Dr. HORVÁTH ZSOLT – FÁBIÁN ZOLTÁN

Információbiztonság lépésről lépésre az egészségügyben

Az egészségügyi intézmények számára egyre nagyobb problémát jelent adataik megfelelő védelme, az adatkezelés folyamatosságának biztosítása. A fenyegetettségek nagyon sokoldalúak és összetettek. Magukban foglalják a kórházi informatikai rendszerek működtetésének megbízhatósági és biztonsági problémáit, a betegdokumentáció kezelésének problémáit, valamint az információszivárgás veszélyeit is.

Az INFOBIZ Kft. kialakított az egészségügyi intézmények számára egy többlépcsős programot, amelyben az információbiztonsági irányítási rendszer kiépítése több, egymást követő és egymásra épülő önálló lépésben valósul meg. Az egyes lépések önálló projektekként is végrehajthatók, azok beruházásigénye így kisebb, és önmagában kézzelfogható és biztonságot tovább javító eredményeket produkálnak.

Ennek a többlépcsős programnak az első lépcsőjét vezette be a Szegedi Tudományegyetem Szent-Györgyi Albert Klinikai Központja. Jelen tanulmány ennek a bevezetésnek a lépéseit és eredményeit mutatja be.

Információbiztonság az egészségügyben – miről is beszélünk?

Az információbiztonság jelentősége a gazdaság minden területének minden szervezete számára megkérdőjelezhetetlen, függetlenül attól, hogy a szervezet tudomást vesz-e róla vagy sem. Minden gazdálkodó szervezet, legyen kicsi vagy nagy, tartozzon az állami vagy versenyszférához, hatékony működését folyamatalapon tudja megszervezni. Folyamatai megbízható működtetéséhez elengedhetetlen, hogy folyamatai erőforrásait menedzselje. A legfontosabb erőforrások közé tartozik maga az ember, a pénzügyi eszközök, a kapcsolódó infrastruktúra (ingatlan, berendezések, eszközök stb.), no és maga az információ.

Semelyik folyamat nem működhet a bemenő (input) és kimenő (output) információk rendelkezésre állása és pontossága (sértetlensége) nélkül. Ha ezek az információk ugyanakkor illetéktelenek tudomására jutnak, akkor azzal visszaélve számos kárt tehetnek a szervezetnek.

Összegezve: az információk biztonsága nem jelent mást, mint az adott (felhasznált illetve kezelt) információk bizalmasságának, sértetlenségének és rendelkezésre állásának biztosítását. Információbiztonsági irányítási rendszerről akkor beszélünk, amikor az információk biztonságát folyamatosan és kockázatalapon, a vállalatvezetési (irányítási) rendszer keretein belül – megfelelve a PDCA ciklus alapelvének – menedzseljük.

Nincs ez másképpen az egészségügyben sem. Az egészségügyi gyógyító szervezetek (kórházak, klinikák, szakrendelők stb.) működése számára is ugyanolyan jelentőséggel bírnak a szervezeti és a szakmai (azaz a főtevékenységet ellátó) működéshez szükséges információk biztonsága.

Ezek az információk jellemzően a következő nagyobb csoportokra (kategóriákra) oszthatók:

- **betegek** egészségügyi és személyes adatai;
- **egészségügyi dolgozók**, beszállítók adatai;
- **gyógyszerek, vizsgálati eszközök és eljárások** adatai;
- **minőségirányítási dokumentációk** és kapcsolódó gyűjtött indikátorok;
- **kórházi gazdasági / finanszírozási / ügyviteli** adatok.

Az információbiztonsági irányítási rendszer az információknak (mint adatoknak) a védelmét szolgálja különböző fenyegetésekkel szemben, és ezáltal biztosítja a védendő információk bizalmasságát, rendelkezésre állását és sértetlenségét. Ha ilyen szemmel nézzük, akkor melyek lehetnek a jellemző fenyegetések az egészségügyben, amelyekkel szemben az adatokat védeni kell:

- **Adatszivárgás** – jogosulatlanok hozzáférése az adatokhoz. Illetékteleneknek (szándékosan vagy véletlenül) kiadott betegadatokkal számtalan visszaélés lehetséges, ezekre rengeteg példa hozható. A betegek személyes és egészségügyi adatainak bizalmasságát külön jogszabályok is védik. De ugyanúgy veszélyes lehet a kórházi dolgozók személyes adatainak (pl. név, cím, TAJ-kártya adatok, bankszámlaszám, bérek), a gyógykezelési eljárásoknak vagy kutatási adatoknak, gépek, műszerek, eszközök aktuális adatainak, vagy éppen a kórház stratégiai terveinek vagy gazdálkodási adatainak nyilvánosságra kerülése vagy illetéktelenek általi velük való visszaélése is.
- **Adatok hibás felhasználása** – hibás információk a gyógyításban, menedzsmentben. Erre tipikus példák lehetnek: az „elnézett vagy elcserélt" vizsgálati eredmények (vagy kórlapok) alapján hozott döntések a kezelésről, vagy a gondatlanul rögzített adatok alapján készült hibás betegdokumentációk vagy a gondatlanul rögzített vagy szándékosan „kozmetikázott" adatok alapján készült finanszírozási adatszolgáltatás, a hamis adatokra épülő ellátástervezés.
- **„Nem az előírt célnak megfelelő" adatkezelés** – adatok illetéktelen célú felhasználása. Példaként gondoljunk itt a szakdolgozatokban, tudományos munkákban nem megfelelően kezelt adatok közzétételére, vagy bizonyos kezelési adatok gyógyszercégek piaci versenyelőnyéhez történő egyoldalú kiszolgáltatására.
- **Adatok rendelkezésre állásának hiánya** – diagnosztikához, beavatkozáshoz, gyógyításhoz nem, vagy késve (vagy hibásan) állnak rendelkezésre a szükséges információk. Jellemző informatikai fenyegetettség, amikor a központi informatikai rendszerben lévő (rövid vagy hosszú) üzemszünet miatt a gyógyításhoz szükséges információk nem elérhetők (ld. a közelmúltban a sajtóban is közzétett egyhetes rendszer-leállás a PTE ÁOK-n). Az adatok, információk rendelkezésre állásának hiányát okozhatják nemcsak az informatikai rendszer hiányosságai, de a papíralapú betegdokumentációk kezelésének problémái is.

Ezekből a példákból látható, hogy az információbiztonság hiánya miatti lehetséges problémák az egészségügyi gyógyító szervezetek mindennapi működésében mindenütt fellépnek és felléphetnek, és súlyos gyógyítási, jogi és működtetési problémákat okozhatnak.

E problémák gyakorlati felismerése után határozta el magát a Szegedi Tudományegyetemen a Szent-Györgyi Albert Klinikai Központ vezetése a megoldás keresésére. Olyan megoldást kellett találni, amely a jelen gazdasági viszonyok mellett nem jelent túl nagy pénzügyi terhet, és amelynek bevezetése a munkatársak számára egyszerű és átlátható, azaz a mindennapi munkavégzésük mellett különösebb megterhelés nélkül megtanulható, alkalmazható. Másrészről pedig csak olyan hatékony megoldás jöhet szóba, amely nem a formális, adminisztrációs terheket növeli, hanem érdemben növeli a biztonságot, és az adatvédelmen túl érdemben növeli a teljes információbiztonságot.

Ennek tükrében jött létre az együttműködés a Szent-Györgyi Albert Klinikai Központ és az INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. között.

Az INFOBIZ Kft. megoldása egészségügyi gyógyító intézmények (kórházak) számára

Az egészségügyi gyógyító intézmények működtetése során a fenti információbiztonsági problémák kielégítő kezelése lényegében egy testre szabott információbiztonsági irányítási rendszer bevezetésével biztosítható.

Az INFOBIZ Kft. figyelembe véve az egészségügy helyzetét, működési jellegzetességeit és speciális információbiztonsági problémáit, **kialakított egy többlépcsős programot az információbiztonsági irányítási rendszer kiépítésére és bevezetésére**. Az egyik alapelve – elsősorban a terhelések mérséklése végett – **a fokozatosság elve** volt. A komplett információbiztonsági irányítási rendszer kiépítése több, egymást követő és egymásra épülő önálló lépésben valósul meg. Az egyes lépések önálló projektekként önállóan is végrehajthatók, azok beruházásigénye kisebb. Az egyes lépések végrehajtása lépésenként önálló, a biztonságot tovább javító eredményeket produkál – az eredményekhez viszonyított olcsó áron.

1. lépés: Biztonságtudatosságot fejlesztő bevezető képzések, önértékelő kérdőíves felmérés és kiértékelése, valamint intézkedési javaslatok a statisztikailag feltárt problémák javítására.

2. lépés: Az egész szervezetet lefedő, szakértői informatikai és információbiztonsági állapotfelmérés, az eredmények értékelése erősségek és gyenge pontok feltárásával, és intézkedési javaslatok a feltárt problémák javítására.

3. lépés: Az adatvagyon, az információs vagyon és fenyegetettségeinek, kockázatainak felmérése, értékelése, és intézkedési javaslatok a nem elfogadható mértékű információbiztonsági kockázatok kezelésére.

4. lépés: A folyamatos kockázatkezelésen alapuló információbiztonsági intézkedések beemelése a szervezet integrált irányítási rendszerébe, és ezzel az információbiztonsági irányítási rendszer (mint a vállalati integrált irányítási rendszer egy részrendszere) életbe léptetése.

A Szent-Györgyi Albert Klinikai Központ elkezdte ennek a programnak a végrehajtását, és a továbbiakban bemutatjuk az első lépés végrehajtásának főbb pontjait, eredményeit és tapasztalatait.

A program első lépésének végrehajtása a Szent-Györgyi Albert Klinikai Központban

A program első részében az INFOBIZ kft. szakértői egy félnapos képzést tartottak a klinika jelen lévő adatvédelmi felelősei és középvezetői számára. Ezután átadták az önértékelések kérdőíveit, amelyeket a klinikán belül – a végrehajtásra hosszabb időt hagyva – feldolgoztunk, és az eredményeket elküldtük az INFOBIZ Kft. szakértőinek. Az eredményeket az INFOBIZ Kft. egy jelentésbe foglalta össze, amely az eredmények és az azokból következő összefüggések leírása után javaslatokat is tartalmazott a problémás területeken az információbiztonság erősítésére.

Az információbiztonsági bevezető képzés

A bevezető információbiztonsági témájú képzés célja egyrészt ismeretfrissítés és az információbiztonsági tudatosság erősítése az adatvédelmi felelősök és a középvezetők számára, másrészt a figyelem felhívása az információbiztonság és informatikai üzemeltetés hatásának jelentőségére a klinika működési és adatbiztonságára és az ezzel kapcsolatos személyi felelősségre.

Ennek megfelelően a képzés főbb témái a következők voltak:

- Gyakorlati példák, esettanulmányok megtörtént, ún. „csapdás" esetekről, előre nem számított negatív eseményekről és ezek tapasztalatainak bemutatása a betegek adatvédelmével kapcsolatban.
- Az információbiztonság főbb területeinek, szerepének és jelentőségének bemutatása egészségügyi szolgáltató szervezetek működésében.
- A kórházi információtechnológiai (IT) adatvédelem főbb gyakorlati szempontjainak bemutatása.
- Az informatikai üzemeltetés, mint a szolgáltatás megbízhatósága elvárásainak, kritériumainak és jellemző mutatóinak bemutatása.

Az önértékelés

Az önértékelés két, egymástól elkülönített részből állt. Az egyik része egy általános célú kérdőív, amely az információbiztonság és az adatvédelem gyakorlatának és tudatosságának felmérésére szolgál. Az önértékelés másik része a klinikai központ informatikai hálózatának és működtetésének kulcs-elemeit és jellemző informatikai védelmi profilját jellemzi. A kétféle kiértékelést a következő táblázat hasonlítja össze.

	Általános célú	Informatikai célú
Célja	A teljes szervezetben az adatvédelem felhasználói gyakorlatának és tudatosságának felmérése.	Az informatikai rendszer fenyegetettségi és védelmi profiljának felmérése.
Módszere	27 kérdésből álló, egyszerű feleletválasztós teszt alapú, az intraneten keresztül kitölthető elektronikus kérdőív[1].	8 – 10 oldalas kérdőív, az informatikai és az informatikai biztonsági rendszer kulcselemeivel.
Résztvevők köre	Minél szélesebb körben, minden betegellátó és adminisztratív egységből több dolgozó.	Szervezet informatikai vezetése.
Kiértékelés módja	IT alapú statisztikai kiértékelés, majd az eredmények alapján a kimutatható gyenge pontok.	Szakértői verbális kiértékelés a kulcselemekre adott válaszok és összefüggéseik alapján.

[1] Ez a kérdőív elektronikus formában meghatározott ideig az intézményi Intraneten volt elérhető. Jellemzői: strukturáltság, azaz főcsoportok és azon belül szempontok, anonimitás, a kérdések értelmezéséhez „help" lehetőség, a lezárás utáni azonnali statisztika, ami a feldolgozás aktualitását biztosítja

Az **általános célú önértékelés témái** felölelik az egyes betegellátó és adminisztratív szervezeti egységek mindennapi gyakorlatában, egységenként a következő témaköröket:

- a papíralapú dokumentációk biztonságos és bizalmas kezelése,
- az adatvédelmi szabályok és előírások megléte, ismerete és betartása,
- az informatikai biztonsági szabályozások megléte, ismerete és betartása.

Az **informatikai célú önértékelés témái** felölelik az informatikai infrastruktúra, az alkalmazások, az üzemeltetés, a felhasználói állomány és a működési környezet kereteinek, működésének jellemzését, valamint ezek tükrében az üzemeltetés meglévő védelmi elemeinek jellemzését.

A program első lépésének eredményei a Szent-Györgyi Albert Klinikai Központban

Az információbiztonságot tudatosító képzést nagy érdeklődés előzte meg, és azon nagyszámú hallgatóság vett részt. A prezentációkat számos kérdés követte, majd a képzés után az adatvédelem és az információbiztonság sokáig téma volt. Jellemzően sokan vették elő a „régóta porosodó" IBSZ-t, és olvasták el újra, ami mindenképp nyomatékot adott a téma iránti általános odafigyelésnek.

Az önértékelő kérdőívek kitöltés során az eredményeket az INFOBIZ Kft. szakértői kiértékelték, és egy részletes jelentésben foglalták össze.

Az általános célú kérdőív eredményei:

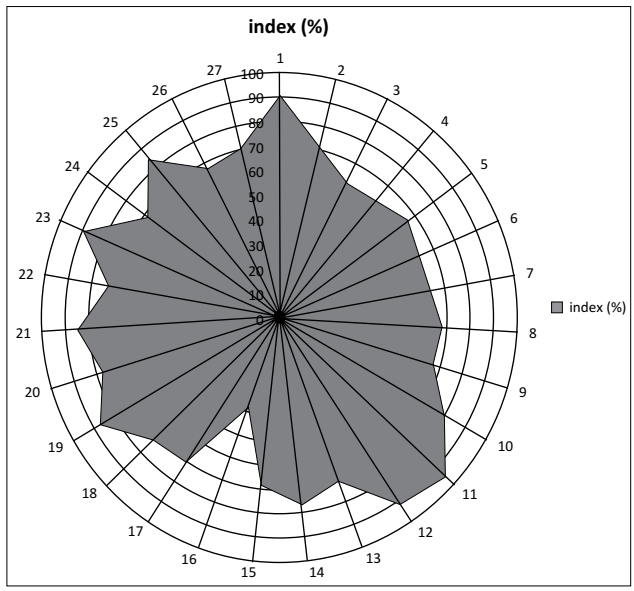
A kérdőívek kitöltésének eredményeit – noha sok érdekes hasznosítható tapasztalatot mutatnak, és sok tendenciára és tanulságra felhívják a figyelmet – csak tendencia-jelleggel szabad értékelni, és ezek nem helyettesítik egy részletes felmérés eredményeit.

A Szent-Györgyi Albert Klinikai Központban a felmérésen összesen kilenc szervezeti egység (klinikák, laborok, ill. intézetek) vett részt.

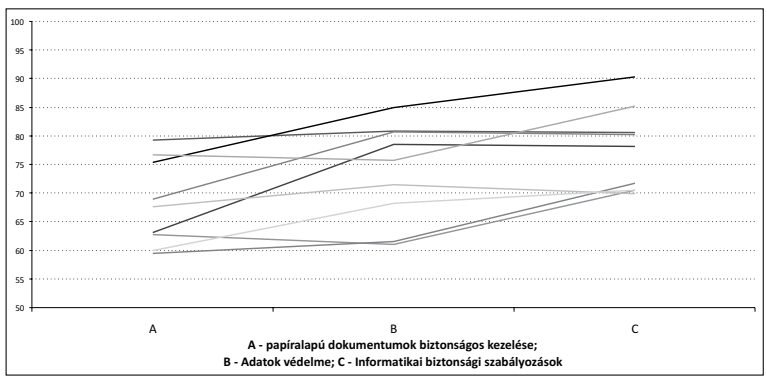
Az eredmények grafikus szemléltetése mellett a tendenciák kiértékelése verbálisan történt. Az értékelés kitért mind az egyes témakörök helyzetének elemzésére, mind a szervezeti egységek szerinti elemzésre. A jelentés bemutatta az általános célú kérdőív kérdésenkénti összesített eredményeit mind a vizsgált szervezeti egységekre vonatkoztatva külön-külön, mind a teljes intézményre összesítve is.

Az egyes klinikák közötti eredmények is (a 9 vizsgált klinika / intézet vonatkozásában) jelentősen eltérnek egymástól. Az egyes részterületek értékelésében, illetve az egyes kérdések megítélésében a különbségek még ennél is nagyobbak. Ez önmagában is utal az egyes klinikák közötti eltérő adat- és információbiztonsághoz való viszonyulásra és gyakorlatra.

Az egyes szervezeti egységek illetve az egész intézmény vonatkozásában a 27 kérdés eredményeinek átlaga szemléletesen egy kördiagramon (radar diagramon) ábrázolható (1. ábra). Az egyes vizsgált szervezeti egységeken belül a 3 témacsoport eredményeinek szemléltetése vonaldiagramos ábrázolással történt (példa a 2. ábrán).



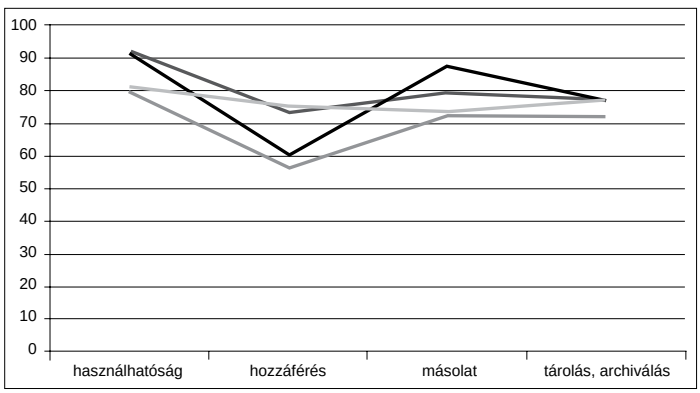
1. ábra: A 27 kérdés eredményeinek összevetése kördiagramon



2. ábra: A három témacsoport eredményeinek összevetése a kilenc résztvevő szervezeti egységnél

A kérdéssor úgy épült fel, hogy a három témacsoporton belül önálló, gyakorlati témakörök különülnek el. Egy témakört egy vagy jellemzően több egymásra épülő kérdés együttesen jellemez, és ezek nagyon jól kimutatják annak a témakörnek a mindennapi gyakorlati működését.

Az egyes témacsoportokon belüli témakörök értékelése külön-külön is kimutatott (lásd példát a 3. ábrán), amely már konkrétan rámutat szervezeti egységenként a vélhető erősségekre és fejlesztendő területekre is. Látható az ábrán, hogy a legnagyobb hiányok a papíralapú betegdokumentációk hozzáférési biztonságából adódnak, azaz a betegdokumentációk kezelésének gyakorlata több helyen könnyen lehetővé teszi az illetéktelen hozzáférést.



3. ábra: A papíralapú dokumentumok biztonságos kezelése témacsoport témaköri eredményeinek összevetése 4 szervezeti egységnél

Az informatikai önértékelési kérdőív eredményei:

A kapott eredmények – mint általában az önértékelések eredményei – figyelemfelhívó jellegűek, rámutatnak lehetséges kritikus helyekre, azonban a részletek pontos megismerése, feltárása végett nem helyettesítik egy átfogó IT / IT biztonsági felülvizsgálat (audit) elvégzését.

A kérdőív négy területen kérdez rá az üzemeltetés és az üzleti felhasználás kulcselemeire (fenyegetettségi profil), és ugyanezeken a területeken az alkalmazott biztonsági szabályok, módszerek illetve eszközök alkalmazására (védelmi profil). Ezek aránya, illetve az egyes témák szükségessége illetve hiánya megmutatja a rendszer lehetséges gyenge pontjait, fejlesztendő területeit.

Az informatikai biztonság szempontjából értékelt négy terület a következő:

- Informatikai (IT) infrastruktúra biztonsága
- Informatikai alkalmazások biztonsága
- Informatika (IT) üzemeltetésének biztonsága
- Humán erőforrások biztonsága

Az értékelés erre a négy területre külön-külön mutatta be az intézményi informatikai rendszer átfogó jellemzését, fenyegetettségi és védelmi profilját és a biztonság szempontjából az erős és a fejlesztendő területeit.

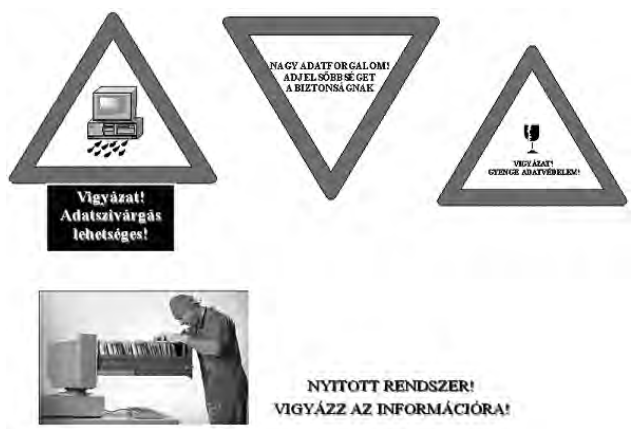
Továbbiakban nagyon jó kiindulási információkat adott ez a felmérés egy későbbi részletes informatikai / informatikai biztonsági felmérés megtervezéséhez és lefolytatásához.

Az eredmények hasznosítása

Az elkészített jelentés a klinika vezetősége számára szemléletesen bemutatta és felhívta a figyelmet az információbiztonság állapotára, főbb hiányosságaira és azok veszélyeire. Ezek eredménye nyomán több intézkedés született:

- Átfogó belső adatvédelmi és információbiztonsági tudatosítási program bevezetése,
- Konkrét, információbiztonságot javító intézkedések szervezése és informatikai intézkedések kezdeményezése,
- Az információbiztonsági irányítási rendszer 2. szakaszának (lépcsőjének) előkészítése.

Az információbiztonsági tudatosítási program keretein belül igyekeztünk új ötletekkel biztosítani az adatvédelemmel kapcsolatos érdeklődést. Ennek egyik példája a biztonság tudatosítását szemléltető KRESZ-tábla jellegű figyelmeztető táblák készítését célzó ötlet. A 4. ábrán bemutatunk néhányat a legjobban sikerültek közül.



4. ábra: Figyelmeztető táblák

Természetesen ezek nem jelentenek előrelépést az információbiztonság javítása tekintetében, de talán alkalmasak arra, hogy a klinikákon egyrészt biztosítsák az érdeklődést az információk biztonságával kapcsolatban, másrészt talán segítenek a jelenlegi meglévő biztonsági színvonal fenntartásában.

Ugyanakkor konkrét lépéseket is tettünk: a bevezető információbiztonsági témájú képzés hatására, és a kiértékelés alapján elkészült egy Adatvédelmi tájékoztató, amely a Klinikai Központ intranet rendszerében valamennyi betegellátó számára folyamatosan elérhető. Segít az adatvédelmi alapismeretek elsajátításában, és ugyanakkor azok gyakorlati alkalmazásában is. Kialakítása révén könnyen elérhetők az adott témához kapcsolódó jogszabályi paragrafusok, vagy az Adatvédelmi Eljárási Rend vonatkozó rendelkezései.

Az elektronikus információáramlás biztonságosabbá tétele érdekében kialakított központosított levelező rendszer tervezésekor és kivitelezésekor tekintettel voltunk a képzésen elhangzott, az önértékelésben és annak kiértékelésében szereplő információbiztonsági alapelvekre. Ennek megfelelően az új levelező rendszer megvalósítja a biztonságot a fizikai rendelkezésre állás, a védett, de ugyanakkor kiterjesztett hozzáférhetőség tekintetében is.

Amit sikerült elérnünk:

- Szemponttá vált az adatbiztonság – nemcsak a vezetés, de a klinikai munkatársak számára is.
- Megerősítettük az adatvédelmi felelősi hálózatunkat: javítottuk a tudatosságot, fejlesztettük ismereteiket az információbiztonsági rendszerünkről.

Persze ez nem sok, de az egészségügy jelenlegi viszonyai között talán nem is kevés...

Szerzők:

Dr. Horváth Zsolt, INFOBIZ Informatikai, Információbiztonsági és Vezetési Tanácsadó Kft. (INFOBIZ Kft.), ügyvezető igazgató,
horvathzs@infobiz.hu

Fábián Zoltán, Szegedi Tudományegyetem Szent-Györgyi Albert Klinikai Központ,
minőségirányítási igazgató,
fabian.zoltan@med.u-szeged.hu