Információbiztonság az egészségügyben

Ködmön József dr., Csajbók Zoltán Ernő dr.
Debreceni Egyetem, Egészségügyi Kar
Egészségügyi Informatikai Tanszék, Nyíregyháza

Az orvos, az ápoló és a többi gyógyítással foglalkozó szakember egyre több időt tölt a számítógép előtt, használja a háziorvosi, szakellátási vagy integrált kórházi rendszereket. A gyógyító-betegellátó munka közben kezelt adatok nagyrészt a különleges adat kategóriába tartoznak, amelyek kezelésére szigorú szabályok vonatkoznak. A jogszabályok, rendeletek, szabályzatok és útmutatók dzsungelében nem könnyű eligazodni. Az ismerethiány azonban nem mentesít a felelősség alól. Jelen tanulmány a szakterülethez tartozó nemzetközi ajánlások, szabványok és jogszabályok legfontosabb tudnivalóit foglalja össze, majd pedig az egészségügyi adatok biztonságos és jogszerű kezelésének megvalósításához ad hasznos gyakorlati tanácsokat.

Kulcsszavak: orvosi informatika, információ védelem, adat védelem

Information security in health care

Doctors, nurses and other medical professionals are spending more and more time in front of a computer, using applications developed for general practitioners, specialized care, or perhaps an integrated hospital system. The data they handle during healing and patient care are mostly sensitive data – its management is strictly regulated. Finding our way in the jungle of laws, regulations and policies is not simple. Notwithstanding, our lack of information does not waive our responsibility. This study is summarizing the most important points of international recommendations, standards and legal regulations of the field, as well as giving practical advices for managing medical and patient data securely and in compliance with the current legal regulations.

Keywords: medical computer science, information protection, data protection

Az informatika eszközeinek egészségügyi alkalmazása gyógyító tényezővé vált. Kialakult az orvosi informatika, mint speciális terület, amely a gyógyítás nélkülözhetetlen eleme lett.

Célszerű megismerkedni az információbiztonság szabályozásával és megvalósításának lehetőségeivel, hiszen komoly gondok forrása lehet az egészségügyi adatok szakszerűtlen kezelése.

Az információbiztonság szabályozása

Az egészségügy működésének legfontosabb folyamatai a valid adatokra és az általuk hordozott meghatározó jelentőségű információra épülnek.

Egy egészségügyi intézmény számára nagy kockázatot jelent, ha bármilyen zavar keletkezik ezeknek az információknak a minőségével, mennyiségével, pontosságával vagy elérhetőségével kapcsolatban. Az adatok sértetlenségének, bizalmasságának és rendelkezésre állásának biztosítása, a sérülések és az adatvesztés elkerülése kritikus fontosságú.

A megoldást kizárólag egy olyan sokrétű szabályozás adhatja, ami a kockázatokkal arányos anyagi ráfordítással megvalósítható életszerű intézkedéseket és tevékenységi formákat tartalmaz.

Az információbiztonsági szabályozás struktúrája hierarchikus jellegű. Meghatározó jelentőségűek az egyes nemzetek jogszabályai, amelyekre azonban erőteljesen hatnak a nemzetközi szervezetek ajánlásai és irányelvei is.

Ajánlások, irányelvek és szabványok

A szabályozás első szintjét a nemzetközi szervezetek ajánlásai, iránymutatásai alkotják, de erre a szintre tartoznak a különféle kapcsolódó területek szabványai és normatívái is.

Valamennyi nemzetközi dokumentum közös jellemzője, hogy igyekszik biztosítani az egyensúlyt a személyes adatok védelme és az információ szabad nemzetközi áramlása között. Igyekszik megvalósítani, hogy az összes személyes adat magas szintű védelmet élvezzen, és a nemzeti törvényalkotás minimális követelményként kezelje az ajánlásokat.

Meghatározó jelentőségű az Európa Tanács Adatvédelmi Egyezménye [1], amelyet Magyarországon a [2] törvény hirdetett ki.

Hasonló fontosságú az Európai Parlament és a Tanács irányelve [3] a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

Kimondottan az egészségügyi szektorra vonatkozik az Európa Tanács ajánlása [4], ami megadja az egészségügyi adatkezeléssel kapcsolatos alapelveket.

Erős, de igen nehezen megvalósítható törekvés az Európai Unióban az információbiztonsági jogharmonizáció. Az Európai Bizottság 2012 elejére előkészített egy adatvédelmi szabályozás-tervezetet [5], melynek célja az európai adatvédelmi szabályok átfogó reformja, egységesebb, egyszerűbb és korszerűbb szabályozása. A tervezett rendelet, mint jogforrás - a korábbi irányelvtől eltérő módon - közvetlenül hatályosulna a tagállamokban, ami a tényleges, azonnali és feltétlen jogharmonizációt garantálná. Egyelőre még nem került sor az elfogadására.

Létezik még egy OECD irányelv [6] is a magánélet védelméről és a személyes adatok határokon átívelő áramlásáról, amit Magyarország is elfogadott.

A Magyar Szabványügyi Testület által is kiadott információbiztonsági szabvány [7] naprakész irányítási eszközt kínál az adatok és információk védelmére, az azokkal összefüggő folyamatok menedzsmentjére, a lehetséges veszélyek azonosítására és elkerülésére, továbbá az informatikai rendszer védelmének folyamatos fejlesztésére.

A működési sajátosságokat figyelembe véve - a vállalatirányítási szempontú ISO 9001 tanúsítás mellé - célszerű megvalósítani az egészségügyi intézmények információbiztonság-irányítási rendszerének a [7] szabvány szerinti tanúsítást is [8].

A [9] magyar szabvány a [10] európai szabvány hazai változata. Ez az egészségügyi szereplők elektronikus kommunikációjához szükséges közös referencia adatmodellt adja meg. Az üzenetszabványok (e-Kórlap, e-Konzílium, e-Lelet, e-Recept és e-Finanszírozás) egyelőre nem kerültek elfogadásra, csak előszabvány formában léteznek. A közös adatmodell és az üzenetszabványok kialakítása figyelembe veszi az adatvédelemmel kapcsolatos elvárásokat is.

A Közigazgatási Informatikai Bizottság 2008-ban kiadta 25. számú ajánlássorozatát Magyar Informatikai Biztonsági Ajánlások (MIBA) címmel. Ennek legfontosabb részét képezi a Magyar Informatikai Biztonsági Irányítási Keretrendszer (MIBIK), amely a [10], [11] és [12] nemzetközi szabványokon, valamint az irányadó EU és NATO szabályozáson alapul. Ezek a dokumentumok is tartalmaznak hasznos információkat az Informatikai Biztonság Irányítási Rendszer (IBIR) egészségügyi alkalmazásáról is.

Az említetteken kívül számos további nemzetközi szabvány és ajánlás is létezik, amelyek elsősorban az elektronikus egészségügyi megoldások adatvédelmének részleteivel foglalkoznak.

Hazai jogi szabályozás

Egy általános és egy ágazati törvény alkotja a vonatkozó jogszabályok legfontosabb részét. A [13] törvény a személyes adatok védelmét, valamint a közérdekű adatok megismeréséhez való jog érvényesülését szolgáló alapvető, általános szabályokról szól.

Az egészségügyi ágazatra pedig a [14] törvény vonatkozik, ami meghatározza többek között az egészségi állapotra vonatkozó különleges adatok és az azokhoz kapcsolódó személyes adatok kezelésének feltételeit és céljait.

A [13] törvény - az 1992-es elődjéhez képest - jelentős változásokat tartalmaz, amit az is jelez, hogy a napi szóhasználatban a korábbi adatvédelmi törvény kifejezés helyette az infótörvény elnevezést szokás rá alkalmazni.

Az alapelv az, hogy a polgár autonóm személy, akinek döntési és cselekvési joga van a róla szóló információk felett. Ezt csak törvény korlátozhatja, ahogyan a közérdekű adatok megismerését is. Mindkét szabály egyértelműen túlmutat a korábbi gyakorlaton, és nem tesz különbséget a hagyományos és számítógépes adatkezelés, valamint a közjogi és magánjogi alkalmazások között.

Az adatkezelés legfontosabb alapelve továbbra is a célhoz kötöttség, ahogyan az a korábbi szabályozásban is szerepelt.

Egy lényeges konkrét változás például, hogy az adatvédelmi ombudsman hivatala helyett a Nemzeti Adatvédelmi és Információszabadság Hatóság (NAIH) működik, hatósági jogkörrel. A folytonosság és stabilitás megőrzése érdekében elnökét kilenc évre nevezik ki.

Az infótörvény az összes adatkezelési terület közös szabályait tartalmazza, így keret jellegűnek tekinthető.

Az ágazati szabályozás az utóbbi években nem sokat változott, néhány helyen az általános szabályozás elvei szerint módosították, illetve átalakítottak egyes adatkezeléssel kapcsolatos szabályokat.

Például a kezelést végző orvos jogosult áttekinteni az OEP adatbázisában, hogy az általa ellátott biztosítottak mikor, hol és milyen típusú egészségügyi ellátásokat vettek igénybe. Ezt azonban az érintett írásban megtilthatja.

Hasonlóan szabályozott a gyógyszerbiztonsági validálás, melynek során a beteg megtilthatja a gyógyszerésznek, hogy megnézze korábbi gyógyszerelésének legfontosabb adatait.

Helyi, intézményi szabályozás

A szabályozásnak ez a szintje szokott a legtöbb gondot okozni mind az adatkezelőnek, mind pedig az érintettnek. Gyakran az egészségügy szereplői is azt gondolják, hogy megfelelő szabályozást adnak a törvények és rendeletek, ezekhez fölösleges intézményi szabályzatokat illeszteni.

A törvények és rendeletek általi szabályozásnak azonban nem lehet célja az apró részletek kidolgozása, illetve az egyes tevékenységek és területek személyes felelőseinek meghatározása.

Mindenképpen szükséges a változásokat, folyamatokat követni képes helyi szabályok megalkotása. Ezek tudják csak megfelelő módon meghatározni a védelmi rendszer hatékony intézkedéseit, amelyek folyamatosan alkalmazkodnak a megváltozott körülményekhez, követik az informatikai rendszer fejlődését.

Minden 20 főnél több adatkezelőt foglalkoztató egészségügyi intézménynek meg kell alkotnia a [14] törvény által előírt saját adatvédelmi szabályzatát, ami a releváns magasabb szintű jogi szabályozáson túl figyelembe veszi a [7] szabvány szerinti tanúsítás lehetőségét is [8].

A kötelezően alkalmazandó belső adatvédelmi felelős mellett hasznos lehet külső adatvédelmi felelős alkalmazása is. Így az ellenőrzés és auditálás függetlensége garantálhatja a magasabb szintű informatikai biztonságot.

Az információbiztonság megvalósítása

Az információbiztonság csak akkor lehet elfogadható szintű, ha megfelel az előzőekben tárgyalt szabályozás kritériumainak.

A védelmi rendszer kialakítása során könnyen előfordulhat, hogy valamelyik elemét túlhangsúlyozzuk, ugyanakkor pedig egy másik fontos részt egészen elhanyagolunk.

Például mágneskártyával nyíló földszinti gyógyszerszoba rácsnélküli ablakát éjszakára nyitva hagyni nyilvánvalóan súlyos hiba. Sajnos azonban az informatikai rendszerek védelmi anomáliái legtöbbször nem ilyen látványosak, de az emberi gyengeségeknek, hibáknak az információbiztonság megvalósítása területén is kulcsszerepük van.

Nyilvánvaló, de mégis fontos hangsúlyozni, hogy az informatikai biztonság csak a fizikai, az ügyviteli és az algoritmusos védelem megfelelő együttes alkalmazásával érhető el.

Fizikai védelem

Egy informatikai rendszer fizikai védelmét a hardver és szoftver elemek, ezek között különösen a számítógépek, a hálózati elemek, a nyomtatók, az adathordozók, dokumentumok és dokumentációk, valamint ezek közvetlen környezetének fizikai hatások elleni védelmét jelenti. Ez a klasszikusnak számító feladat bizonyos helyiségek, térrészek általános fizikai hozzáférés-védelmére egyszerűsíthető le.

Az egészségügy intézményei viszonylag jó megoldásokat alkalmaznak a fizikai védelem megvalósítására, hiszen ez erősen összefügg a vagyonvédelem megoldásával is.

Könnyen előfordulhat, hogy egy számítógépen dolgozó orvosnak hirtelen más tennivalója lesz, és ott marad az informatikai rendszer az ő bejelentkezésével, lehetővé téve másoknak az orvos megszemélyesítését. Ekkor a jó fizikai védelem és a későbbiekben tárgyalt további védelmi lehetőségek enyhíthetik a problémát.

Ügyviteli védelem

Az ügyviteli védelem az informatikai rendszert üzemeltető szervezet ügymenetébe épített védelmi intézkedések, biztonsági szabályok, tevékenységi formák együttese.

A védelemnek ezt a területét szokták adminisztratív védelemnek is nevezni. Míg a fizikai védelem a rendszerbe való engedélyezett belépési pontokat jelöli ki, addig az ügyviteli védelem a belépési pontok igénybevételének elfogadható, elvárt formáit rögzíti. Az ügyviteli védelem mintegy összekapcsolja a fizikai és algoritmusos védelem eszközrendszerét, ezzel valósítva meg az informatikai biztonság teljességét.

Az egyes szervezetek gyakran elkövetik azt a hibát, hogy a hagyományos, papír alapú ügyviteli rendszerekre kidolgozott biztonsági intézkedéseket változtatás nélkül próbálják alkalmazni az informatikai eszközökkel támogatott adminisztrációs rendszerekre. Ez a szemlélet súlyos biztonsági hibák forrása lehet. A hagyományos ügyvitel egy statikus, lassan változó rendszer, az informatikai rendszerek azonban igen dinamikusan fejlődnek, biztonságos használatuk

csak a változásokat megfelelő ütemben követő, szintén dinamikusan változó helyi szabályok megalkotásával lehetséges.

Az informatikai biztonság megvalósításának ez a szintje áll legközelebb a különféle szervezetek életéhez, ezért ennek kell megoldania a védelem részletes, dinamikusan változó szabályozását. A törvényhozás képtelen követni az informatikai rendszerek gyors fejlődését, ezért az ezen a szinten elkövetett hibák az egész szervezetre nézve súlyos következményekkel járhatnak. A megfelelő szabályzatok körültekintő, gondos elkészítése a szervezet elemi érdeke.

Algoritmusos védelem

Ez a védelmi szint azokból az eljárásokból, protokollokból áll, amelyek a rendszer szolgáltatásaival egyidejűleg, velük szorosan együttműködve látják el a védelmi feladatokat. Gyakran az informatikai biztonság megteremtésének egyetlen eszközeként tartják számon. Ez a szemlélet azonban erősen eltúlozza az algoritmusos védelem jelentőségét.

Az információ algoritmusos módszerekkel történő védelméhez kapcsolódó tudományterületet kriptográfiának nevezzük, ezért használatosak a kriptográfiai védelem vagy a logikai védelem kifejezések is. Annak ellenére, hogy ennek a védelmi szintnek külön tudományterülete van, sohasem szabad megfeledkezni arról, hogy a kriptográfia eszközrendszere csak megfelelő fizikai és ügyviteli védelemmel ellátott környezetben képes a hatékony működésre.

Az algoritmusos védelem sarkalatos pontja a felhasználó azonosítás, ami leggyakrabban a felhasználó névhez tartozó jelszó megadásával történik.

A jelszó

Digitális életünk legfontosabb és legértékesebb szereplői a különböző informatikai rendszerekben használt jelszavaink.

A jelszó működésének meghatározó eleme az úgynevezett egyirányú függvény. Egy ilyen *f* függvénynél az *x* értékből a *h=f(x)* függvényértéket - amit lenyomatnak nevezünk - könnyű meghatározni, de megfordítva a *h* lenyomatból az *x* kiszámítása csaknem lehetetlen.

A jelszó feltörését nehezítő további megoldás az úgynevezett salt alkalmazása, ami egy véletlen módon megadott hosszú számsor. Minden felhasználóhoz egyedileg határozza meg a számítógépes rendszer.

Ha a felhasználók jelszavaiból képzett számok rendre $x_1, x_2, x_3, \ldots$, akkor a megfelelő lenyomat érték kiszámítása

$$h_i = f(x_i + s_i), \text{ ahol } i = 1,2, \ldots$$

képlettel történik, ahol f az egyirányú függvény, az s_i és a h_i a felhasználóhoz rendelt salt illetve lenyomat érték.

A számítógépes rendszer minden felhasználóhoz elkészíti az 1. táblázat egy sorát.

felhasználó név	lenyomat	salt
Aladár	h_1	s_1
Béla	h_2	s_2
Cecil	h_3	s_3
. . .	. . .	...

1. táblázat A jelszavak tárolt adatai

Látható, hogy maga a jelszó (*x* érték) nincs tárolva a rendszerben, ezért az elfelejtett jelszót sehogyan sem lehet innen megszerezni, nyilvánvalóan a rendszergazda sem tudja azt.
A felhasználó által belépéskor megadott jelszó ellenőrzése a fenti táblázatban tárolt adatok alapján történik. A rendszer kikeresi az adott felhasználó névhez tartozó salt értéket, elvégzi a fenti képlet szerinti számítást a megadott jelszóval (*x* érték). Ha az így kapott lenyomat (h érték) és a táblázatban tárolt lenyomat érték megegyezik, a jelszó helyes.
Egy jelszó elfogadhatóan biztonságosnak tekinthető, ha legalább 8 karaktert tartalmaz, amik között szerepel kisbetű, nagybetű, szám és egyéb jel. Fontos még az is, hogy ne legyen értelmes, azaz szótárban megtalálható szavakat ne tartalmazzon. Kerülendő a felhasználóhoz tartozó keresztnevek, évszámok, autórendszámok és hasonlók alkalmazása. Ékezetes betűk és speciális, a billentyűzeten nem szereplő karakterek használata nem ajánlatos.

Az interneten található sok olyan alkalmazás, például [15], ami a jelszó erősségét méri. Ezek azonban általában csak formálisan mérnek, nem tudják meghatározni a jelszó értelmes elemeit. A "Zoli1955" jelszót erősnek minősítik, annak ellenére, hogy egy keresztnevet és egy születési évszámot tartalmaz.
Kézenfekvő a kérdés: Hogyan lehet megjegyezni egy elegendően hosszú, de értelmes részt nem tartalmazó jelszót?

Az alábbi módszer viszonylag jól használható jelszó előállítására és megjegyzésére.

1. Válasszunk egy könnyen felidézhető memoritert, amely egy általunk jól ismert versrészlet, közmondás, dalszöveg, idegen nyelvű szövegrészlet vagy más hasonló szöveg.

2. A kiválasztott szövegrészlet első betűi alkotják a jelszó egyik részét.

3. Ehhez hozzáteszünk néhány számot és írásjelet, ügyelve arra, hogy értelmes részek ne keletkezzenek.

Például, ha a választott memoriter a "Góg és Magóg fia vagyok én." verssor, akkor a jelszó lehet például: **GeMfve753+**. Az elől szereplő betűk a verssor szavainak ékezet nélküli kezdőbetűi, az utána szereplő számok a numerikus billentyűzet egyik átlójában vannak, a + jel pedig a 3-as szám fölött szerepel a fő billentyűzeten. Így tehát memoritert és klaviatúra logikát használva viszonylag könnyen fölidézhetünk egy egyébként megjegyezhetetlennek tűnő jelszót.

Ugyanazt a jelszót nem célszerű több alkalmazáshoz használni, ezért általában több jelszót kell megjegyeznünk. Ehhez használhatunk különféle memoritereket és klaviatúra logikákat, de félő, hogy összekeverjük ezeket.

Több jelszó megjegyzéséhez jól használható egy alkalmasan megválasztott könyv. Egy oldalról négy jelszó nyerhető, felhasználva a szövegmező sarkait, ahonnan a szöveget függőleges irányban fentről lefelé illetve lentről felfelé hat karakter hosszan ékezetek nélkül kiolvassuk. Az első betűt nagybetűvé alakítjuk, hozzáírunk néhány számot és egyéb jelet, klaviatúra logika szerint.

Ha a jelszót hetente kell változtatni a hét sorszámával megegyező könyvoldalt kell választani. A módszer nyilvánvalóan csak akkor használható jól, ha mások által nem zavarva, külön irodában van lehetőségünk dolgozni, a jelszót a mindig rendelkezésre álló könyv alkalmazásával megadni.

Több jelszó kezeléséhez jobb megoldás lehet egy jelszó menedzser szoftver alkalmazása. Egy ilyen rendszer erősen védett adatbázisban, "széfben" tárolja az egyes alkalmazásokhoz tartozó felhasználónév jelszó párokat.

Az adatbázist master jelszó is védi, amit semmilyen más alkalmazásban nem használunk, és például a memoriteres módszerrel tudunk felidézni. Az ilyen szoftverek erőssége, hogy nagyon biztonságos, szinte tökéletes jelszavakat generálnak, és a felhasználónév jelszó párok adatbázisát szinkronizálják különféle eszközökre, így bármilyen környezetben alkalmazhatók.

Komoly hátrányuk viszont, hogy a master jelszó elvesztése vagy bármilyen kompromittálódása esetén az összes alkalmazás rendelkezésre állása veszélybe kerül.

Nagyon körültekintően kell kiválasztani a jelszómenedzsert, mert sok - akár fizetős - szoftver található az interneten, aminek eredete bizonytalan, ezért használata jelentős biztonsági kockázattal jár. Elsősorban ismert forráskódú, szabad szoftvereket célszerű választani, amik általában ingyenesek is. Ilyen például a Password Safe [16] szoftver, ami magyar nyelven is rendelkezésre áll, és Bruce Schneier [17], neves biztonsági szakember tervezte.

Ezt a jelszó menedzsert kétfázisú felhasználó azonosítással is lehet használni, ami a "valamivel rendelkezik és valamit tud" elvet alkalmazza. Ebben a rendszerben a "valamivel rendelkezik" egy úgynevezett token, a "valamit tud" pedig a master jelszó. A token általában egy USB csatlakozóba helyezett speciális eszköz, ami a felhasználó személyes felügyelete alatt van. Ilyen látható a 1. ábrán.

1. ábra Kulcscsomóra felfűzött token csatlakoztatása a számítógéphez

A Password Safe rendszerbe történő bejelentkezés a token USB portra csatlakoztatásával és a master jelszó megadásával történik.

Amennyiben az egészségügy szereplői már rendelkeznek intelligens kártyával, a token lehet maga az ellátásban közreműködő kártyája.

Az intelligens kártyák bevezetésére az OEP már 2006-ban elindított egy pilot projektet [18], a legutóbbi egészségügyi informatikai fejlesztési tervek pedig az állampolgári kártya egészségügyi alkalmazását szorgalmazzák [19], [20].

Mindaddig, míg nem kerül bevezetésre intelligens kártya az egészségügyben, érdemes alkalmazni egy jól megválasztott jelszó menedzsert.

Az egészségügyben dolgozó rendszergazdák, informatikusok és felső vezetők számára ajánlott a jelszómenedzser használata USB csatlakozóra helyezhető tokennel. Ez megfelelő biztonságot ad az általuk használt rendszerekre vonatkozóan.

Az ellátást végző orvosoknak, ápolóknak, adminisztrátoroknak és más hasonló felhasználóknak elegendő a jelszómenedzser alkalmazása, token nélkül.

A master jelszó felidézéséhez pedig érdemes használni a memoriter módszert és a klaviatúra logikát.

Hasznos lehet a master jelszavakat tűzbiztos páncélszekrényben, lezárt borítékban őrizni. Nem várt események bekövetkezésénél - különösen szükséghelyzet vagy katasztrófa esetén - gondoskodni kell a jelszavak és tokenek megfelelően dokumentált, szabályszerű átadásáról.

A jelszó használat megerősítésének egészségügyben is használható, könnyen bevezethető és olcsó alternatívája lehet a mobilaláírás alkalmazása [21]. Ebben a rendszerben a bejelentkezés

a felhasználó név és a jelszó megadása után a felhasználó mobiltelefonjára, SMS-ben kapott számsor beírásával történik. A módszert eredményesen alkalmazzák a bankok is az interneten működő elektronikus pénzügyi tranzakciók biztonságának fokozására.

Ez a bejelentkezési megoldás egy speciális kétfázisú felhasználó azonosítás, amelyben a token a mobiltelefon. Ennek a költséghatékony módszernek a bevezetése jelentősen javítaná az egészségügyi adatkezelés biztonságát, és ezáltal az ellátás színvonalát.

IRODALOM

[1] Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe, Strasbourg, 1981

[2] Act VI of 1998 for the protection of individuals with regard to automatic processing of personal data, the promulgation of the Convention, dated Strasbourg the 28th day of January 1981 [1998. évi VI. törvény az egyének védelméről a személyes adatok gépi feldolgozása során, Strasbourgban, 1981. január 28. napján kelt Egyezmény kihirdetéséről] [Hungarian]

[3] Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Strasbourg, 1995

[4] Recommendation No. R (97) 5 on the Protection of Medical Data, Council of Europe, Committee of Ministers, Strasbourg, 1997

[5] COM (2012) 11: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Strasbourg, 2012

[6] The Recommendation of the OECD Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013

[7] MSZ ISO/IEC 27001:2014 Information technology. Security techniques. Information security management systems. Requirements

[8] *Guba, T., Lampé, Zs. T.,:* Information security aspects at a county hospital - system configuration and certification experiences [Információbiztonsági kérdések egy megyei kórházban - rendszer kiépítési és tanúsítási tapasztalatok], IME, 2013, 12(7), 16-19. [Hungarian]

[9] MSZ 22800:2008 Health informatics. Reference Information Model [Egészségügyi informatika. Közös adatmodell] [Hungarian]

[10] BS EN 13606-1:2007 Health informatics. Electronic health record communication. Reference model

[11] BS ISO/IEC 27002:2013 Information technology. Security techniques. Code of practice for information security controls

[12] BS ISO/IEC 27005:2011 Information technology. Security techniques. Information security risk management

[13] Act CXII of 2011 on information self-determination and freedom of information [2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról] [Hungarian]

[14] Act XLVII of 1997 on processing and protection of the health care and related personal data [1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről] [Hungarian]

[15] The Password Meter. http://www.passwordmeter.com. Accessed: 25.03.2015.

[16] Password Safe. http://www.passwordsafe.sourceforge.net. Accessed: 25.03.2015.

[17] Schneier on Security. http://www.schneier.com. Accessed: 25.03.2015.
[18] *Király, Gy*.: Modernization projects in the public health insurance system [Az egészségbiztosítás közigazgatási rendszerének korszerűsítési projektjei], IME, 2006, 5(2) 40-42. [Hungarian]
[19] Digital Renewal Action Plan 2010 - 2014 [Digitális megújulás cselekvési terv 2010 - 2014], Nemzeti Fejlesztési Minisztérium, 2013. [Hungarian]
[20] National ICT Strategy 2014 - 2020 [Nemzeti infokommunikációs stratégia 2014 - 2020], Nemzeti Fejlesztési Minisztérium, 2014. [Hungarian]
[21] *Ködmön, J., Bodnár, K.*: Safer user authentication in health care [Biztonságosabb felhasználó azonosítás az egészségügyben], IME, 2007, 6(9) 46-51. [Hungarian]