtévesztő adatok bevitele és képzése,
- zavarás (feldolgozások, munkafolyamatok).

Nem szándékos, illetve gondatlan károkozás:

- figyelmetlenség (ellenőrzés hiánya),
- szakmai hozzá nem értés,
- a gépi és eljárásbeli biztosítékok beépítésének elhanyagolása,
- a megváltozott körülmények figyelmen kívül hagyása,
- vírusfertőzött adathordozó behozatala,
- biztonsági követelmények és gyári előírások be nem tartása,
- adathordozók megrongálása (rossz tárolás, kezelés),
- a karbantartási műveletek elmulasztása.

A szükséges biztonsági-, jelző és riasztó berendezések karbantartásának elhanyagolása veszélyezteti a feldolgozás folyamatát, alkalmat ad az adathoz való véletlen vagy szándékos illetéktelen hozzáféréshez, rongáláshoz.

15. Az adatok tartalmát és a feldolgozás folyamatát érintő veszélyek

15.1. Tervezés és előkészítés során előforduló veszélyforrások

- a rendszerterv nem veszi figyelembe az alkalmazott hardver eszköz lehetőségeit,
- hibás adatrögzítés, adatelőkészítés, az ellenőrzési szempontok hiányos betartása.

15.2. A rendszerek megvalósítása során előforduló veszélyforrások

- hibás adatállomány működése,
- helytelen adatkezelés,
- programtesztelés elhagyása.

15.3. A működés és fejlesztés során előforduló veszélyforrások

- emberi gondatlanság,
- szervezetlenség,
- képzetlenség,
- szándékosan elkövetett illetéktelen beavatkozás,
- illetéktelen hozzáférés,
- üzemeltetési dokumentáció hiánya.

16. Az informatikai eszközök környezetének védelme

16.1. Vagyonvédelmi előírások

- a gépteremek külső és belső helyiségeit biztonsági zárral kell felszerelni,
- a gépterembe való be- és kilépés rendjét szabályozni kell,
- a gépterembe, szerverterembe történő illetéktelen behatolás tényét az intézmény vezetőjének
- azonnal jelenteni kell,
- az informatikai eszközöket csak az intézmény arra felhatalmazott alkalmazottai használhatják,

- az informatikai eszközök rendeltetésszerű használatáért a felhasználó felelős.

16.2. Adathordozók

- könnyen tisztítható, jól zárható szekrényben kell elhelyezni úgy, hogy tárolás közben ne sérüljenek, károsodjanak,
- az adathordozókat a gyors hozzáférés érdekében azonosítóval kell ellátni, melyről nyilvántartást kell vezetni,
- a használni kívánt adathordozót (floppy, CD) a tárolásra kijelölt helyről kell kivenni, és oda
- kell vissza is helyezni,
- a munkaasztalon csak azok az adathordozók legyenek, amelyek az aktuális feldolgozáshoz
- szükségesek,
- adathordozót másnak átadni csak engedéllyel szabad,
- a munkák befejeztével a használt berendezést és környezetét rendbe kell tenni.

16.3. Tűzvédelem

A gépterem illetve kiszolgáló helyiség a „D” tűzveszélyességi osztályba tartozik, amely mérsékelt tűzveszélyes üzemet jelent.

A menekülési útvonalak szabadon hagyását minden körülmények között biztosítani kell.

Az intézmény géptermeibe, szerverszobáiba minimum 1-1 db tűzoltó készüléket kell elhelyezni.

Az intézmény géptermeiben, szerverszobáiban elektromos vagy más munkát csak a tűzvédelmi vezető tudtával, ill. engedélyével szabad végezni.

A nagy fontosságú, pl. törzsadat-állományokat 2 példányban kell őrizni és a második példányt elkülönítve tűzbiztos páncélszekrényben kell őrizni. (Ezen adatállományok kijelölése az informatikai vezető feladata.)

17. Az informatikai rendszer alkalmazásánál felhasználható védelmi eszközök és módszerek

17.1. A számítógépek és szerverek védelme

- Elemi csapás (vagy más ok) esetén a számítógépekben vagy szerverekben bekövetkezett részleges vagy teljes károsodáskor az alábbiakat kell sürgősen elvégezni:
- menteni a még használható anyagot,
- biztonsági mentésekről, háttértákról a megsérült adatok visszaállítása,
- archivált anyagok (ill. eszközök) használatával folytatni kell a feldolgozást.

17.2. Hardver védelem

- A berendezések hibátlan és üzemszerű működését biztosítani kell.
- A működési biztonság megóvását jelenti a szükséges alkatrészek beszerzése.
- Az üzemeltetést, karbantartást és szervizelést az informatikusok végzik.
- A munkák szervezésénél figyelembe kell venni:

- a gyártó előírásait, ajánlatait,
- a tapasztalatokat.
- Alapgép megbontását (kivéve a garanciális gépeket) csak informatikus végezheti el.

17.3. Az informatikai feldolgozás folyamatának védelme

17.3.1. Az adatrögzítés védelme

adatbevitel hibátlan műszaki állapotú berendezésen történjen, tesztelt adathordozóra lehet adatállományt rögzíteni, a bizonylatokat és mágneses adathordozókat csak e célra kialakított és megfelelő tároló helyeken szabad tartani, az adatrögzítő szoftver védelme. Lehetőség szerint olyan szoftvereket kell alkalmazni, amelyek rendelkeznek ellenőrző funkciókkal és biztosítják a rögzített tételek visszakeresésének és javításának lehetőségét is.
hozzáférési lehetőség:

- a bejelentkezési azonosítók használatával kell szabályozni, hogy ki milyen szinten férhet hozzá a kezelt adatokhoz. (alapelv: a tárolt adatokhoz csak az illetékes személyek férjenek hozzá).
- az adatok bevitele során alapelv: azonos állomány rögzítését és ellenőrzését ugyanaz a személy nem végezheti.
- A szerverek rendszergazda jelszavát az informatikai vezető kezeli.
Az adatrögzítés folyamatához kapcsolódó dokumentációk:
 - adatrögzítési utasítások,
 - ellenőrző rögzítési utasítások,
 - tesztelő és törlő programok kezelési utasításai,
 - megőrzési utasítások,
 - gépkezelési leírások.

17.3.2. Az adathordozók nyilvántartása

Az adathordozókról az egységeknek nyilvántartást kell vezetni. Az adathordozókat a gyors és egyszerű elérés, a nyilvántartás és a biztonság érdekében azonosítóval (sorszámmal) kell ellátni.

17.3.3. Adathordozók tárolása

Az adathordozók tárolására műszaki-, tűz- és vagyonvédelmi előírásoknak megfelelő helyiséget kell kijelölni, illetve kialakítani.

17.3.5. Az adathordozók megőrzése

Az adathordozók megőrzési idejét a törvényekben meghatározott bizonylat őrzési kötelezettségnek megfelelően kell kialakítani

17.3.6. Selejtezés, sokszorosítás, másolás

A selejtezést az intézmény selejtezésének szabályzata alapján kell lefolytatni. Sokszorosítást, másolást csak az érvényben lévő belső utasítások szerint szabad végezni. Biztonsági illetve archív adatállomány előállítását másolásnak számít.

17.3.8. Leltározás

A szoftvereket és adathordozókat a Leltározási Szabályzatban foglaltaknak megfelelően kell leltározni.

17.3.9. Mentések, file-ok védelme

Az adatfeldolgozás után biztosítani kell az adatok mentését. A munkák során létrehozott általános (pl. Word és Excel) dokumentumok mentése az azt létrehozó munkatársak (felhasználók) feladata. A felhasználó számítógépén lévő adatokról biztonsági mentéseket a felhasználónak kell készítenie. Az archiválásban az informatikusok segítséget nyújtanak. A szervereken tárolt adatokról a mentést rendszeresen el kell végezni. A mentésért az informatikai vezető illetve a rendszergazdák a felelősek.

17.4. Szoftver védelem

17.4.1. Rendszerszoftver védelem

Az informatikai vezetőnek biztosítani kell, hogy a rendszerszoftver naprakész állapotban legyen és a segédprogramok, programkönyvtárak mindig hozzáférhetők legyenek a felhasználók számára.

17.4.2. Felhasználói programok védelme

Programhoz való hozzáférés, programvédelem

A kezelés folyamán az illetéktelen hozzáférést meg kell akadályozni, az illetéktelen próbálkozást ki kell zárni.

Gondoskodni kell arról, hogy a tárolt programok, fájlok ne károsodjanak, a követelményeknek megfelelően működjenek.

Programok megőrzése, nyilvántartása

A programokról a leltárfelelősöknek naprakész nyilvántartást kell vezetni

A számvitelről szóló többször módosított 2000. évi C. törvény értelmében az intézményeknek az üzleti évről készített beszámolót, valamint az azt alátámasztó leltárt, értékelést, főkönyvi kivonatot, továbbá más, a számviteli törvény követelményeinek megfelelő nyilvántartást olvasható formában legalább 10 évig meg kell őrizni.

A bizonylat elektronikus formában is megőrizhető, ha az alkalmazott módszer biztosítja az eredeti bizonylat összes adatának kétsédelem nélküli előállítását, folyamatos leolvashatóságát, illetve kizárja az utólagos módosítás lehetőségét.

A programok nyilvántartásáért és működőképes állapotban való tartásáért a vezetők a felelősek.

18. A központi számítógép és a hálózat munkaállomásainak működésbiztonsága

18.1. Központi gépek

Szünetmentes áramforrást célszerű használni, amely megvédi a berendezést a feszültségingadozásoktól, áramkimaradás esetén adatvesztéstől.

A központi gépek háttértáiról folyamatosan biztonsági mentést kell készíteni.

Az alkalmazott hálózati operációs rendszer adatbiztonsági lehetőségeit az egyes konkrét feladatokhoz igazítva kell alkalmazni.

A vásárolt szoftverekről biztonsági másolatot kell készíteni.

18.2. Munkaállomások

Külső helyről hozott, vagy kapott anyagokat ellenőrizni kell vírusellenőrző programmal.

Vírusfertőzés gyanúja esetén az informatikusokat azonnal értesíteni kell.

Új rendszereket használatba vételük előtt szükség szerint adaptálni kell, és tesztadatokkal ellenőrizni kell működésüket.

Az intézmény informatikai eszközeiről programot illetve adatállományokat másolni a jogos belső felhasználói igények kielégítésein kívül nem szabad.

A hálózati vezeték és egyéb csatoló elemei rendkívül érzékenyek, mindennemű sérüléstől ezen elemeket meg kell óvni. A hálózat vezetékének megbontása szigorúan tilos.

Az informatikai eszközt és tartozékait helyéről elvinni csak az eszköz leltárfelelőse tudtával és engedélyével szabad.

19. Ellenőrzés

Az ellenőrzésnek elő kell segíteni, hogy az informatikai rendszereknél előforduló veszélyhelyzetek ne alakuljanak ki. A kialakult veszélyhelyzet esetén cél a károk csökkentése illetve annak megakadályozása, hogy az megismétlődjön.

A munkafolyamatba épített ellenőrzés során az IBSZ rendelkezéseinek betartását az adatkezelést végző szervezeti egység vezetői folyamatosan ellenőrzik.




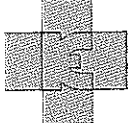
20. GDPR alapelveinek megfelelő felhasználói biztonsági szempontok érvényesítése

A felhasználók figyelmének felhívása értekezletek alkalmával, valamint az alábbiak szűrőpróba szerű ellenőrzése:

- minden egyes felhasználó a munkaállomáson, programban a saját nevével van bejelentkezve
- felhasználó elhagyja a munkaállomást, kötelező a kijelentkezés, időkorlátos automatikus kiléptetés
- automatikus jelszó megjegyzés tilalma
- felhasználók tájékoztatása a személyes adatok kezelésének felelősségére

22. Adatvédelmi incidens kezelése

Az intézmény biztosítja az adatkezeléshez kapcsolódó kockázat mértékének megfelelő adatbiztonságot, melynek sérülése esetén késedelem nélkül, de legkésőbb a tudomásra jutástól számított 72 órán belül adatvédelmi tisztviselőnk, vagy ennek hiányában az

			KOMLÓI EGÉSZSÉGCENTRUM, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ H-7300 KOMLÓ, MAJÁLIS TÉR 1. TEL.: (36 72) 582 340 FAX: (36 72) 482 045	
---	---	---	---	---

adatkezelő/adatfeldolgozó vagy képviselője bejelentést tesz a felügyeleti hatóságnak és tájékoztatja az érintettet is.

Intézményünk az adatvédelmi incidens tudomására jutását követően haladéktalanul megteszi a szükséges biztonsági intézkedéseket az adatvédelmi incidens alapját adó sérülés megszüntetése, helyreállítása céljából.

Az érintettet értesítjük a megtett intézkedésekről és azok eredményéről.

23. Jogorvoslati tájékoztatás:

Magyarországon az adatvédelmi felügyeleti hatóság: Nemzeti Adatvédelmi és Információszabadság Hatóság (továbbiakban: NAIH, címe: 1125 Budapest, Szilágyi Erzsébet fasor 22/C, e-mail címe: ugyfelszolgalat@naih.hu). Az érintett panaszt nyújthat be a NAIH-hoz amennyiben álláspontja szerint a rá vonatkozó személyes adat kezelés nem felel meg a jogszabályi kötelezettségeknek.

A NAIH döntése ellen bírósági felülvizsgálat kezdeményezhető.

ZÁRÓ RENDELKEZÉSEK

Ez a szabályzat *2018. május 25-én* lép hatályba.

ADATKEZELÉSI TÁJÉKOZTATÓ

Az adatkezelő és képviselőjének megnevezése és elérhetőségei:

Adatkezelő neve: Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ

Elérhetőségei:

Székhely: 7300 Komló, Majális tér 1.

Telefon: 06 – 72 / 582 340

FAX: 06 – 72 / 482 045

Email: titkarsag@komloikorhaz.hu

Képviselő neve: Dr. Tánczos Frigyes Attila főigazgató

Személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja:

- 1997. évi XLVII. törvény alapján az alaptevékenység: betegellátás nyújtásához kapcsolódóan a betegek adatait kezeljük;
- munkavállalók adatainak kezelése;
- szerződéses partnerek kapcsolattartói adatainak kezelése a szerződés teljesítése céljából;
- vagyonvédelem, személyi biztonság;
- törvényben meghatározott kötelezettség teljesítése céljából.

Személyes adatok tárolásának időtartama:

- A számlákat jogi kötelezettség miatt legalább 8 évig megőrizzük. A számlakiállítás alapjául szolgáló iratok megőrzési ideje 8 év.
- A munkaviszony, közalkalmazotti jogviszony, közreműködői jogviszony alapjául szolgáló iratok megőrzési ideje: 50 év.
- Szerződés teljesítéséhez kapcsolódó adatok megőrzése: 5 év.
- Pályázati projektek elszámolásához kapcsolódó adatok megőrzése a támogatási szerződésben meghatározott időtartam.
- Zárójelentés megőrzési ideje 50 év
- Egészségügyi dokumentáció megőrzési ideje 30 év
- Képközlő diagnosztikai eljárással készített felvétel megőrzési ideje 10 év, a felvételtől készített lelet megőrzési ideje 30 év

Tájékoztatjuk, hogy az érintettnek joga van az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az ilyen személyes adatok kezelése ellen történő kérelmezéséhez, valamint az érintett adathordozhatóságához való jogáról; valamint az adatkezelési hozzájárulás bármely időpontban való visszavonásához.

A felügyeleti hatósághoz címzett panasz benyújtható:

Nemzeti Adatvédelmi és Információszabadság Hatóság

Cím: 1125 Budapest, Szilágyi Erzsébet fasor 22/C

Email: ugyfelszolgalat@naih.hu

NYILATKOZAT a személyes adatok kezeléséről

Alulírott

Név:

Lakcím:

Telefonszám:

E-mail cím:

hozzájárok Komlói Egészségcentrum, Bányászati Utókezelő és Éjjeli Szanatórium Egészségügyi Központ részére fenti személyes adataim kezeléséhez, az alábbi feltételekkel:

Az adatkezelésére a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) irányadó. Az adatszolgáltatás önkéntes. A betegellátás során adatkezelés a 1997. évi XLVII. törvény alapján történik.

További személyes adatok kezelése törvényi felhatalmazáson alapulhat, amelynek célja jogszabályi kötelezettségek teljesítése.

Hozzájárulok, hogy az Adatkezelő részemre levelet küldjön. Ezen hozzájáruló nyilatkozat nem vonatkozik a kezelt adatok harmadik személy részére történő átadására, ez a törvényben írt kivételekkel kizárólag az előzetes hozzájárulásommal történhet. Jelen hozzájáruló nyilatkozat bármikor korlátozás, feltétel és indokolás nélkül visszavonható. Kijelentem, hogy ezen hozzájárulásomat önkéntesen, minden külső befolyás nélkül, a megfelelő tájékoztatás és a vonatkozó jogszabályi rendelkezések ismeretében tettem meg.

Kelt,,év hónap nap

.....
Nyilatkozattevő aláírása

Előttünk mint tanúk előtt:

Név:..... Név:.....

Lakcím:..... Lakcím:.....

Aláírás:..... Aláírás:.....

KAMERÁVAL MEGFIGYELT TERÜLET!

Tájékoztató adatkezelésről

Tájékoztatjuk Tisztelt Betegeinket, Látogatóinkat, hogy
a Komlói Egészségcentrum,
Bányászati Utókezelő és Éjjeli Szanatórium
Egészségügyi Központ (7300 Komló, Majális tér 1.) területén,
az épületen belüli, illetve az épületen kívüli
mozgást elektronikus megfigyelő rendszerrel
(továbbiakban: kamerákkal) figyeljük,
mely során személyes adatokat tartalmazó képfelvételek készülnek.

Az adatkezeléshez történő hozzájárulás önkéntes, ráutaló magatartással történik. Ön az intézmény területére történő belépéssel és az itt tartózkodással hozzájárulását adja a képfelvétellel kapcsolatos adatkezeléshez. A megfigyelésnek és a képfelvételek rögzítésének célja az intézmény területén tartózkodó személyek életének, testi épségének, továbbá az intézmény vagyontárgyainak védelme. Ennek keretében cél a jogsértő cselekmények megelőzése, a jogsértések észlelése, az elkövető tettenérése, illetve a felvételek bizonyítékként történő felhasználásra a hatósági eljárások keretében. A képfelvételeket a kamerák központi felvevő egységén 3 munkanapig tároljuk. A kamerarendszert az intézmény működteti. A kamerák pontos elhelyezéséről, és az általuk megfigyelt területről az informatikai biztonsági szabályzatból informálódhat. Bármely meghatározott, személyes adat alapján azonosított vagy – közvetlenül vagy közvetve – azonosítható természetes személy kérelmezheti a tájékoztatását személyes adatainak kezeléséről, személyes adatainak helyesbítését, valamint a személyes adatainak – a kötelező adatkezelés kivételével – törlését vagy zárolását.