

Adatvédelem, adatbiztonság az egészségügyben

Ködmön József

Az orvos által ismert adatok tárolása, kezelése a szakma évszázados hagyományai alapján, az orvosi titoktartás szabályai szerint történik. Az orvos személyes felelőssége, hogy a megismert adatokat a betegek gyógyítása, egészségük megőrzése érdekében használják föl.

Az orvos-beteg kapcsolat természetesen nem egyszerű adatszolgáltató-adatkezelő kapcsolat, hanem annál sokkal több, teljes bizalomra épülő viszony, amelyben napjainkban egyre nagyobb szerepet kapnak az informatikai eszközök. Az egészségügyi adatok jelentős részének gyűjtése, tárolása, feldolgozása és értékelése az orvosi munka része. Éppen úgy szolgálja a megelőzést és gyógyítást, mint a diagnosztikai és terápiás tevékenységek.

Napjaink felgyorsult tudományos-technikai fejlődésére tekintettel már a gyógyító-megelőző munkában sem lehet kizárólag az évszázados hagyományokra szorítkozni. Az eddigi jól bevált gyakorlatot megtartva szükséges fölülvizsgálni, az európai normák szerint újragondolni a mai orvosi munka meglehetősen összetett problémáit. Különös figyelmet érdemelnek az informatikai eszközök, hiszen ezek egy új típusú szemléletet, szakértelmet igényelnek (1).

A legtöbb és legnagyobb gond az adatkezelés körül alakult ki. Napjainkban különösen fontos az egészségügyben keletkezett adatok védelme és biztonságos használata.

Az egészségügy különböző területein egyre elterjedtebbek a számítógépek, a hagyományos ügyviteli, adminisztrációs rendszereket számítógépes szoftverek helyettesítik. Ez a technikai váltás azonban még nem hozott egyértelmű javulást az adatvédelem, az adatbiztonság területén, csak újabb problémák merültek fel.

A hagyományos, papíralapú egészségügyi adminisztrációban különösebb szakértelem nélkül lehetséges a hozzáférés az érzékeny adatokhoz. A lázlapokon tárolt adatok minden látogató számára publikusak, az osztályirodák, orvosi szobák védelme sem megfelelő. A dokumentációs kényszer miatt a növekvő adathalmazok szinte kezelhetetlenné válnak, a hagyományos dokumentáció tárolása egyre költsé-

gesebb. Az archivált dokumentumok hatékony használata szinte teljesen lehetetlen, komoly gondokat okozhat egy-egy dokumentum elvesztése is. A hagyományos egészségügyi adminisztrációt mielőbb szükséges lenne informatikai alapokra helyezni, hiszen a jobb adatvédelem, a dokumentumok olcsóbb, hatékonyabb tárolása, az egész dokumentáció jobb kezelhetősége sokat javíthatna az egészségügy jelenlegi állapotán.

A számítógépen tárolt adatokhoz való hozzáférés az eddigiektől eltérő szakértelmet igényel. A módosítás vagy törlés tökéletesen, nyomtalanul elvégezhető, hacsak hatékony adatvédelmi rendszerbe nem ütközik a betolakodó. Ilyen azonban a jelenleg gyakori, többségében maximum jelszavas védelmet, esetleg kulcslemez használatát követelő, leginkább személyi számítógépes környezetben működő rendszerek esetében alig fordul elő.

Az egészségügy jelenlegi állapotában az egyszerű jelszavas, kulcslemez védelmi rendszerek elfogadhatóak, a hagyományos, papíralapú adminisztráció védelmi lehetőségeihez mérten előrelépést jelentenek. Ezen a területen nem az intelligens bűnözés a jellemző. Tudomásom szerint számítógépen tárolt egészségügyi adatokkal kapcsolatos bűncselekmény nem jutott bírósági szakaszig. Ez azonban nem jelenti azt, hogy ilyen jellegű esetek még nem fordultak elő. A számítógépes adatmanipulációk megakadályozására csak megfelelő informatikai alapú védelmi rendszerek használatával van esély.

Természetesen az informatikai eszközök használatának is vannak árnyoldalai. A hagyományos több köbméternyi dokumentáció egy-egy számítógépbe koncentrálódik. Apró gondatlanság, kicsi műszaki hiba igen nagy károkat képes okozni, különösen akkor, ha a számítógépes rendszert nem megfelelő szakértelemmel üzemeltetik. Találkoztam olyan adatvédelmi felelőssel, aki szerint az egyik kórházi osztály információs rendszerének legfontosabb adatvédelmi tényezője az, hogy csak néhány munkatárs ért a számítógép kezeléséhez.

A személyi számítógép a DOS operációs rendszer gyenge adatvédelmi funkciói miatt nem igazán alkalmas a megfelelő adatvédelem megvalósítására. A legtöbb

egész
rülhe
nélki
nyire
és d
állapi
jelen
Az
ezért
A vé
tonsá
de cs

Az

Az e
adatv
határ
funkc
védel
szóló
terüle
megh
alapv

A
irány
ügyi,
beruh
titokv
Az en
güek :

A l
zás. S
terüle
tervez
kezelé
formá

A n
maza.
lalkoz
matik.
ekkel
bályoz

- a
mok k
- az
- az
kötele

- az
jogai,
- a
szankc
Ebb
szerep
egyéb

egészségügyi rendszer védelme általában könnyen kike-
rülhető, az adatállományok direkt módon, nyom
nélkül manipulálhatók. Az ilyen rendszerben több-
nyire nem naplózhatók a változtatások, a rendszeridő
és dátum nem használható megbízhatóan, nem
állapítható meg egyértelműen, hogy ki, mikor és miért
jelentkezett be a rendszerbe.

Az egészségügyi adat és információ nagy érték,
ezért hatékony védelmére mindenképpen szükség van.
A védelemnek meg kell engedni a tárolt adatok biz-
tonságos felhasználását, feldolgozását, kiértékelését,
de csak az arra jogosultak számára (2).

Az adatvédelem szabályozási szintjei

Az első szinten a törvényi szabályozás áll. Ez az
adatvédelmi rendszer működésének általános elveit
határozza meg. Magyarországon ezt az általános
funkciót megvalósító törvény a személyes adatok
védelméről és a közérdekű adatok nyilvánosságáról
szóló 1992. évi LXIII. törvény. Az egészségügy
területén ehhez társul a 1972. évi II. törvény, amely
meghatározza az egészségügy működésére vonatkozó
alapvető rendelkezéseket.

A második szint a műszaki normák, szabványok,
irányelvek, rendeletek szintje. Ide tartoznak az építés-
ügyi, tűzvédelmi normák, szabványok és rendeletek; a
beruházásokra, az általános és speciális iratkezelésre, a
titokvédelemre vonatkozó jogszabályok és rendeletek.
Az európai egészségügyben meghatározó jelentősé-
gűek az Európa Tanács, valamint a WHO ajánlásai.

A harmadik szint az ágazati, tárcaszintű szabályo-
zás. Sajnos az egészségügyi ágazatban jelenleg ezen a
területen csak egy régen elfogadásra váró törvény-
tervezet létezik. Ez rögzíti az egészségügyi adatok
kezelésének alapfogalmait és az adatkezelés lehetséges
formáit.

A negyedik szint a helyi, intézményi szabályok hal-
maza. Minden egészségügyi adat kezelésével fog-
lalkozó intézménynek kellene készíteni egy „Infor-
matikai Biztonsági Szabályzatot”. Ebben – az előző-
ekkel egyeztetve – az alábbiakat lenne célszerű sza-
bályozni:

- a védelmet igénylő adatok, eszközök és objektu-
mok köre;
- az információs rendszer elemeinek védelme;
- az adatvédelmi felelős tevékenysége, jogai,
kötelezettségei;
- az adatokat kezelő személyzet tevékenysége,
jogai, kötelezettségei;
- a rendelkezéseket megszegők ellen alkalmazott
szankciók.

Ebben a szabályzatban tehát olyan intézkedések
szerepelnének, amelyek illeszkednek az intézmény
egyéb szabályzataihoz, és az informatikai rendszerre

irányuló veszélyeket, veszélyforrásokat elfogadható
mértékűre csökkentenék (3–4).

Mivel az adatvédelmi törvény a szabályozásnak csak
a kereteit adja meg, a helyi szabályozás nehezen készít-
hető el. Ez a nagymértékű szabályozatlanság igen ked-
vezőtlen hatást gyakorol a magyar egészségügyre.

Az adatvédelem megvalósításának szintjei

A fizikai védelem szintje a számítógépnek, közvetlen
környezetének és az adathordozóknak a védelmét
jelenti. A számítógépes helyiséget különféle beléptető
rendszerekkel és mozgás-, valamint hőérzékelő beren-
dezésekkel szokás védeni. A fokozott védelmi igényű
adatállományokról másolatot kell készíteni, és azokat
tűzbiztos pánccs szekrényben illik tárolni.

Az ügyviteli védelem az informatikai rendszert
üzemeltető szervezet ügymenetébe épített biztonsági
szabályok, tevékenységi formák együttese, amelyet az
Informatikai Biztonsági Szabályzat ír le. Az ügyviteli
védelem a fizikai védelemre épül, a teljes védelem egy
következő rétegét képezi. Míg a fizikai védelem a
rendszerbe való engedélyezett belépési pontokat jelöli
ki, addig az ügyviteli védelem a belépési pontok igény-
bevételének elfogadható, elvárt formáit rögzíti (3–4).

Az algoritmikus védelem azokból az eljárásokból
áll, amelyek a rendszer szolgáltatásaival egyidejűleg,
velük szorosan együttműködve látják el a védelmi
feladatokat. A magas szintű adatvédelem algoritmikus
eszközei a következők:

- az adatok titkosítása, rejtjelezés,
- partnerazonosítás, -hitelesítés,
- digitális aláírás és időpecsét,
- eseménynapló.

Ezek az eszközök eredményesen csak számítógépes
környezetben használhatók, mai fejlettségi szintjükön
elvéleg lehetővé teszik a papírmentes adminisztráció
megvalósítását.

Ha egy adatvédelmi rendszerben mindhárom
védelmi szint összehangoltan megvalósul, akkor azt
teljes védelmi rendszernek nevezzük (5).

Az egészségügy speciális védelmi követelményei

Az egészségügyi adat – azaz az érintett testi, lelki és
értelmi állapotára, kóros szenvedélyére és szexuális
szokásaira, valamint a megbetegedés körülményeire
vonatkozó adat (6) – a személyes adatokon belül a
különleges adat kategóriájába tartozik, melynek
kezelését csak az érintett vagy a törvény engedé-
lyezheti.

Az 1992. évi LXIII. törvény csupán az általános adatvédelem kereteit szabja meg, 10. szakasza szerint: „Az adatkezelő köteles gondoskodni az adatok biztonságáról, köteles továbbá megtenni azokat a technikai és szervezési intézkedéseket és kialakítani azokat az eljárási szabályokat, amelyek e törvény, valamint az egyéb adat- és titokvédelmi szabályok érvényre juttatásához szükségesek. Az adatokat védeni kell különösen a jogosulatlan hozzáférés, megváltoztatás, nyilvánosságra hozás vagy törlés, illetőleg a sérülés vagy megsemmisülés ellen.” Ennek alapján az egészségügyben kezelt különleges adatok kezelésére semmilyen konkrét adatvédelmi intézkedést nem lehet tenni, szükség lenne tehát megfelelően konkrét ágazati szabályozásra.

Az egészségügyi adatok védelmének fontosságát az Európa Tanács R(81)1. számú ajánlása is elismeri (7). A társadalombiztosítási célok érdekében használt személyes adatok védelmével pedig az R(86)1. számú ajánlás foglalkozik (8). Az adatkezelés és adatvédelem egy speciális részkerdését tárgyalja az írásos bizonyíték megkövetelésére vonatkozó jogszabályok harmonizációjáról és az iratmásolatok, illetve a számítástechnikai eszközökön rögzített adatok elfogadásáról szóló R(81)20. számú ajánlás (9). Ez előírja, hogy az ilyen típusú dokumentumoknak milyen biztonsági elvárásoknak kell eleget tenniük. Természetesen a magyar egészségügy számára is igen fontos lenne, hogy a számítógépen rögzített adatok, iratok az igazságszolgáltatási eljárás során bizonyítékként elfogadhatók legyenek.

Az Európai Közösségben működő egészségügyi információs rendszereknek az alábbi alapvető követelmények betartása ajánlott (7, 10):

- A lakosságról gyűjtött egészségügyi adatoknak és információs rendszereknek az egészségügyi szolgáltatás javulását kell szolgálnia.

- A társadalomnak minden működő információs rendszerről tudnia kell, továbbá biztosítani kell, hogy képviselői útján azok működését ellenőrizhesse.

- Az információs rendszerben létezni kell olyan eljárásoknak, amelyek biztosítják az adatok valódiságát, valamint lehetővé teszik az információk korrektt felhasználásának bizonyítását.

- Létezniük kell olyan garanciáknak, amelyek megátolják, hogy egy személy egészségügyi adatainak egyéb adataival való összekapcsolása, kiértékelése automatikusan vagy nagyrészt automatikusan történjen.

- Minden érintettnek biztosítani kell a lehetőséget, hogy a rá vonatkozó adatokat megismerhesse, a hibásakat kijavíthassa, függetlenül attól, hogy a feldolgozás manuális vagy automatikus.

- Bármilyen egészségügyi adatot csak egészségügyi alkalmazott változtathat meg.

- Az adatokhoz való hozzáférést előre definiált procedúrákhoz kell kötni, amelyeket törvény szabályoz.

- Az adatok harmadik személy részére való

átadását törvényes meghatalmazáshoz kell kötni.

- Az információs rendszerekben használt adatvédelmi technikáknak nem szabad rontani az egészségügyi szolgáltatások minőségén, sebességén vagy hatékonyságán; ha ez teljes mértékben nem valószínűsíthető meg, akkor optimális kompromisszumot kell találni a gazdaságosság és a biztonságosság között.

- Az egészségügyi szektorra vonatkozó speciális szabályokat nem az általános szabályok kivételeként kell kezelni, hanem további garanciákat adó önálló szabályokként.

Ezek az elképzelések ugyan több mint tízévesek, de talán érdemes végiggondolni alkalmazásukat a hazai viszonyokra.

Magyarországon az adatvédelem, adatbiztonság általános, keret jellegű szabályozása jónak mondható. Az egészségügyi ágazat adatkezelésére vonatkozó konkrét, a gyakorlatban használható magas szintű jogi szabályozás viszont nem került elfogadásra. Csak egy törvénytervezet létezik, amely a gyakorlat számára is megfelelően szabályozza az egészségügyben használt különleges adatok kezelését. Jó megoldás lenne, ha ezt a törvénytervezetet, valamint a szintén elkészült betegjogi kódexet beépítenék az egyébként is megújításra váró, többször módosított 1972. évi II. törvénybe, és egy egységes szerkezetű, az egészségügy működését komplex módon szabályozó törvényt fogadnának el. A hiányzó ágazati szintű szabályozás miatt a helyi, intézményi szabályozás a hazai egészségügyi intézmények jelentős részénél nem is létezik. Még több a gond a személyes és különleges adatok hatékony védelmével.

Ha európai szintű, az informatikai eszközöket hatékonyan alkalmazó egészségügyi ellátórendszert kívánunk működtetni, akkor az adatvédelem, adatbiztonság hiányosságait mielőbb pótolnunk kell. A legjobb megoldás talán egy intelligens memóriakártya alapú adminisztrációs rendszer bevezetése lenne. A viszonylag magas egyszeri bevezetési költségek elég hamar megtérülnének, hiszen a számos előnyös tulajdonság mellett jelentős költségmegtakarítást is el lehetne érni. Lehetővé válna a hagyományos, papíralapú adminisztrációs rendszer kiváltása egy korszerű, biztosítási kártyán alapuló, csaknem teljesen papírtmentes rendszerrel.

A papírtmentes adminisztráció megvalósítása az egészségügyben

Figyelembe véve a számítástechnikai, informatikai eszközök jelenlegi technikai színvonalát, talán nem könnyelműség kijelenteni, hogy az egészségügy intézményeiben elvileg lehetséges a biztonságos papírtmentes adminisztráció és kommunikáció megvalósítása. Ez természetesen nem azt jelenti, hogy

min
tosít
képe
igén
bete
szár

A.

léhe:

lizál

eljár

gozr

a nyi

az e

ciós

papí

egés

a m

prog

vizsg

mint

nek l

megc

A

haték

nyújt

nek.

Közö

Term

neses

IRO

1. Jáv

19

2. Ké

Bu

3. Di

NC

4. Vis

Bu

5. Ne

Ak

6. 13

ről.

7. Rec

me

Co

ii.
datvé-
egész-
vagy
való-
ot kell
ött.

eciális
leként
önálló

sek, de
hazai

tonság
dható.

tkozó
tű jogi

ak egy
nára is

asnált
ha ezt

észült
ént is

évi II.
szség-

rvényt
lyozás

egész-
étezik.

adatok

özöket
dszert

atbiz-
kell.

mória-
zetése

i költ-
zamos

mg-
nagyo-

váltása
em tel-

n

natikai
n nem

ségügy
aságos

meg-
hog

minden adat kizárólag mágneslemezen és a biztosítási kártyán szerepel, és csak a számítógépek képernyőjén nézhető meg. A beteg valószínűleg igényli az írásos kórházi zárójelentést, de például a betegforgalmi naplót feltehetőleg elegendő kizárólag a számítógép mágneslemezen tárolni.

Az egészségügyi eljárások papírmentessé tételéhez a hagyományos, papírhordozójú iratok digitalizált, mágnesesen tárolt változatainak hitelesítő eljárásait, a kriptográfiai protokollokat kell kidolgozni. A titkosítás, a digitális aláírás, az időpecsét és a nyilvános kulcsú adatkommunikáció felhasználása az egészségügy számítástechnikai és kommunikációs rendszereiben lehetővé teszi a majdnem teljesen papírmentes adminisztráció bevezetését. Minden egészségügyi tevékenységhez meg kell konstruálni a megfelelően biztonságos, hiteles számítógépes programmal kezelhető változatot. Meg kell például vizsgálni a háziorvos gyógyszerrendelésének, valamint a gyógyszertár gyógyszerkiadási tevékenységének biztosítási kártyával való biztonságos, hatékony megoldását.

A számítógépesített rendszernek legalább olyan hatékonyságot, adatbiztonságot és hitelességet kell nyújtania, mint a hagyományos, papíralapú rendszernek. Sőt elvárható, hogy megfeleljen az Európai Közösség korábban említett követelményeinek is. Természetesen meg kell teremteni a garanciáit a mágneses hordozón tárolt egészségügyi dokumentum

bizonyíték értékű elfogadásának az igazságügyi eljárásokban, hiszen enélkül aligha képzelhető el a papírmentes adminisztráció (11-12).

Következtetés

Az egészségügyi ellátórendszer által kezelt személyes, valamint különleges adatok védelme és biztonsága nem megfelelő. Különösen az adatvédelem gyakorlati megvalósítása működik rosszul, amelynek oka az ágazati szabályozatlanságban keresendő.

Nem nagy anyagi ráfordítással az adatvédelem, adatbiztonság problémái megoldhatók lennének, hiszen más területeken ezeket az ismert védelmi módszereket és eszközöket eredményesen használják.

A legjobb megoldás az említett komplex egészségügyi törvény megalkotása és egy jó technikai szintű biztosítási kártya bevezetése lenne. A megfelelő törvényi szabályozás biztosítaná az adatkezelés intézményi szintű szabályozásának kidolgozását, a jó minőségű biztosítási kártya pedig tovább erősítené az adatvédelmi funkciókat, továbbá megvalósítható lenne egy alacsonyabb költséggel működő, majdnem teljesen papírmentes egészségügyi adminisztrációs rendszer. Mindez természetesen egy, a betegek által is érezhető minőségi javulást eredményezne az egészségügyi szolgáltatásokban.

IRODALOM

1. Jávor A. Adatvédelem az egészségügyben. HISEC '94, Budapest, 1994. június 8-11. Budapest: NJSZT, 1994.
2. Kékes E, Kincses Gy, Várhelyi T. Egészségügyi informatika. Budapest: Springer Hungarica, 1993.
3. Dietz Gné, Pap M. Adatvédelem, adatbiztonság. Budapest: NOVORC, 1995.
4. Visnyei A, Vörös G. A számítógépes információbiztonság alapjai. Budapest: LSI Oktatóközpont, 1996.
5. Nemetz T, Vajda I. Algoritmikus adatvédelem. Budapest: Akadémiai Kiadó, 1991.
6. 13482. számú törvényjavaslat az egészségügyi adatok kezeléséről. Budapest: Népjóléti Minisztérium, 1994.
7. Recommendation No.R(81)1 on the regulations for automated medical data banks. Strasbourg: Committee of Ministers of the Council of Europe, 1981.
8. Recommendation No.R(86)1 on the protection of personal data used for social security purposes. Strasbourg: Committee of Ministers of the Council of Europe, 1986.
9. Recommendation No.R(81)20 on the harmonisation of laws relating to the requirement of written proof and to the admissibility of reproductions of documents and recordings on computers. Strasbourg: Committee of Ministers of the Council of Europe, 1981.
10. Study on New Technologies. A challenge to privacy protection? Strasbourg: Council of Europe, 1986.
11. Pernice A, Doare H, Rienhoff O. Healthcare Card Systems. Amsterdam: IOS Press, 1993.
12. Köhler C, Rienhoff O, Schaefer O. Health Cards '95. Amsterdam: IOS Press, 1995.