10. Péter Orsolya Márta

Az orvosi titoktartás, az egészségügyi adatok és a digitalizált világ

Amit kezelés közben látok vagy hallok – akár kezelésen kívül is a társadalmi érintkezésben –, nem fogom kifecsegni, hanem titokként megőrzöm.

- Részlet az eredeti hippokratészi eskü szövegéből

„Adatok a szemétdombról”

2021 februárjában két, adatvédelemben jártas számítógépes szakember tárta a nyilvánosság elé a következő esetet [1]*. Egyikük egy szemeteskonténerben talált rá egy kidobott számítógépre, amit egy sörért megvásárolt a konténerre vigyázó férfitől. Ezt követően kollégájával együtt – laikusok által is hozzáférhető és könnyen használható program segítségével – vizsgálatnak vetették alá a merevlemezt. Ennek során kiderült, hogy a gépet korábban egy magyar nagyváros orvosi rendelőjében használhatták, mivel a gépen hatalmas mennyiségű titkosítatlan egészségügyi adatot találtak – többek között háromezernél is több páciens TAJ-számát, születési adatait, lakcímét, e-mail címét, a nekik felírt gyógyszerekre vonatkozó információkat, vizsgálati eredményeket, de képalkotó diagnosztikai eszközökkel készített felvételeket is. A szakemberek ezt követően fizikailag megsemmisítették a merevlemezt. Figyelmeztetésük szerint az adatvédelemmel kapcsolatos jogszabályok egyértelmű megsértése történt, ami azért is igen veszélyes, mert az ilyen információk birtokában nem csak kéretlen reklámlevelekkel lehet elárasztani az érintetteket, hanem akár zsarolni is. Emiatt nem véletlen az, hogy az online feketepiacokon komoly értékkel bírnak az egészségügyi adatok.*

Bevezető

Az orvos titoktartási kötelezettsége igen mélyen gyökerezik az úgynevezett „nyugati" gyógyítási kultúrában. Az i.e. 4. század körül keletkezett hippokratészi eskü szövegében már szerepel az, hogy az orvos titokként köteles megőrizni mindazt, amit betegéről megtudott, s e kötelezettségvállalás a mai napig – Magyarországon, de más országokban is – az orvosi fogadalom szerves részét képezi.

E szabály létét az ókortól kezdődően az a jól ismert körülmény indokolja, hogy az orvos-beteg kapcsolat lényegi eleme a bizalom. A gyógyulásban reménykedő páciens sokszor életének olyan részleteit osztja meg orvosával, amiket esetleg még legközelebbi hozzátartozói, családtagjai, régi barátai előtt is titkol. Az orvosukban bízó betegek szívesebben működnek együtt az egészségügyi dolgozókkal, kezelésük emiatt – kételkedő és bizalmatlan betegtársaikéhoz képest – gyakorta sikeresebb, továbbá a kapott ellátás minőségét is magasabbra értékelik, elégedettebbek orvosukkal és általában az egészségügyi ellátórendszerrel is [2].

A 21. században a titoktartás már régóta nem csak etikai elvárás, hanem azt a vonatkozó jogszabályok is kötelezettségként írják elő. Ezen túl tisztában kell lennünk azzal is, hogy az „orvosi" titoktartásra jogilag kötelezett személyek köre tágabb annál, mint amit az eredeti kifejezés sugall. A modern betegellátás csapatmunkát igényel, e folyamat résztvevői pedig természetszerűleg nem csak orvos végzettségűek lehetnek.

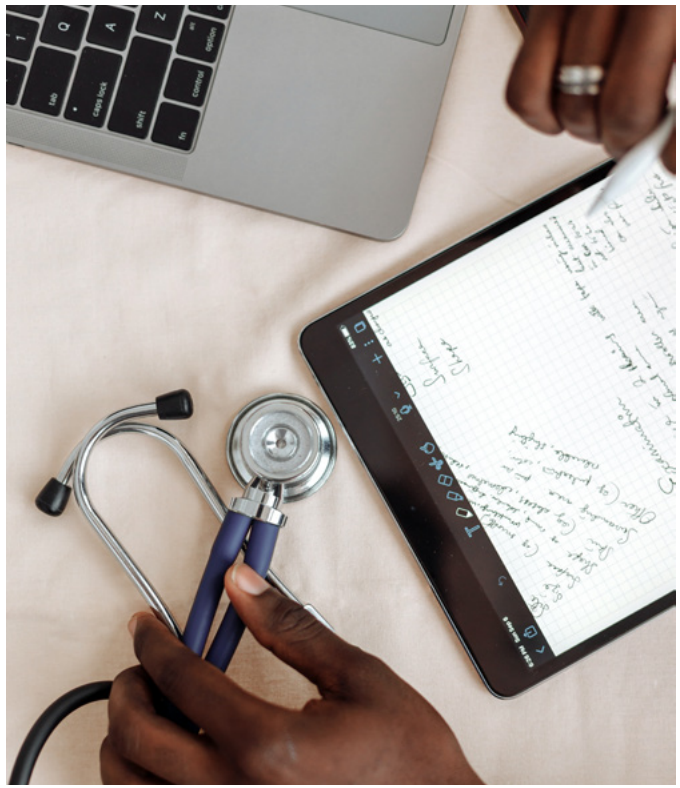
Magyarországon az egészségügyi törvény (az 1997. évi CLIV. törvény, röviden Eütv.) a betegek egyik jogaként rögzíti a következőket: *„A beteg jogosult arra, hogy az egészségügyi ellátásában részt vevő személyek az ellátása során tudomásukra jutott információkat, különösképpen a beteg egészségügyi és személyes adatait csak az arra jogosulttal közöljék, és azokat a vonatkozó jogszabályok szerint kezeljék."*

Egy további, részletesebben megszövegezett paragrafusban a jogalkotó a fentieket az egészségügyi dolgozók kötelességeként is megfogalmazza: *„Az egészségügyi dolgozót, valamint az egészségügyi szolgáltatóval munkavégzésre irányuló jogviszonyban álló más személyt minden, a beteg egészségi állapotával kapcsolatos, valamint az egészségügyi szolgáltatás nyújtása során tudomására jutott adat és egyéb tény vonatkozásában, időbeli korlátozás nélkül titoktartási kötelezettség terhel, függetlenül attól, hogy az adatokat közvetlenül a betegtől, vizsgálata vagy gyógykezelése során, illetve közvetetten az egészségügyi dokumentációból vagy bármely más módon ismerte meg."* [3]

A fenti, első olvasatra ugyancsak összetettnek és bonyolultnak tűnő rendelkezések legfontosabb üzenetei a következők.

- A beteg egészségügyi ellátásában részt vevő személyeket (tekintet nélkül arra, hogy orvosi szakképesítéssel rendelkeznek-e), továbbá az adott egészségügyi szolgáltatónál dolgozó más munkavállalókat titoktartás terheli.

- E titoktartás tárgya mindazon információ, amit a fenti személyek a beteggel kapcsolatban megtudnak – és ami nem kizárólag csak a beteg egészségi állapotára vonatkozhat. Ezeket az információkat sem szóban, sem írásban, sem pedig más módon (pl. fényképfelvétel formájában) nem oszthatják meg olyasvalakivel, aki erre nem jogosult.
- E kötelezettség attól függetlenül áll fenn, hogy a fenti személyek milyen jogszerű módon jutottak az információhoz: maga a beteg vagy a beteg hozzátartozója, családtagja közölte-e a kérdéses adatot (pl. hogy a páciens dohányzik), azt az orvos vagy más egészségügyi dolgozó a beteg vizsgálata vagy ellátása során észlelte (pl. hogy a beteg panaszait epekő okozza), vagy az információt az illető a beteg egészségügyi dokumentációjában látta-olvasta.
- A titoktartás parancsa egyben adatvédelmi kötelezettséget is ró az egészségügyi dolgozókra, valamint rajtuk kívül mindenkire – tehát az egészségügyi képzettséggel nem rendelkező munkatársakra, pl. irodai dolgozókra is –, aki egy beteg személyével és egészségi állapotával kapcsolatos adathoz jogszerűen hozzáférhet, azt megismerheti.
- Az adatvédelmi kötelezettség a valamilyen formában rögzített információkra, adatokra (az úgynevezett egészségügyi dokumentációra) vonatkozik.
- Fontos továbbá az is, hogy a fenti rendelkezések egyformán vonatkoznak az állami és magánegészségügyre – ennek megfelelően pl. az egyéni vállalkozóként működő orvost, illetve a magánrendelő kartonozójában dolgozó adminisztrátort ugyanúgy kötik a fenti szabályok, mint az állami ellátórendszerben foglalkoztatott társaikat.



Személyes adatok és egészségügyi adatok

A titoktartásra vonatkozó fenti rendelkezések ugyanakkor további kérdéseket vetnek fel. Pontosan mit jelent a „személyes adat" és az „egészségügyi adat"? Az szinte mindenki számára egyértelmű, hogy orvosként baráti társaságban nem szabad úgy anekdotáznunk, hogy a problémás vagy érdekes esetet jelentő betegeinket nevükön nevezzük, esetleg még foglalkozásukat, családi körülményeiket is megemlítjük. Szintén jogszerűtlen az, ha a kórházi nővérpultnál az ápolók számos páciens füle hallatára vitatják meg, hogy a hármas kórteremben fekvő, epehólyag-műtéten átesett Kovács bácsi állapota a reméltnél lassabban javul. Viszont felmerül, hogy egészségügyi adatnak tekinthető-e például az a tény, hogy valaki olyan helyen él, ahol a vezetékes víz minősége kifejezetten rossz?

E kérdések megválaszolásához három további jogszabályt kell segítségül hívnunk.

- 2018. május 25-től kezdődően az Európai Unió összes tagállamában, így Magyarországon is közvetlenül alkalmazni kell az EU általános adatvédelmi rendeletét, a *General Data Protection Regulation*-t, közismert rövidítéssel a GDPR-t [4]. A GDPR a jogszabályi hierarchia tetején található, ami azt jelenti, hogy az egyes EU-tagállamok nemzeti jogszabályai nem állhatnak ellentétben a GDPR-ban rögzített szabályokkal. Fontos tudnunk továbbá, hogy a GDPR első mondata sarkalatos értékként határozza meg a következőket: *„A természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog"*. A fentieken túl a GDPR különleges kategóriába tartozó, magasabb szintű védelmet igénylő adatként nevesíti az egészségügyi adatokat.

TUDTA?

A GDPR fő szabályként megtiltja a különleges adatok, ezen belül az egészségügyi adatok kezelését, és e szabály alól csak néhány kivételt enged. Ilyen kivételt jelent, ha az egészségügyi adatok kezeléséhez az érintett kifejezett hozzájárulását adta, vagy az adatkezelés a GDPR-ban megjelölt különleges célok érdekében történik. Többek között ilyen cél az orvosi diagnózis felállítása, továbbá egészségügyi ellátás vagy kezelés nyújtása. Egészségügyi adatokat akkor is lehet kezelni, ha kezelésük a népegészségügy területét érintő, olyan közérdekből szükséges, mint például a határokon át terjedő járványok megelőzése, terjedésük megfékezése.

- Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [5] („Infotv.") általában rendelkezik a személyes adatok védelméről. Fontos, hogy e törvény – a GDPR-ral összhangban – különleges adatnak minősíti az egészségügyi adatokat, amelyek kezelése során viszont csak akkor kell az Infotv. rendelkezéseit alkalmazni, ha az erre vonatkozó speciális jogszabály nem tartalmaz eltérő rendelkezéseket, vagy egyáltalán nem rendelkezik egy adott kérdésről.
- Mint címe is mutatja, az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről szóló 1997. évi XLVII. törvény [6] (rövidítve „Eüak.") jelenti azt a speciális jogszabályt, amelynek rendelkezéseit tiszteletben tartva kell az egészségügyi adatokat kezelni.
- Ezen túl a fentiekben már említett Eütv. is tartalmaz néhány, adatvédelemmel kapcsolatos rendelkezést.

Miként határozzák meg tehát a fenti jogszabályok a „*személyes adat*" és az „*egészségügyi adat*" fogalmát?

Ami a „*személyes adat*"-ot illeti, az Infotv. meglehetősen szűkszavúan annyit mond, hogy személyes adatnak minősül az érintettre (azaz a bármely információ alapján azonosított vagy azonosítható természetes személyre) vonatkozó bármely információ. A GDPR több magyarázattal szolgál, amikor a fenti meghatározáshoz hozzáteszi: „*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.*" Fontos látnunk, hogy a GDPR a példák között kifejezetten említi az olyan adatokat, amelyek a modern technológiák használata révén keletkeznek – ilyen pl. az IP-cím, a mobiltelefon által gyűjtött helymeghatározó adatok, vagy éppen a vezetéknév.utónév@munkahely.com típusú e-mail címek.

A fentiekhez képest az „*egészségügyi adat*" szűkebb és különlegesebb kategória, amelynek meghatározását – a GDPR-ral összhangban – az Infotv. szolgáltatja számunkra: az 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.*"

Ez a meghatározás is igencsak tágnak és általánosnak tűnik. Szerencsére a GDPR segítségünkre siet az értelmezésben. Eszerint az egészségügyi személyes adatok közé tartoznak az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról. Ide tartoznak az olyan személyes adatok, amelyeket az egészségügyi szolgáltatások céljából történő nyilvántartásba vétel, vagy ilyen szolgáltatások nyújtása során gyűjtöttek az érintettről. Ilyen továbbá az egészségügyi célokból történő egyéni azonosítás érdekében az érintetthez rendelt szám, jel vagy adat, valamely test-

rész vagy a testet alkotó anyag – beleértve a genetikai adatokat és a biológiai mintákat is – teszteléséből vagy vizsgálatából származó információk, és bármilyen további, például az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától, amely lehet például orvos vagy egyéb egészségügyi dolgozó, kórház, orvostechnikai eszköz vagy *in vitro* diagnosztikai teszt.

Az egészségügyi adatok védelme és az adatvédelmi incidens

Az orvosi titoktartás és az egészségügyi adatok védelme szorosan összefüggő kötelezettségeket jelentenek. Mindezt hangsúlyozza az Eüak. is, amikor leszögezi: orvosi titoknak minősül *„a gyógykezelés során az adatkezelő tudomására jutott egészségügyi és személyazonosító adat, továbbá a szükséges vagy folyamatban lévő, illetve befejezett gyógykezelésre vonatkozó, valamint a gyógykezeléssel kapcsolatban megismert egyéb adat.*" Egészségügyi adatot kezelni tehát csak titoktartási kötelezettség mellett lehet.

TUDTA?

Ha az adatkezelőt hivatásából kifolyólag orvosi titoktartási kötelezettség terheli, e titoktartási kötelezettség vonatkozik az általa kezelt személyes és egészségügyi adatokra is. Ha az adatkezelőt nem terheli a hivatásbeli titoktartás, vele az orvosi titoktartási kötelezettséggel azonos terjedelmű titoktartási nyilatkozatot kell aláíratni.

Míg azonban a régmúlt korok orvosai sokszor emlékezetükben tárolták a betegeikre vonatkozó tudást, vagy esetleg saját maguk által választott módon és stílusban vezettek írásos feljegyzéseket a pácienseikről – Sigmund Freud például noteszkönyvbe jegyzetelt –, korunkban a betegek személyes és egészségügyi adatait szervezett és rendszerezett módon, rögzített formában tároljuk. Mindez nem is történhetne másképp: az egészségügyi ellátórendszer a korábbiakhoz képest mindennél nagyobb számban látja el az orvosi segítségre szorulókat, akikről mára szinte felfoghatatlan mennyiségű adat keletkezik (minderről lásdd „Az adatok szerepe a digitális egészségügyben"

című fejezetet). Ezen adattömegek tárolását egyre inkább a számítástechnika eszközeivel oldjuk meg, az adattárolás az egészségügyben is hatalmas léptekkel halad a teljes digitalizáció irányába.

A betegek adatait az úgynevezett egészségügyi dokumentáció tartalmazza, amelynek fogalmát az Eütv. és az Eüak. – néhány kifejezésbeli eltéréssel – a következő módon határozza meg: *„az egészségügyi szolgáltatás során az egészségügyi dolgozó tudomására jutó, a beteg kezelésével kapcsolatos egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától" (Eütv.);* illetve *„a gyógykezelés során a betegellátó tudomására jutott egészségügyi és személyazonosító adatokat tartalmazó feljegyzés, nyilvántartás vagy bármilyen más módon rögzített adat, függetlenül annak hordozójától vagy formájától"* (Eüak.).

Rendkívül fontos továbbá az, hogy az egészségügyi dokumentációban rögzített adatokat – mivelhogy azok egyben orvosi titkot is képeznek – megfelelő módon védeni kell minden lehetséges titoktöréstől. Az Eüak. a következő módon fogalmazza meg az adatvédelmi kötelezettséget: *„Az egészségügyi és személyazonosító adatok kezelése és feldolgozása során biztosítani kell az adatok biztonságát véletlen vagy szándékos megsemmisítéssel, megsemmisüléssel, megváltoztatással, károsodással, nyilvánosságra kerüléssel szemben, továbbá, hogy azokhoz illetéktelen személy ne férjen hozzá"*.

Az internet és az elektronikus adathordozók széles körű elterjedését megelőzően viszonylag egyszerűbb volt a titoktartással és adatvédelemmel kapcsolatos fenti parancsokat a gyakorlat szempontjából értelmezni, valamint azokat a mindennapokban alkalmazni. Jogszerű-e, ha egy háziorvosi rendelőben a betegkartonokat nem zárt szekrényben tárolják, így azokba akár a takarítószemélyzet is különösebb erőfeszítés nélkül beleolvashat? Jogszerű-e, ha a kötelező megőrzési idő lejártával ezeket a kartonokat egyszerűen kidobjuk a kukába? Jogszerű-e, ha az orvos íróasztalán úgy hever számos beteg lelete, hogy azokba az íróasztal másik oldalán éppen üldögélő páciens minden további nélkül belelát? A fenti rendelkezések szellemében a válasz egyértelműen „nem".

Viszont hogyan kell értékelnünk azt, ha például egy orvos több betegének titkosítatlan adatait egy pendrive-ra másolja, hogy eseteiket otthon tanulmányozhassa, majd azt útközben elveszíti? Mi a helyzet akkor, amikor egy orvos titkosítás nélkül a Google által biztosított tárhelyre menti a magánrendelőjében kezelt betegek adatait, majd fiókját valaki feltöri, és így hozzájut annak teljes tartalmához? Hogyan viszonyuljunk ahhoz, ha kibertámadás következtében egy kórházban órákra elérhetetlenné válnak a képalkotó berendezések által generált felvételek? Minek minősül az, ha egy beteg laborleleteit tévedésből rossz e-mail címre küldjük? És ha egy orvosi rendelő időpontfoglalást szolgáló weboldala gondatlanságból úgy van beállítva, hogy az időpontfoglaló rendszerbe a betegek által feltöltött leleteket mindenki láthatja és letöltheti?

A GDPR megalkotásának szükségességét az Európai Bizottság többek között pontosan az efféle események elszaporodásával, tehát

az információs technológia gyors fejlődésével, a globalizáció hatásaival, továbbá az elektronikus adatkezelés és -feldolgozás során fellépő új adatvédelmi kihívásokkal indokolta. Ennek megfelelően a GDPR szabályai elsősorban az automatizált (jellemzően számítógép használatával végzett) adatkezelésre fókuszálnak.

TUDTA?

A GDPR nem csak az automatizált módon (legtöbbször számítógéppel) kezelt személyes adatokra, hanem azokra az adatokra is vonatkozik, amelyeket hagyományos módon, „papíralapon" kezelnek – feltéve, hogy ezek az adatok valamely nyilvántartási rendszer részét képezik, vagy azokat egy nyilvántartási rendszer részévé kívánják tenni. Ennek megfelelően a kórházak, rendelőintézetek, más egészségügyi szolgáltatók által rendszerezetten, visszakereshető módon tárolt papíralapú betegdokumentumokra is alkalmazni kell a GDPR előírásait.

A titkosítatlan egészségügyi adatokat tartalmazó pendrive elvesztése, az ilyen adatokat tartalmazó felhő-tárhelyből történő adatlopás, az orvosi képfelvételek elérhetetlenné válása, egy beteg egészségügyi adatainak rossz e-mail címre történő elküldése, vagy éppen az egészségügyi dokumentumok korlátlan letölthetősége mind-mind az adatbiztonság sérülését jelenti, úgynevezett *adatvédelmi incidensnek* minősül.

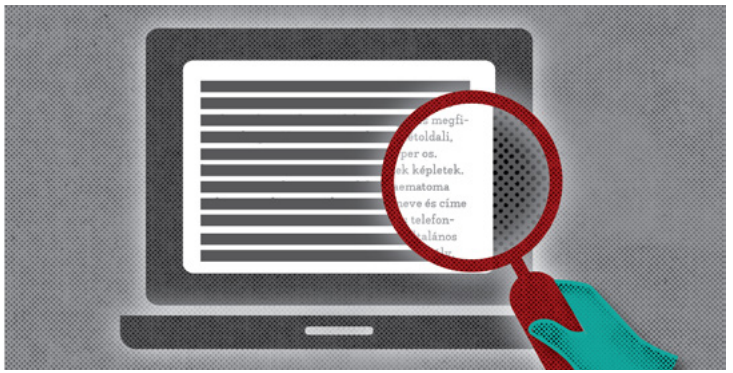
Az egészségügyi adatok a személyes adatok olyan különleges kategóriáját képezik, amely fokozott védelemben részesül, emiatt a biztonsági intézkedésekre is fokozott figyelmet kell fordítani. Az adatvédelmi incidens jogsérelmet, nyilvánvaló károkat okozhat a betegnek. Ha az egészségügyi adataival együtt kezelt személyazonosító adatai illetéktelen kezekbe kerülnek, akár személyazonosságával is visszaélhetnek. Ha adatvesztés következik be – mert például bizonyos egészségügyi adatok visszaállíthatatlan módon törlődnek a nyilvántartási rendszerből –, ennek következtében a beteg késedelemmel juthat a szükséges orvosi ellátáshoz. Ha akarata ellenére nyilvánossá válik valamely betegségének, egészségügyi problémájának a ténye, ennek révén akár zaklatás, kiközösítés áldozatává is válhat – különösen, ha a többségi társadalom által szégyenletesnek tartott, például pszichiátriai vagy nemi betegségtől szenved.

Ha egy egészségügyi szolgáltatónál felmerül az adatvédelmi incidens gyanúja, az adatkezelő haladéktalanul belső vizsgálatot köteles lefolytatni annak megállapítása céljából, hogy tényleg adatvédelmi incidensnek tekinthető-e az esemény.

Ha valóban adatvédelmi incidens történt:

1. *Az adatkezelőnek mindent meg kell tennie annak érdekében, hogy csökkentse a veszteségeket, valamint megelőzze a további károkat (pl. használatba kell vennie az érintett adatokról készült biztonsági másolatot).*
2. *Értékelnie kell, hogy az incidens mekkora kockázattal jár az érintettekre. Ennek során az adott eset számos körülményét kell mérlegelnie, mint például:*
    - *Milyen adatokat érint az incidens?*
    - *Mi történt az adatokkal?*
        - » *Adatlopás esetén az adatok titkosítva voltak-e, vagy azokhoz könnyen hozzá lehet férni?*
        - » *Elvesztés vagy sérülés esetén helyreállíthatóak-e az adatok?*
    - *Hány személyt érint az incidens?*
    - *Az adatok nyilvánosságra kerülése milyen sérelmet okozhat az érintetteknek?*
3. *Az adatkezelő köteles az incidensekről nyilvántartást vezetni.*
4. *Szükség esetén az adatkezelőt értesítési kötelezettség is terheli.*

Az adatvédelmi incidenst az adatkezelő indokolatlan késedelem nélkül – fő szabály szerint az incidensről való tudomásszerzését követő legkésőbb 72 órán belül – köteles bejelenteni az illetékes felügyeleti hatóságnak, ami Magyarországon a Nemzeti Adatvédelmi és Információszabadság Hivatal (NAIH). A bejelentésben le kell írni az incidens mibenlétét, annak valószínűsíthető következményeit, továbbá az adatvédelmi incidens orvoslása érdekében már megtett, illetve megteendő intézkedéseket. A bejelentési kötelezettség alól kivételt képez, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a betegek jogaira nézve – például ha szerverhiba miatt adatvesztés történt, de a biztonsági másolatból az eltűnt adatokat azonnal helyre lehetett állítani. A NAIH megvizsgálja a bejelentést, és akár adatvédelmi bírságot is kiszabhat, ha megállapítása szerint az adatkezelő megszegte az adatvédelmi előírásokat, például ha az adatvédelmi incidens azért következett be, mert az adatkezelő elmulasztotta a megfelelő biztonsági intézkedések megtételét.



Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül köteles értesíteni az érintette(ke)t is. A kockázat nagyságát az érintettek szemszögéből kell mérlegelni. Szinte mindig valószínűsíthetően magas a kockázat akkor, ha az incidens egészségügyi adattal kapcsolatos. Az érintetteket közérthető módon tájékoztatni kell a következőkről:

- az adatvédelmi incidens jellege (pl. adatvesztés, adatlopás),
- az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó neve és elérhetőségei,
- az incidens valószínűsíthető következményei,
- az adatkezelő által az incidens orvoslására tett intézkedések (beleértve az esetleges hátrányos következmények enyhítését célzó intézkedéseket is),
- továbbá tájékoztatás arról, hogy az érintett miként védekezhet a lehetséges hátrányos következményekkel szemben.

Ami az adatbiztonságot illeti, a GDPR-nak és a többi adatvédelmi jogszabálynak való megfelelés bizonyos szempontból egyéniesített módon követeli meg az óvintézkedéseket mindazoktól, akik személyes adatokat, ezen belül érzékeny adatnak minősülő egészségügyi adatot kezelnek. Egy egyéni vállalkozóként dolgozó orvostól túlzás lenne megkövetelni azt, hogy magánrendelőjében a betegei egészségügyi adatainak tárolására használt számítógépet biztonsági kamerákkal megfigyelt, számkódos zárral ellátott külön helyiségben őrizze – míg ugyanezen intézkedések egy megyei kórház szerverei esetén már nem tűnhetnek eltúlzottnak. Ha valaki egy állam által működtetett intézményben dolgozik, elsősorban az a teendője, hogy a kérdéses intézmény adatvédelmi szabályzatában előírtakat kövesse – e szabályzatot az adatvédelmi szakemberek az adott intézmény jellegzetességeire tekintettel (is) dolgozták ki. Ha valaki egyéni vállalkozó vagy kisebb társas vállalkozást működtet, az ő feladatát képezi az adatvédelmi szabályzat létrehozása, ennek során pedig célszerű adatvédelemben járatos szakemberrel konzultálni arról, hogy számára mi jelenti a GDPR előírásainak megfelelő adatvédelmi megoldásokat.

Néhány gyakorlati szempont

elsősorban a magán-praxisban dolgozók számára

Tegyünk biztonságossá minden olyan elektronikus és internetes kommunikációs csatornát, amit a betegeinkkel történő kapcsolattartásra használunk. Az adatvédelmi előírások jegyében számos munkáltató maga gondoskodik minderről. Ha a biztonságos kapcsolattartás létrehozásáért mi vagyunk a felelősek, a fentiek megvalósításához vegyük igénybe adatvédelmi, illetve informatikus szakember segítségét. A piacon számos elérhető megoldás létezik, a letölthető adattitkosító segédprogramoktól kezdve az olyan e-mail szolgáltatókig (mint pl. a Protonmail), akik szavatolják a teljes üzenetküldési folyamat biztonságosságát. Ha tanácstalanok vagyunk, feltétlenül konzultáljunk megfelelő szakértővel.

Ha saját honlapot üzemeltetünk, azt olyan informatikus szakemberrel terveztessük meg, aki járatos a GDPR adatvédelmi szabályrendszerében.

Ha „Az online vizit" fejezetben említett videóhívásos távkonzultációt folytatunk, azt adatvédelmi szempontból megbízható platformon tegyük. Mérvadó vélemények szerint ilyen például a Microsoft Teams és a Skype for Business, míg a Facebook Messenger és a WhatsApp nem GDPR-kompatibilis. Mivel azonban nem létezik „feltörhetetlen" platform, betegünket feltétlenül tájékoztassuk arról, hogy még a biztonságos csatornán is történhet – habár rendkívül ritkán – adatvédelmi incidens.

A betegeinkkel történő e-mailes kapcsolattartás során lehetőleg ne használjunk ingyenes, tömegek által használt, adatvédelmi szempontból nem teljesen megbízható levelezőszolgáltatásokat.

Ha betegünknek tömegek által használt ingyenes levelezőszolgáltatásnál van fiókja, lehetőleg írásban kérjük nyilatkozatát arról, hogy tudomásul veszi, miszerint saját magának kell gondoskodnia a levelek adatvédelmi szempontból biztonságos fogadásáról és küldéséről, illetve hogy tisztában van-e a népszerű levelezőprogramok nem tökéletes megbízhatóságával. A NAIH állásfoglalása szerint az adatkezelő ugyanakkor nem mentesül a személyes adatok biztonságos továbbításának követelménye alól pusztán azért, mert a címzett nem képes az üzenet biztonságos fogadására. Ha tehát betegünk a Yahoonál vagy Citromailnél nyitott fiókjába kéri a levelezést, nekünk ennek ellenére gondoskodnunk kell a kimeneti adatvédelemről.

A betegeinkkel történő e-mailes kapcsolattartás során lehetőleg ne használjuk privát e-mail címünket. Számos munkáltató adatvédelmi megfontolásból egyenesen tiltja, hogy munkaügyben történő levelezésre magáncímünket használjuk.

Betegünket figyelmeztessük az e-mailes kapcsolattartás esetleges biztonsági veszélyeire, így például arra, hogy az e-mailek esetén is történhet félrekézbesítés, továbbá kérjük meg annak megfontolására, hogy vajon mások (például kíváncsi családtagok) nemkívánatos módon hozzáférhetnek-e a levelezéshez. Ha páciensünk ennek ellenére kéri az e-mailes kapcsolattartást, nyilatkozatát lehetőleg írásban rögzítsük.

Ha egészségügyi adatot tartalmazó dokumentumot csatolmányként küldünk, a dokumentumot védjük jelszóval. A szövegszerkesztő programok (mint pl. a Microsoft Word) lehetővé teszik a dokumentumok jelszóval történő levédését – használjuk e funkciót.

Ha titkosítatlan csatornán küldünk e-mailt betegünknek, az ne tartalmazzon személyes adatot. Az adatvédelmi szempontból nem biztonságos e-mailt csak olyan semleges adatok küldésére használjuk, mint például egy időpontfoglalás tényének visszaigazolása.

Az e-mailek „Tárgy” mezőjében ne szerepeljenek személyes adatok.

SMS vagy hangposta-üzenet formájában betegünkkel egészségügyi adatokat ne közöljünk.

E-mailes jelszavaink (és általában az egészségügyi adatok védelme során használt jelszavaink) legyenek biztonságosak. A biztonságos jelszó legalább 8 karakter hosszúságú, tartalmaz kis- és nagybetűt, számokat és speciális karaktereket, továbbá nem köthető a felhasználóhoz. Jelszóként ne használjuk például házastársunk születési dátumát vagy gyermekeink keresztnevét.

Jelszavainkat őrizzük mások által nem hozzáférhető módon, azokat időközönként változtassuk, továbbá ne használjuk azokat egynél több helyen.
Ha e-mail fiókjainkhoz, webboltos regisztrációinkhoz, Facebook-oldalunkhoz és más hasonlókhoz ugyanazt a jelszót használjuk, ezáltal rendkívül sérülékennyé válunk.

Felhőalapú szolgáltatás igénybevételekor mindig győződjünk meg arról, hogy az adatokat tároló szerver melyik országban található. Lehetőleg ne válasszunk olyan szolgáltatót, akinek a szerverparkja az Európai Gazdasági Térségen kívül található. Ha mégis úgy döntünk, hogy ilyen szolgáltatóra bízzuk az adatok feldolgozását, figyeljünk arra, hogy – fő szabály szerint – e szolgáltatónak is a GDPR által elvárt biztonsági szinten kell működnie.

Egészségügyi adatot lehetőleg ne tároljunk felhőben. Ha mégis ezt választjuk, gondosan tájékozódjunk a felhőszolgáltatónál alkalmazott biztonsági intézkedésekről – minimumkövetelménynek tekinthetjük a megfelelő titkosítást és jelszavas védelmet.

Az egészségügyi adatokat tartalmazó fájlokat lássuk el jelszóvédelemmel.

Minden egészségügyi adatot tartalmazó elektronikus adathordozót (számítógépet, pendrive-ot, stb.) szintén védjünk jelszóval, illetve alkalmazzunk titkosítást.

Adathordozóinkat tároljuk biztonságos helyen, például kulccsal zárható helyiségben elhelyezett, szintén kulccsal zárható szekrényben. A kisebb méretű elektronikus adathordozó (pl. egy külső merevlemez) biztonságos tárolásához a legmegbízhatóbb megoldás a páncélszekrény.

Az általunk kezelt egészségügyi adatokról rendszeresen készítsünk biztonsági mentést egy olyan adathordozóra, ami a számítógépünkről leválasztható, elkülönülten tárolható.

Használjunk megbízható vírusvédelmi megoldásokat, tűzfalat.

Aranybánya vagy tiltott kincs? Az egészségügyi adatok kutatási célú felhasználása

Ahogyan ezt „Az adatok szerepe a digitális egészségügyben” című fejezetben is olvashatjuk, az adat az „új olaj”, az egészségügyi ellátórendszer pedig minden pillanatban száz- és százezernyi újabb „olajcseppet”, egészségügyi adatot hoz létre. Már egyetlen ellátónál is jelentős mennyiségű információ gyűlik össze, a központosított egészségügyi adatbázisokban tárolt adatok száma azonban ennek sokszorosa. Példának okáért Magyarország új e-egészségügyi rendszere, az Elektronikus Egészségügyi Szolgáltatási Tér (EESZT) 2017. november 1-jén kezdte meg működését, a felhasználók pedig – nem egészen egy év alatt – több mint 500 millió egészségügyi adatot töltöttek fel a rendszerbe. 2018 őszén az EESZT Fenntartási és Üzemeltetési Főosztályának vezetője úgy nyilatkozott, hogy naponta 800 ezer és egymillió közötti eReceptet és több millió egyéb dokumentumot töltenek fel az egészségügyi intézmények [7]. Azóta a felhasználók köre tovább bővült, hiszen a közfinanszírozott ellátókat követően 2020. január 1-ig a teljes magánszolgáltatói körnek is csatlakoznia kellett a rendszerhez, így nyilvánvalóan a rendszerbe feltöltött adatok száma is egyre nő.

A régebbi, papíralapú rendszerekhez képest a modern digitalizált adatbázisoknak nem csak az az előnye, hogy szinte végtelen mennyiségű adat tárolására képesek, hanem az is, hogy sokkal könnyebb keresést végrehajtani bennük. Az irattárakban, archívumokban iratlapozgatással töltött hosszú órák helyett a vágyott adatot – vagy éppen a kívánt adatok egész tömegét – pár perc alatt, néhány gombnyomással is megszerezhetjük.

Nem véletlen, hogy a digitalizált adatbázisok a különböző szakterületeken működő tudományos kutatók figyelmét is felkeltették, az orvostudományok területén tevékenykedő szakembereket is ideértve. A hagyományos módszerekkel folytatott orvosbiológiai kutatások mellett olyan új kutatási irányok is megjelentek, amelyek az egészségügyi elektronikus adattároló rendszerekben tárolt nagy mennyiségű adat vizsgálatán nyugszanak, tehát amelyek elemzik az adatállományokat és következtetéseket vonnak le belőlük – anélkül, hogy a kutatási alanyokon bármiféle orvosi beavatkozást végeznének, sőt anélkül, hogy a kutatási alanyok egyáltalán jelen volnának [8].

TUDTA?

A nagy mennyiségű egészségügyi adatot tartalmazó nyilvántartásokban végzett kutatást orvostudományi kutatásnak kell tekinteni. Ilyen kutatást csak etikai bizottsági hozzájárulással és hatósági engedéllyel lehet folytatni, tehát az egészségügyi adatok kezelője az ilyen adatokat csak érvényes engedély alapján adhatja ki a nála jelentkező kutatónak, a kutatót pedig a megismert személyes adatok vonatkozásában titoktartási kötelezettség terheli [9].

A GDPR megalkotói szintén felismerték a különböző adatbázisok tudományos jelentőségét, ennek megfelelően pedig a bevezető rendelkezések között találhatjuk a következő megállapítást: *„A nyilvántartásokból nyert információk összevetésével a kutatók jelentős értékű új tudásra tehetnek szert többek között a széles körben elterjedt betegségekkel – például a szív- és érrendszeri betegségekkel, a rákkal, és a depresszióval – kapcsolatban.*" Ennek megfelelően a GDPR lehetővé teszi azt, hogy a személyes adatok különleges kategóriájának minősülő egészségügyi adatokat tudományos kutatási célból kezeljék.

Ez az adatfelhasználás két formában történhet. Egyrészt végezhetünk olyan kutatást, amely közvetlenül a tudományos tanulmányozás céljára gyűjtött egészségügyi adatok felhasználásával jár: ez történik például akkor, ha a cukorbetegség vizsgálatára irányuló kutatás keretében cukorbetegektől gyűjtenek egészségügyi adatokat kérdőív használatával. Egészségügyi adatokat kutatási célra azonban úgynevezett „további adatkezelés" formájában is használhatunk: ekkor a kérdéses egészségügyi adatokat eredetileg más célból gyűjtötték, a kutató pedig saját kutatási tervének megfelelően búvárkodik az adatok között. Ez történik például akkor, ha egy kórház adatbázisában vizsgálják a császármetszések számának alakulását az elmúlt 10 év során. Az egészségügyi adatok kutatási célú kezelését minden esetben a GDPR adatkezelési elveivel összhangban, a személyes adatok e különleges kategóriájának jogszerű kezelésére vonatkozó előírások megtartásával, egyben az adott uniós tagállam nemzeti jogszabályainak megfelelő módon kell gyakorolni [10].

Lényegében a „további adatkezelés" esetét szabályozza – meglehetősen szűkszavú módon – a magyar Eüak. is, amikor kimondja a következőket: *„Tudományos kutatás céljából az intézményvezető vagy az adatvédelmi tisztviselő engedélyével a tárolt adatokba be lehet tekinteni, azonban tudományos közleményben nem szerepelhetnek egészségügyi és személyazonosító adatok oly módon, hogy az érintett személyazonossága megállapítható legyen. Tudományos kutatás során a tárolt adatokról nem készíthető személyazonosító adatokat is tartalmazó másolat.*" A jogszabály továbbá kötelező intézkedésként írja elő azt, hogy a tárolt adatokba betekintett személyekről, a betekintés céljáról és időpontjáról nyilvántartást kell vezetni. A nyilvántartás kötelező megőrzési ideje 10 év.

A fenti rendelkezések két, társadalmi szempontból egyaránt kiemelkedően fontos értéket próbálnak meg kiegyensúlyozott mó-

don óvni: az egyik a személyes adatok védelme, a másik pedig az egész társadalom számára hasznos orvostudományi kutatások segítése. Nem szabad ugyanakkor megfeledkeznünk arról sem, hogy mindez egy olyan globális környezetben történik, ahol az adatok egyre inkább árucikké válnak: egy 2018-as pénzügyi elemzés szerint az egészségügyi big data-val történő globális kereskedelem értéke 2017-ben 14,25 milliárd USA-dollár volt, amely 2025-re valószínűleg eléri majd a 68,75 milliárd dollárt [11]. Nem meglepő, hogy több országban az érdekelt piaci szereplők – a szabályok lazítása érdekében – igyekeznek nyomást gyakorolni a vonatkozó jogszabályok megalkotóira. Ennek ellenére a GDPR továbbra is annak fontosságát hangsúlyozza, hogy bizonyos típusú személyes adatokat (ezen belül pedig egészségügyi adatokat) elsősorban az érintett beleegyezésével lehet kezelni, ugyanakkor elismeri azt is, hogy bizonyos helyzetekben az adatkezelésbe történő beleegyezés követelményét – természetesen megfelelő biztosítékok mellett – alá kell rendelni más jogos érdekeknek. Ilyen helyzet lehet például az, ha az egészségügyi adatokon a társadalom számára kiemelkedő fontosságú orvostudományi kutatást folytatnak, hiszen ha az érintett személyek tömegesen visszavonnák az adataik kezelésére vonatkozó beleegyezésüket, mindez veszélyeztetné a kutatás tudományos érvényességét, sikerét. A GDPR ugyanakkor csak elvi szinten fogalmazza meg azt a követelményt, hogy az egészségügyi adatokon folytatott kutatások esetén az egyéni és társadalmi érdekek között gondosan megfontolt kompromisszumot kell kötni, a konkrét szabályok megalkotását az egyes tagállamokra hagyja. Mivel azonban az országonként eltérő szabályok nehezítik az uniós szintű tudományos együttműködést, a részletszabályok vonatkozásában is egységesítésre volna szükség. [12]

„Nem mondhatom el senkinek, elmondom hát mindenkinek” – egészségügyi adatok megosztása az interneten

Közismert tény, hogy az ezredforduló környékén valódi világhálóvá fejlődött internet valamilyen mértékben minden felhasználójának életét megváltoztatta – többek között azért is, mert az online univerzum társas kapcsolataink színhelyévé is vált [13]. Barátaink, de akár valamely híresség életét is a Facebookon követjük, szeretteinkkel e-mailezünk és Skype-olunk, egy-egy internetes szerepjátékban pedig olyan emberek lehetnek a társaink, akik Ausztráliától Indián át Norvégiáig bármelyik országban élhetnek, és akikkel valószínűleg sohasem találkozunk majd személyesen.

Míg az online világ milliárdnyi szállal kötődik a „valódi” élethez, számos olyan tulajdonsággal is bír, ami igencsak eltér a minket kör-

bevevő anyagi valóságtól [14]. Ezek közül az egyik legfontosabb az, hogy az online világban egy felhasználó névtelenséget élvezhet: számos platformon nem kötelező megadnunk személyes adatainkat, saját nevünk helyett felhasználónéven (nicknéven) szerepelhetünk, ha pedig valaki beleegyezésünk nélkül leplezi le kilétünket, hozza nyilvánosságra nevünket, lakcímünket vagy más személyes adatunkat (ez az úgynevezett doxing), cselekedete – az adott országban hatályos jogszabályoktól függően – akár büntetőjogi jogkövetkezményekkel is járhat [15].

Az anonimitáson túl az online környezet láthatatlanságot is biztosíthat. Az elsősorban szöveges kommunikációra épülő felületeken – mint például egy honlap kommentszekciójában – a hozzászólók nem látják és hallják egymást. A kibertér továbbá lehetővé teszi az aszinkron, időben elcsúszó kommunikációt, amikor tehát egy közlés és a válaszreakció között hosszabb idő is eltelhet: egy e-mailben feltett kérdésünket a címzett akár órákkal vagy napokkal később válaszolhatja meg, egy Facebook-bejegyzésükre hónapokkal később érkezhet lájk vagy éppen lekicsinylő megjegyzés. Megtörténhet, hogy időközben már régen elfelejtettük, mit is posztoltunk a világhálón. A névtelenség, arctalanság, valamint a tettek látszólagos „következmények nélkülisége" könnyen azt a gondolatot keltheti a felhasználókban, hogy az online térben senkit semmilyen felelősség nem terhel a tetteiért.

Mivel az online térben sokszor nem támaszkodhatunk a metakommunikációra, fantáziánk is szabadabban szárnyalhat. Számunkra fontos olyan testi és lelki tulajdonságokat, érzelmeket – őszinte megértést, toleranciát, érzékenységet, iránt unk érzett mély megbecsülést – tulajdoníthatunk csevegőtársainknak, amivel az offline világban egyáltalán nem bírnak, ugyanis a hiányzó információdarabkákat képzeletünkkel, vágyainkkal pótoljuk ki. Ez a pszichológiában jól ismert projekció, kivetítés jelensége.

Ahogyan ez „A közösségi médiahasználat alapkérdései" című fejezetben is olvasható, az online világ fenti sajátosságai képesek számos gátlást feloldani, ez pedig olyan cselekedetek elkövetésére csábíthatja a felhasználókat, amiket a „valódi" életben nem valósítanának meg [16]. Ennek kártékony változata az, ha az internet úgynevezett dezinhibíciós, gátlásokat oldó hatása a negatív érzelmek és viselkedésformák – elsősorban a düh és agresszió – előretörésében mutatkozik meg. Míg csalást, rágalmazást, zaklatást, személyes adattal való visszaélést legtöbbünk nem követne el az offline világban – például azért, mert a kérdéses tettek számos ország jogszabályai szerint bűncselekménynek minősülnek –, a virtuális térben egyre gyakoribb a *catfishing* (álidentitás használata) és *cyberbullying*, az internetes trollkodás, vagy az adathalászat [17].

Az online világ gátlásokat oldó hatása ugyanakkor pozitív módon is érvényesülhet. A kutatások szerint az online térben sokak empátiája is erősebben működik, segítőkészebben viselkednek, így például könnyebben és gyakrabban adományoznak jótékony célra, mint az offline világban [18]. Vannak, akik gyorsabban nyílnak meg, könnyebben „beszélnek" érzéseikről a virtuális térben, mint azt egy

hagyományos találkozás során tennék. Az offline életben különböző okok miatt magányosan élők úgy érezhetik, hogy a világháló tágítja emberi kapcsolatrendszerüket, enyhíti az elszigeteltség érzését; az online világban barátságok, sőt akár szerelmek is szövődhetnek [19].

Az online kapcsolattartás fenti sajátosságai miatt azonban igen rövid időn belül olyan információkat is megoszthatunk frissen szerzett ismerőseinkkel, amelyeket a „valódi" életben csak több évnyi ismeretség után fednénk fel előttük – ha egyáltalán valaha is úgy döntenénk, hogy elmeséljük nekik titkainkat [20]. Számos más információ mellett sokak számára az egészségükkel kapcsolatos bizonyos részletek is a „szigorúan bizalmas" kategóriába tartoznak. Az offline világban nagyon megfontolják, hogy kivel osszák meg azt a tényt, miszerint a gyermeknemzéshez nem rendelkeznek megfelelő minőségű spermiummal, avagy hogy kezdődő Alzheimer-kórt diagnosztizáltak náluk – ugyanakkor az online világban nyíltan „beszélgetnek" számos, többségében anonim felhasználóval e súlyos gondjaikról. Mindazonáltal, ahogyan ezt az adatvédelem kapcsán már említettük, az egészségügyi adatok igencsak érzékenyek, s ha azok illetéktelen kezekbe kerülnek, mindez komoly hátránnyal járhat az érintett számára. Éppen ezért célszerű alaposan megfontolnunk, hogy a Facebookon – de akár az anonim módon működő nyílt közösségi oldalakon vagy internetes fórumokon is – milyen információkat teszünk közzé egészségügyi állapotunkról. Egy nicknév mögött bárki megbújhat, de még a Facebookon is léteznek álprofilok [21]; mielőtt tehát egészségünkkel kapcsolatos személyes adatokat tennének fel a világhálóra, mérlegeljük, hogy a megosztani tervezett információt vajon mások a későbbiekben esetleg felhasználhatják-e ellenünk. Egy kíváncsi vagy egyenesen rosszindulatú személy számára az általunk elhullajtott „ténymorzsák" (mint például foglalkozásunk vagy a lakhelyünkül szolgáló város neve), a feltöltött fényképek metaadatai vagy a rajtuk látható, jól beazonosítható arcok mind-mind segítségül szolgálhatnak személyazonosságunk kinyomozása során. Egyfajta alapelvként érdemes követni azt az általános szabályt, hogy minél kevesebb érzékeny személyes információt, ezen belül pedig minél kevesebb egészségügyi adatot osztunk meg magunkról, annál kevesebb támpontot adunk a visszaélést esetlegesen tervezgető egyéneknek is.

> ***2010-ben egy angol édesanya [22] Gracie nevű kétéves kislányáról tett fel néhány fényképet a Facebookra, a képeket nézegető egyik – egészségügyi végzettségű – ismerősének pedig feltűnt, hogy a kislány két szeme nem egyforma módon reagált a fénykép készítése során használt vaku fényére. Javaslatának megfelelően a kislányt szülei orvoshoz vitték, aki egy agresszív, gyorsan fejlődő daganatfajtát, úgynevezett retinoblastomát diagnosztizált Gracie bal szemében. A gyors diagnózisnak köszönhetően a kislány életét megmentették, bár beteg szemét el kellett távolítani.***

Ugyanakkor tagadhatatlan, hogy – amint ez A közösségi médiahasználat az egészségügyben című fejezetben is említésre kerül

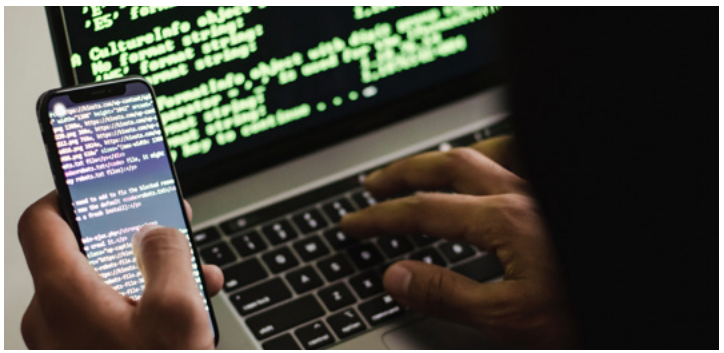
– a személyes információk közösségi médiában, interneten történő megosztása orvosilag hasznos is lehet. Az internet széles körű elterjedése jelentős mértékben serkentette az úgynevezett *online health community*-k (OHC-k), azaz olyan online közösségek kialakulását, amelyek tagsága elsősorban valamely krónikus és gyógyíthatatlan betegségtől szenvedő egyénekből áll, de a tagok között egészségügyi szakembereket is találhatunk. A Parkinson-kórral, HIV/AIDS-fertőzéssel vagy éppen szklerózis multiplexszel küzdő páciensek egyrészt élvezhetik sorstársaik érzelmi támogatását, amit a gondozásukban alkalmanként megfáradt hozzátartozóik nem mindig képesek megadni nekik, másrészt a betegségükkel, illetve állapotukkal kapcsolatos információkat is kaphatnak a többi résztvevőtől [23]. Az OHC-k azonban nem kizárólag krónikus betegeket tömöríthetnek: vannak, akik arra szeretnének választ kapni, hogy életmódjuk vagy családi előtörténetük alapján milyen egészségügyi kockázatoknak vannak kitéve, hogyan tudnák megakadályozni vagy lassítani egy-egy betegség bekövetkeztét, vagy éppen orvosi tanácsot remélnek betegségük jobb kezelésére vonatkozóan.

Akármilyen is legyen azonban az OHC-k célja és tagsága, mindegyik online közösség ugyanazzal a dilemmával szembesül: az egészségügyi képzettséggel nem rendelkező tagok csak akkor élvezhetik teljes egészében a közösség által biztosított előnyöket, ha a lehető legtöbb egészségügyi információt teszik nyilvánossá saját magukról, ha a lehető legnagyobb részletességgel számolnak be tüneteikről, gyógyszerszedési szokásaikról, életmódjukról.

Míg többeket mindez nem tölt el különösebb aggodalommal, egyre növekszik azoknak a száma, akik – a terjedő kiberbűnözés, az internetes visszaélések, adatszivárgással kapcsolatos botrányok tükrében – egyre inkább kételkednek abban, hogy bizalmas és érzékeny adataik valóban biztonságban vannak a közösségen belül. Az OHC-k működéséért felelős adminisztrátorok így kettős kihívással szembesülnek. Egyrészt növelniük kell az egészségügyi adatok közösségen belüli nyilvánosságra hozásából származó előnyöket, másrészt csökkenteniük kell a tagok adatvédelemmel kapcsolatos aggodalmait – például úgy, hogy biztonságosabbá teszik az internetes felületeket, négyszemközti orvosi konzultációs lehetőséget biztosítanak a közösség tagjainak, továbbá a csoporton belül erősítik a védő és támogató légkört. Ezen túl az adminisztrátoroknak folyamatosan hangsúlyozniuk kell a titoktartási előírások fontos mivoltát, növelniük kell a személyes adatok védelmét szolgáló megoldások és eszközök biztonsági szintjét, valamint a tagok figyelmét is fel kell hívniuk az adatvédelem fontosságára. A tagoknak maguknak is egyfajta tanulási folyamaton kell(ene) végigmenniük, amelynek során alaposabban megismerkedhetnek a titoktartásra vonatkozó jogszabályok lényeges rendelkezéseivel, az adott OHC-ben érvényesülő adatvédelmi előírásokkal, képessé válnak felismerni azt, hogy milyen egészségügyi adataikat célszerű megosztani az OHC-vel, valamint hogy tudatosabban, körültekintőbb és visszafogottabb módon járjanak el akkor, amikor az egészségi állapotukkal kapcsolatos érzékeny és bizalmas adatok megosztására készülnek [24].

> *2018 tavaszán a Twitteren végigsöpört a #ShareAStoryInOneTweet (kb. „Ossz meg egy történetet egyetlen tweetben") hashtaggel jelölt kezdeményezés. A 2018 májusában megosztott 43374 ilyen témájú tweetből 1206-ot egészségügyi dolgozók, ezen belül túlnyomórészt orvosok közöltek a nagyvilággal. A történetek olyan megdöbbentő arányban tartalmaztak személyes részleteket (alkalmanként akár még a kezelt páciens teljes nevét is), hogy a kutatók megalapozott véleménye szerint 754 orvosi tweetből 242 esetben, tehát az esetek majdnem egyharmadában a barátok és családtagok képesek voltak beazonosítani a történet főhősét* [25].

A fenti szempontok megfontolása azonban nem csak azoknak lehet hasznos, akik egészségügyi gondjaikkal kapcsolatban fordulnak segítségért az „internet népé"-hez: fontos felismernünk azt is, hogy az online környezet korábbiakban körvonalazott gátláscsökkentő hatása az egészségügyi szakembereket sem hagyja érintetlenül.



Az Egyesült Államokban már a 2000-es évek elején elterjedőben voltak az orvosi blogok, amelyekben egy-egy egészségügyi szakember osztotta meg történeteit a világgal – 271 ilyen jellegű blog tartalmának elemzését követően pedig a kutatók arra az eredményre jutottak, hogy 114-ben szerepeltek egyedi esetleírások, 45 blogszerző pedig annyira részletesen írta le az általa kezelt páciensek történetét, hogy az érintettek személyazonosságát könnyen ki lehetett találni [26]. Ennek következtében – teljesen érthető módon – felvetődött a következő kérdés: vajon etikusan jár-e el az az egészségügyi szakember, aki betegei előzetes jóváhagyása nélkül, nyilvános módon blogol róluk [27]?

Az internet óvatlan kommunikációra serkentő hatását igazolta továbbá az a kutatás is, amelyben fiatal orvosok Facebook-használati szokásait elemezték: 338 frissen végzett új-zélandi orvosból 65%-nak volt Facebook-fiókja, ezen belül a fióktulajdonosok 63% állította be fiókját úgy, hogy azt csak a „barátok" láthatták. A nyilvánosan maradt fiókok tulajdonosai sokszor osztottak meg egészségbarát tevékenységekkel (sportolással, egészséges étkezéssel stb.) kapcsolatos információkat, azonban a posztolók 46%-a olyan fényképeket is közzétett magáról, amelyek alkoholfogyasztás közben ábrázolták őt, továbbá olyan magánjellegű információkat is megosztott (pl. hogy valaki a *„Perverts united"* – kb. *„Világ perverzei egyesüljetek"* – elnevezésű Facebook-csoport tagja), amelyek alkalmasak lehetnek arra, hogy a betegekben visszatetszést keltsenek, bizalomvesztést okozzanak, megváltoztassák az orvos-beteg kapcsolat professzionális jellegét, valamint aláássák az orvosi hivatás tekintélyét [28].

A fentiek alapján egyáltalán nem meglepő az, hogy az orvosi témájú blogok, tweetek és Facebook-posztok elszaporodásával megjelentek a betegek ezzel kapcsolatos panaszai is. Egyetlen adalékként érdemes felidézni azt, hogy 2015. január elseje és 2017. június 30. között az Egyesült Királyságban működő orvosszakmai nyilvántartási és felügyeleti főszerv (a General Medical Council) huszonnyolc esetben folytatott le vizsgálatot azért, mert a betegek panasza szerint orvosuk nem megfelelően használta a Facebookot, Twittert, illetve WhatsAppot [29]. Természetesen ma már elképzelhetetlen volna olyan elvárást támasztani az egészségügyi dolgozókkal szemben, hogy tartsák távol magukat az internettől és a közösségi média különféle platformjaitól: számos felidézett példa egyértelmű módon igazolja azt, hogy az orvosok, szakápolók, klinikai szakpszichológusok, gyógytornászok online jelenléte több mint hasznos és kívánatos. Mielőtt azonban egészségügyi dolgozóként megosztanánk egy munkahelyünkön készült fényképet a Facebookon, vagy éppen elmesélnénk egy megható vagy felzaklató betegtörténetet a Twitteren, mindig emlékeznünk kell arra, hogy a hivatásunkra vonatkozó etikai és jogi előírások – ezen belül pedig különösen az orvosi titoktartás kötelezettsége – ebben az esetben is kötnek minket. A világ több országában már láthattunk példát arra, hogy valakinek a kórházi munkahelyébe került egy meggondolatlanul közzétett Facebook-poszt – mi lehetőleg ne szaporítsuk ezeknek az eseteknek a számát [30].

Egészségügyi dolgozóként hogyan használhatjuk etikus és jogszerű módon a közösségi médiumokat, valamint az internetet?

Tegyük	Ne tegyük
Vonjunk határvonalat személyes és szakmai online életünk, internethasználatunk között.	Ne ringassuk magunkat abba a csalóka hitbe, hogy kommentjeink, más online megnyilvánulásaink nem kerülhetnek ki a nagyközönség elé.
Használjuk a közösségi médiát edukációs célokra.	Az online világban ne „beszéljük ki" kollégáinkat, betegeinket, munkahelyünket – az orvosi titoktartás itt is köt minket.
A közösségi médiában fiókunk biztonsági szintjét állítsuk a lehető legmagasabbra, „barátaink" és követőink száma a lehető legkevesebb legyen.	Ne töltsünk fel saját magunkról, kollégáinkról vagy betegeinkről készült munkahelyi fényképeket az internetre.
Mielőtt bármit is leírnánk, gondolkodjunk el: valóban szükséges és hasznos leírnunk-megosztanunk az interneten mindazt, amit éppen publikálni készülünk?	Ne kommentáljuk meggondolatlanul kollégáink közösségi médiában megjelenő megnyilvánulásait.
Mindig járjunk el tisztességesen – a törölt kommentek, posztok a legtöbb esetben visszaállíthatóak.	Az online világban könnyelműen és meggondolatlanul ne osztogassunk orvosi tanácsokat.
Minden online megnyilvánulásunkat tekintsük úgy, mintha azok nyilvánosak, eltüntethetetlenek és a nagyközönség által továbbadhatóak-megoszthatóak lennének.	A közösségi médiafelületeket ne használjuk olyan módon, ami alááshatja az orvosi hivatásba vetett bizalmat.
Szigorúan kövessük az internet- és médiahasználatra vonatkozó munkahelyi előírásokat.	Ne használjuk a közösségi médiát arra, hogy magánjellegű kapcsolatot létesítsünk vagy tartsunk fenn jelenlegi vagy hajdani betegeinkkel.

Mit ígér a jövő?

Az adatvédelmi kérdéseken túl a hihetetlen sebességgel fejlődő orvosi technológiák a 21. század jogászait olyan további kihívások elé is állítják, amelyek néhány éve még a tudományos fantasztikum világába tartozónak tűntek. Az egészségügy területén alkalmazott okos algoritmusok előítéletessége miatt vannak, akik – majdhogynem Asimov híres robotika-törvényeire emlékeztető módon – jogszabályban fektetnék le azt, hogy az ilyen algoritmusok fejlesztését végző csapatok összeállítása során a munkahelyi diverzitást a lehető legnagyobb mértékben legyen kötelező érvényesíteni, illetve hogy az egészségügyben alkalmazott algoritmusokat külső, pártatlan szakértőkkel kelljen felülvizsgáltatni és jóváhagyatni.

További kérdésként a sebészeti robotok és orvosi képelemző szoftverek használata az orvoslásban eddig még nem tapasztalt felelősségi kérdéseket vet fel. Bár ezeket a megoldásokat egyelőre inkább csak kifinomult segédeszközként használják az orvosok – így például az algoritmus által kiválogatott képfelvételek végső elemzését ember végzi, illetve a robotkarokat is ember mozgatja –, mégis el kell gondolkodnunk azon, hogy miként alakuljon az orvosi eljárásért való jogi felelősség akkor, ha a közeljövőben ezek a rendszerek autonóm módon diagnosztizálnak, illetve műtenek majd. Példának okáért a sebészeti beavatkozás során bekövetkező hibáért kit tekintsünk felelősnek? Az emberi sebészt, aki maga használta a robotot vagy engedélyezte annak használatát? A robot tervezőjét vagy programozóját? Azt a kórházat, amelyik lehetővé tette az eljárás alkalmazását?

További új kihívást jelent az is, hogy genetikai ismereteink rohamos bővülésével egyre többet tudhatunk meg minden emberi lényről, ezzel együtt pedig mind csábítóbb az a lehetőség is, hogy a genetikai információkat táguló körben használjuk fel. Megengedhető-e például az, hogy egy biztosítótársaság csak olyan ügyféllel kössön szerződést, aki hajlandó genetikai tesztnek alávetni magát? Elképzelhető-e az, hogy egy idősotthon visszautasítsa egy olyan lakójelölt befogadását, aki – genetikai tesztje alapján – hajlamos az Alzheimer-kórra, tehát elképzelhető, hogy ellátása a későbbiekben sok gonddal fog járni és a „problémás" lakó rontja majd az idősotthon piacképességét is?

Ezek a felhasználási módok egyelőre a világ számos országában tiltottak, azt azonban nem láthatjuk előre, hogy a fentiekkel kapcsolatban egyre jelentősebbé váló piaci érdekek milyen irányba tolják majd el a szabályozást. Egyidejűleg számolnunk kell azzal is, hogy az egészségügyi adatok – ezen belül pedig különösen a hatalmas adatbázisok – jelentős kereskedelmi értékkel bírnak, immár nem csak a feketepiacon. Jelenleg például az Amerikai Egyesült Államok egyetlen tagállamában érvényesül az a szabály, hogy a digitalizált egészségügyi adatok tulajdonosa maga a páciens, a többi tagállam jogalkotása vagy az egészségügyi ellátót nevezi meg az adatok tulajdonosaként, vagy nem rendezi a kérdést. Ennek következtében a digitalizált adatokkal való kereskedelem milliárdos iparággá nőtte

ki magát, míg a betegek mindebből anyagilag nem profitálnak. Kérdéses az, hogy megállítható-e ez a folyamat, vagy a későbbiekben az anonimizált egészségügyi adatokkal történő szabad kereskedés fog bevett gyakorlattá válni azokban az országokban is, ahol mindezt eddig még nem tették jogszerűvé. Olyan változásoknak vagyunk tehát tanúi, amelyek mihamarabbi válaszadásra, az évtizedekig megszokott gondolkodásmódtól való eltávolodásra, gyökeresen új megközelítések alkalmazására kényszerítik a jogalkotókat és a jogalkalmazókat egyaránt.

Következtetések

Számos más szakterület művelőihez hasonló módon az internet valódi világhálóvá fejlődése visszavonhatatlanul átalakította az egészségügyi dolgozók hivatásgyakorlásának kereteit is. Az egyre gyorsabban zajló digitalizáció, az egyre nagyobb mennyiségű egészségügyi adat egyre gyorsabb áramlása, az orvos-beteg kapcsolat online térbe történő fokozatos áthelyeződése szinte naponta szembesíti a szereplőket olyan új problémákkal, amelyeknek eddig még nem tapasztalt etikai-jogi vonatkozásai is vannak. A 21. század e-egészségügyében jelenleg a legnagyobb kihívást a személyes adatok megfelelő jogi védelme jelenti, hiszen az orvosi titoktartás évezredes parancsát az online világban egyre nehezebb megfelelő módon követni. Emiatt is különösen fontos az, hogy – úgy orvosként, mint betegként – lehetőleg legyünk tisztában néhány olyan alapvető jogi előírással és jó gyakorlattal, amelyek megkönnyíthetik számunkra az online világban történő biztonságos jelenlétet, valamint a jogsértő helyzetek megelőzését és elkerülését.

Kvízkérdések:

Az alábbiak közül melyik NEM minősül egy beteg egészségügyi adatának?

- ◯ A páciens zajos és poros munkahelyen dolgozik.
- ◯ A páciens feleségének édesanyja cukorbeteg.
- ◯ A páciens munkahelyi problémái miatt rosszul alszik.
- ◯ A páciens édesapja és édesanyja egyaránt parlagfű-allegiától szenved.

Ellopnak egy olyan laptopot, amelyen a kórházi informatikai rendszerben tárolt egészségügyi adatok másolata van, titkosított formában. A titkosítás miatt a tolvaj nem fér hozzá az adatokhoz. Történt-e adatvédelmi incidens?

- ◯ Nem történt, hiszen az adatok nem vesztek el, semmisültek meg, vagy kerültek nyilvánosságra.
- ◯ Történt, de az valószínűsíthetően nem jár kockázattal a betegek jogaira nézve, így elegendő az incidenst az adatkezelő nyilvántartásába bejegyezni.
- ◯ Történt, méghozzá olyan, amely valószínűsíthető kockázattal jár a betegek jogaira nézve, ezért azt a NAIH-nak be kell jelenteni.
- ◯ Történt, méghozzá olyan, amely valószínűsíthetően magas kockázattal jár a betegek jogaira nézve, ezért azt a NAIH-nak be kell jelenteni, továbbá az érintett betegeket is értesíteni kell.

Az online világ miért késztet sok embert olyan viselkedésre, amit offline, a hétköznapi életben nem tanúsítana?

- ◯ Az internet világában könnyű névtelennek maradnunk, nem kell felfednünk valódi kilétünket.
- ◯ Számos fórumon „arctalanul", írásban kommunikálhatunk a többiekkel.
- ◯ Mivel az online világban nem mindig kapunk azonnali reakciót a megnyilvánulásainkra, könnyen gondolhatjuk azt, hogy kommentünknek vagy tweetünknek nincsenek következményei, nem gyakorolnak hatást másokra.
- ◯ A fenti tényezők mindegyike közrejátszik az online világ emberi gátlásokat csökkentő jellegének kialakulásában.

Továbbgondolandó kérdések:

- Hosszabb távon milyen hatásokat gyakorolhat az orvosi titoktartás kötelezettségére az, hogy az egészségügyben egyre nagyobb szerephez jut a digitalizáció?
- Milyen lehetséges következményekkel járhat az, hogy egyre nagyobb számban keletkeznek rólunk egészségügyi adatok, amelyeket digitalizált formában tárolnak, és amelyeket néhány pillanat alatt lényegében a világ bármely pontjára lehet továbbítani?
- Vannak, akik a gyors tudományos-technikai fejlődés kerékkötőjének vélik az adatvédelmi jogszabályokat, amelyek nélkül sokkal több és jobb minőségű egészségügyi adatot „taníthatnánk meg" például egy mesterséges intelligencia-alapú, okos algoritmusnak. A személyes adatok védelme valóban a tudományos fejlődés gátját jelenti?
- Akár laikusként, akár egészségügyi szakemberként használja az internetet, milyenek az Ön személyes tapasztalatai az online világ feltárulkozásra késztető hatásával kapcsolatban?
- Milyen elővigyázatossági szabályokat érdemes betartanunk akkor, amikor – akár laikusként, akár egészségügyi szakemberként – egészségügyi adatokat, információkat osztunk meg másokkal az online világban?