Információbiztonsági kérdések egy megyei kórházban – rendszerkiépítési és tanúsítási tapasztalatok

Guba Tamás, Dr. Lampé Zsolt Tibor
Kenézy Gyula Kórház- és Rendelőintézet, Debrecen

Murphy szerint: „Ami elromolhat, az el is romlik". Az igazi kérdés, hogy megengedhetjük-e magunknak, hogy megvárjuk az incidens bekövetkezését. Egy váratlan hiba megjelenése akkor és ott káoszt okoz, kezelése gyors, logikus és egyértelmű döntéseket igényel. Tudnunk kell azonban, hogy a stresszhelyzetben hozott döntések alacsonyabb hatékonyságúak, mint a normál környezetben hozottak. Ugyanakkor a bekövetkezett kár mértéke, a hiba keletkezése és elhárítása között eltelt idő függvényében exponenciálisan növekszik. A kár, egy kórház esetében, akár emberéletet is jelenthet. Ezt természetesen egyetlen egészségügyi intézmény sem tekintheti elfogadható kockázatnak.

According to Murphy: "If anything can go wrong, it will." The real question is whether we can allow ourselves to wait until the incident happens. An unexpected failure can result in an instantaneous chaos that requires logical and direct decision making. We have to know however, that decisions made in stressful situations are less efficient than decisions made under normal circumstances. At the same time the extent of damage exponentially grows as a function of time between the occurrence of the failure and the remedy of the event. In the case of a hospital, a failure can result even in the loss of life. Naturally there is no healthcare institution that can take this as an acceptable risk.

BEVEZETÉS

Miközben az országban az egészségügyi intézmények „átalakítása" folyik, a Kenézy Gyula Kórház- és Rendelőintézet vezetősége merész lépésre szánta el magát. A szerzők bemutatják az MSZ ISO/IEC 27001:2006 információbiztonsági szabványnak megfelelő rendszer bevezetésének folyamatát, az ennek során szerzett tapasztalatokat, mintaként más intézmények felé. A szabvány és a kiépített rendszer mérete nem teszi lehetővé valamennyi bekezdés elemzését, ezért a szerzők csak a legjellemzőbb, esetenként átgondolásra okot adó momentumokat ragadták ki.

ÚT A TANÚSÍTÁSIG

2013 márciusában zajlott a Kenézy kórház. MSZ ISO/IEC 27001:2006 információbiztonsági szabvány (továbbiakban: IBIR) szerinti tanúsítása. Szinte napra pontosan egy évvel korábban született meg a kórház felső vezetésének körében az elhatározás, hogy az immár hagyományosnak számító, 2000 óta működő ISO 9001-es (köztudottan vállalatirányítási szempontú) tanúsítás mellett szükség van egy olyan eszközre, amellyel fel tudjuk mérni a napi működést fenyegető kockázati tényezőket, és fel tudunk készülni azok minimalizálására, elhárítására. Mivel az IBIR alapvetően kockázatelemzési szabvány, ezért hamar világossá vált a vezetőség számára, hogy szükségünk van erre a rendszerre.

A kórház az IBIR szabvány szempontjából szerencsés és kettős helyzetben volt. Szerencsés, mert:

- rendelkezésére állt egy több mint 10 éve működő, kiforrott minőségirányítási rendszer (mögötte egy kis létszámú, de annál hatékonyabb csapattal), amihez az IBIR-t hozzá lehetett illeszteni;
- rendelkezésére állt olyan munkatárs, aki korábban már több cégnél vezette be és üzemeltette az ennek a szabványnak megfelelő kockázatelemzési rendszert;
- az „átalakulás" kapcsán páratlan lehetősége adódott arra, hogy a kórház a hagyományokon alapuló, kőbe vésett jellegű szabályokat felülvizsgálja, átírja.

Kettős, mert az intézmény működési sajátosságaiból adódóan, a bevezetés és a tanúsítás ideje alatt, a kórháznak csak a betegellátásra kellett összpontosítania, valamennyi kiszolgáló tevékenységet az egyik tagvállalat, a „háttérszolgáltató" látta el. Ugyanakkor a tanúsítás idején még küszöbön állt az „átalakulás", áprilistól már ezek a szervezeti egységek is a kórház színeiben működtek – vagyis a dokumentációt és magát a rendszert már erre az állapotra kellett felkészíteni.

A dokumentációs rendszer kiépítése nem okozott különleges kihívást. Az MSZ ISO/IEC 27001:2006 azon kevés szabványok egyike, amelyiknek egyik fejezete (4.3.1) tételesen és részletesen felsorolja, hogy milyen kézikönyvre, szabályzatokra, eljárásokra, utasításokra van szükség. Ezek bevezetése, majd oktatása megtörtént. A kórház MIR felelősei külön oktatásban részesültek, számítva a belső auditokon való részvételre. Az idő szűkössége és a szabvány specialitásai miatt valamennyi belső auditot az IBIR felelős végezte el, a gyógyító oldalon saját készítésű kérdésjegyzéket, a kiszolgáló egységeknél a szabvány „A melléklet"-et használva. A belső auditok során néhány, a 9001-es auditokból megszokott téma mellett, a következő pontok elemzése történt meg:

- az adott osztály, a hozzá tartozó járóbeteg-munkahelyek és egyéb helyiségek (öltözök, irattárak, raktárak) elhelyezkedése;
- a fent meghatározott épületek, épületrészek, helyiségek megközelíthetősége, a bejutási pontok osztályozása;

- az adott szakma információ leállító/feldolgozó/tároló/továbbító eszközökkel való ellátottsága, azok és a rajtuk tárolt információ elhelyezkedése és hozzáférhetősége;
- kiemelten a papír alapú betegdokumentáció (beleértve a receptek) tárolása és hozzáférhetősége használat előtt/alatt/után.

A tanúsítás az ISO 9001-es auditokhoz hasonló menetrend szerint zajlott.

A TANÚSÍTÁS TANULSÁGAI – A RENDSZER TOVÁBBFEJLESZTÉSE

Az auditor távozásával azonban a feladatok nem érnek véget, sőt, az igazi munka most következik. A bevezetés során ugyanis a felkészítő igyekezett a szabványt a mindennapi munkához igazítani, azonban be kell látni, hogy ez nem lehetséges minden esetben, mivel helyenként a kórház működését kell a szabvány követelményeinek megfelelően módosítani.

(Az alábbi fejezetcímek megegyeznek a szabvány főbb bekezdéseinek címével, azonban nem részletezik valamennyit.)

BIZTONSÁGI SZABÁLYZAT

A stresszhelyzetekben hozott alacsony hatékonyságú döntések elkerülése érdekében össze kell gyűjteni az intézményt érintő/érinthető kockázati tényezőket, azokat rangsorolni/osztályozni kell. Ilyen osztályozási szempontok lehetnek:

- „tudok róla, de nem foglalkozom vele – elhanyagolhatónak tekintem";
- „tudok róla, és meg fogom szüntetni a következményt";
- „tudok róla, és meg fogom szüntetni az okot";
- „tudok róla és azonnal, teljes körűen beavatkozom".

A kockázati elemzést ki kell terjeszteni a kórház valamennyi folyamatára. Ennek megvalósításában nagy előnyt jelent a már működő ISO 9001-es rendszer, hiszen annak keretében már kidolgozott folyamatleírásokkal rendelkezünk.

A feltárt kockázatra – amennyiben az nem az első kategóriába kerül besorolásra – vészforgatókönyvet kell kidolgozni (szorosan együttműködve az érintett szervezeti egységgel), majd azokat rendszerezni és rendszeresen felülvizsgálni, illetve tesztelni kell.

Egy egyszerű példa a lázmérés. Ebben a tevékenységben a következő kockázati tényezők fogalmazhatók meg. (A felvetések időnként mosolyra adhatnak okot, de ugyanakkor elgondolkodtatóak is.)

- Rendelkezésre áll-e a szükséges eszköz? (van-e lázmérő az osztályon?)
- Megfelelő minőségű-e a szükséges eszköz? (működőképes-e a meglévő lázmérő?)
- Az eszköz meghibásodása esetén áll-e rendelkezésre olyan eszköz, amivel ugyanezt a mérést el tudom végezni? (van-e tartalék lázmérő az osztályon?)
- Az eszközt használó munkaerő kapott-e megfelelő képzést az eszközhasználatra? (tudja-e az ápoló, hogyan kell használni a lázmérőt?)
- Hibás mérési eredmény esetén a munkaerő képes-e felismerni a vészhelyzetet? (az ápoló rájön-e, hogy a lázmérő hibás értéket mutat? Ha igen, meg tudja-e ítélni, hogy a lázmérő hibájából, vagy a beteg együttműködésének hiányából keletkezett a hibás érték?)
- A vizsgálati eredmény mikor (az információ keletkezésétől számítva mennyi időn belül) és hogyan kerül rögzítésre? (Az ápoló rögtön beírja a lázlapra, a dekurzus lapra, rögzíti a medikai rendszerbe, esetleg megpróbálja megjegyezni, amíg visszamegy a nővérpulthoz és a kórlaptartóból előkeresi a megfelelő bizonylatot?)
- Hogyan tárolom a vizsgálati eredményt? (akár papíron, akár elektronikusan; mennyire hozzáférhető az arra jogosultaknak, vagy az illetéktelenek számára)

Ezzel rá is világítottunk az IBIR-rel kapcsolatos leggyakoribb tévedésre: ugyanis az információ-biztonság alaposan túlmutat az informatikai biztonságon.

Az információbiztonság szervezete

Egy ekkora intézménynél a működőképes IBIR üzemben tartásához a jelenlegi felállás nem elégséges. A bevezetést az IBIR felelős végezte, szükség esetén a jogászok, informatikusok, a MIR osztály és a kórház MIR felelőseinek együttműködését kérve.

Azonban a rendszer működésének biztosításához létre kell hozni egy munkacsoportot, amelynek állandó és ideiglenes tagjai is vannak. Állandó tagok az IBIR vezető(k), az ideiglenes tagok az osztályokon dolgozó IBIR felelősök és IBIR auditorok. Az állandó tagoknak a rendszer fejlesztése, karbantartása az elsődleges állandó feladatuk; az ideiglenes (megfelelő képzettséggel rendelkező) munkatársak a MIR-hez hasonlóan csak meghatározott időszakokban vesznek részt a folyamatokban, ugyanakkor ők azok, akikhez a szervezeti egységek dolgozói elsődlegesen fordulhatnak.

Az IBIR vezetőnek megfelelő hatáskörrel is kell rendelkeznie. Amennyiben új információ-bevitelre/feldolgozásra/tárolásra/továbbításra használatos eszközt akar beszerezni a kórház; az informatikai, gazdasági, orvosszakmai jóváhagyás mellett szükséges az IBIR jóváhagyása is: ne kerüljön be olyan eszköz, amit nem lehet a rendszerbe illeszteni.

Közvetetten tartozik a kórház szervezetéhez, de nem szabad figyelmen kívül hagyni az „illetékes hatóság" és a „különleges érdekcsoport" fogalmát.

A szabvány előírásainak megfelelően meg kell határozni, hogy egy kórház esetében kit kell

- illetékes hatóságnak (pl. NAV, tűzoltóság, rendőrség, katasztrófavédelem, OEP, OTH, GYEMSZI, önkormányzat), vagy
- különleges érdekcsoportnak (pl. tulajdonosi kör, vevők (azaz egy kórház esetében a betegek, esetenként azok

közeli hozzátartozói, gondnokai), a megrendelők, az elsővonalbeli beszállítók, a lakókörnyezet, a szakmai kollégiumok, oktatási intézmények és a környező alap-és szakellátással foglalkozó intézmények) tartani.

Meg kell határozni, hogy milyen kockázati tényezőt jelent a kórház számára a fenti hatóságok és csoportok nem megfelelő működése, együttműködése, rendelkezésre állása.

Vagyontárgyak kezelése

Teljes körű értékleltárt kell készíteni (ami nem egyezik meg a gazdasági rendszerből előállítható vagyonleltárral! – összesíteni kell, hogy milyen „értékekkel" (a szabvány értelmében milyen információ előállító, tároló, feldolgozó és továbbító eszközökkel) rendelkezik a kórház; ennek megfelelően nem csak az IT berendezéseket kell a leltárba bevenni. Tisztában kell lenni azzal, hogy a szabvány értelmében ilyen jellegű eszközök például:

- diagnosztikai eszközök (pl. lázmérő, EKG-készülék, valamennyi képalkotó diagnosztikai eszköz)
- terápiás eszközök információ-előállító/megjelenítő egységei (pl. terheléses EKG-készülék szobakerékpárjának monitora és nyomtatója)
- nővérhívó rendszer (a kórteremben lévő nyomógombtól az ajtó felett és a nővérpultban felvillanó lámpákig)
- betegmonitor rendszerek (pl. sürgősségi, vagy posztoperatív kórtermek beteg-állapot figyelő eszközei)
- őrző-védő céllal elhelyezett monitorok és a felvétel tárolására alkalmas berendezések
- tűzjelző rendszerek.

Az emberi erőforrások biztonsága (az alkalmazást megelőzően, az alkalmazás ideje alatt és megszűnése, illetve megváltozása esetén)

A munkaerő felvétel és az elbocsátás, minden jól működő cég jól kidolgozott folyamata, azonban annak ellenőrzése általában teljes mértékben elhanyagolt.

A munkaerő felvétele az álláshirdetéssel kezdődik. Megoldást kell találni a pályáztatás során jelentkező általános problémára – a kórház meghirdet egy álláshelyet, és jelen körülmények között, az elbírálást követően nincs joga megtartani (pontosítok: meg kell semmisítenie) a beérkezett önéletrajzokat/pályázatokat (vagyis a nyertesét sem teheti be annak személyi anyagába).

Valamilyen formában tudatosítani/elfogadtatni/aláíratni, tulajdonképpen engedélyeztetni kell a pályázóval, hogy a kórház még bizonyos ideig felhasználhatja az önéletrajzot/pályázatot (hozzájárulási nyilatkozat). Ez a probléma nem vonatkozik a munkát kereső személy által behozott, önkéntesen leadott önéletrajzokra. (Bár, ebben az esetben a kórháznak érdemes azt igazolnia, hogy a jelentkező részéről önkéntes átadás történt.)

IBIR szempontból a próbaidős dolgozó kiemelt kockázati tényező. Az ok egyszerű: a hatályos jogszabályok értelmében bármikor távozhat. Az új dolgozók esetében tehát érdemes megfontolni, hogy a belépő dolgozó rögtön teljes, vagy csak korlátozott hozzáférést kapjon a munkájához szükséges informatikai rendszerekhez. Az új dolgozók oktatását, mely a kórházban központosított formában zajlik, érdemes kiegészíteni nevesített információbiztonsági képzéssel – a későbbi számonkérhetőség miatt. A két pont összevonásához vezetői döntés szükséges, amíg az új dolgozó nem kapta meg a fent említett „új-dolgozó képzést", addig ne kapjon jogosultságot a későbbiekben általa használt rendszer(ek)hez.

Miért tartják be a dolgozók a kórházon belüli „játékszabályokat"? Mert másnap is be akarnak jönni a munkahelyükre. De mi a helyzet azokkal, akik már nem akarnak bejönni? IBIR szempontból kedvezőbb a helyzet, ha felmondanak a munkavállalónak, de így is jelentős a kockázat. Az elmenő dolgozó esetében a kritikus időszak nem a bejelentéssel, hanem a vezetői döntés meghozatalával kell hogy kezdődjön.

Ahogy megtörtént a bejelentés, attól kezdve már nem várható el a dolgozótól, hogy betartsa a „játékszabályokat". Védelmi szempontból kedvezőbb, ha a döntés meghozatalát követő legrövidebb időn belül elkezdődik a jogszabályi kereteknek megfelelő hozzáférés-korlátozás, e-mail és hálózati megfigyelés. A folyamatban kritikus pont, hogy az elmenő dolgozóról általában csak a kiköröző lap körbevitele/aláíratása során (vagyis a bevett szokás szerint az utolsó munkában töltött napon) szereznek tudomást az intézmény érintett szervezeti egységei (pl. az informatika) – a kórház szempontjából kedvezőbb, ha már a döntés meghozatalakor értesülnek.

A fenti helyzet súlyosabb formája az önként távozó dolgozó, hiszen ott nem lehet megbecsülni sem, hogy pontosan mikor született meg az elhatározás. Ilyenkor a megoldás esetleg a visszamenőleges hálózati megfigyelés, a naplófájlok elemzése lehet. Bevett gyakorlat a kilépő dolgozó e-mailjeinek kezelésére, hogy az utolsó munkában töltött napot követő 6 hónapig a munkahelyi vezető postafiókjába történik az átirányítás. Ezzel adatvesztést kerülhetünk el, illetve valóban lezárásra kerülhetnek az elbocsátott dolgozó által kezelt folyamatok.

Kiemelt kockázatú alvállalkozók a takarító és az őrzésvédelmet ellátó cég. Ezek azok a külsős dolgozók, akik a napi tevékenységük során rendszeresen találkoznak / találkozhatnak adatokkal. Érdemes szervezett oktatást tartani a számukra az általános és a helyi IBIR szabályokról (amit akár vizsgával és egy általunk kiadott „oklevéllel" is zárhatunk), aminek a megtörténte után számon kérhető az alvállalkozón az esetleges incidens. Emellett természetesen elengedhetetlen a szerződések felülvizsgálata: a feladatok elvégzésének körülményei, a fizikai értelemben vett mozgástér rögzítése pontosan és egyértelműen le van-e írva. (Ugyanakkor, a rendszer fejlesztése kapcsán ezek az alvállalkozók kiváló tapasztalati forrásnak tekinthetők.)

Fizikai védelem és a környezet védelme

Fizikai környezeti védelmi szabályokat/szabályzatot kell alkotni (minősített határzónák, zónában tartózkodás, oda való bejutás szabályainak rögzítésével).

Zónatérképeket kell készíteni a kórház épületeinek alaprajzai alapján: meg kell határozni, hogy melyek a tervezett (azon belül a zárható, és a nyitott), valamint a megszüntetendő bejutási pontok. Ezeket a későbbiekben ellenőrzés (folyamatos, vagy szúrópróbaszerű) alatt kell tartani.

Berendezések védelme

Tudatossági képzések kellenek a felhasználók részére, szorosan együttműködve az informatikusokkal és az orvosműszerészekkel. A klasszikus szabályokon túl (rendeltetésszerű használat) – hozzá kell szoktatni a dolgozókat, hogy az információ-bevitelre / feldolgozásra / tárolásra / továbbításra használt eszközöket csak illetékes szakember mozgassa. Például köztudott, hogy a számítógépek elhelyezése (tápegység ventillátora és a fal/asztal közötti távolság), vagy a rajta díszítő céllal elhelyezett virágcserép és hűtőmágnes befolyásolhatja az adott munkaállomás teljesítőképességét, élettartamát.

A kommunikáció és az üzemeltetés irányítása

Érdemes összeállítani egy információ-biztonsági etikai kódex-et – amit nehéz megírni és még nehezebb betartatni, de a bevezetése után oktatható és számon kérhető. Kezelni kell az osztott tulajdonosú munkaállomások problémáját: már a számítógépbe (nem a medikai, vagy gazdasági rendszerbe, hanem a Windows-ba) belépett dolgozót is tudni kell azonosítani.

E-mail kezelés: vajon minden kórház tisztában van-e azzal, hogy ha a dolgozója a céges postafiókon keresztül folytat jogsértő tevékenységet, akkor első körben az intézményt büntetik. A mobil eszközök (pen-drive, okostelefon, memóriakártya, optikai és mágneses adathordozók) használatát is szabályozni kell, ugyanakkor jellegüknél fogva más szabályok vonatkoznak ezekre, mint az „asztali gépekre". A használatot – a hozott szabályok keretei között – érdemes engedélyezni, hogy a későbbiekben – akár tervezetten, akár szúrópróbaszerűen – ellenőrizhessük az alkalmazás módját, vagy akár az adathordozó tartalmát (erre megfelelő jogosultsággal rendelkező munkakör szükséges). A tiltással csak annyit érhet el a kórház, hogy a dolgozók „eldugják és titokban használják", tehát IBIR szempontból ellenőrizhetetlenné válnak (a portok kiiktatása nem életszerű, és nem is célszerű).

Irattárolás/iratmegsemmisítés – ha a kórháznak a jogszabályban meghatározott ideig KELL tárolnia a betegdokumentációt, az azt is jelentheti, hogy a határidő lejárta után egy nappal már nem jogosult rá.

A gazdasági jellegű dokumentumoknak (szerződések, számlák, jelentések stb.) is jogszabályban van rögzítve a kötelező tárolási ideje, azonban azon túl, amíg rendelkezésre áll, felhasználható az intézmény ellen. A jelenlegi jogszabályok ismeretében az iratok nem a bezúzáskor/elégetéskor semmisülnek meg, hanem amikor az illetékes aláírta a megsemmisítési jegyzőkönyvet – ennek hiányában szintén megbüntethető a kórház.

Hozzáférés-ellenőrzés

Optimális esetben a munkaügy rendszeres időközönként elküldi az informatikának a kilépő és belépő dolgozók listáját. Ez kivédi annak veszélyét, hogy a kikörözés alkalmával az informatikus valamilyen okból elfelejti törölni a regisztrációt. Ennek a módszernek továbbfejlesztett változata, amikor a szervereken aktív regisztrációval rendelkező felhasználók listáját összevetik a munkaügyi nyilvántartásokkal. Rendszer-takarítás – egyszerű és brutális, viszont célravezető és a szabvány elvárásainak teljes mértékben megfelelő módszer a bizonyos ideig inaktív hozzáférések megszüntetésére. A medikai rendszer felhasználói között kockázati tényezőt jelentenek a gyakorlatukat a kórházban töltő rezidensek, ugyanis a távozásukról általában nem kap értesítést az Informatikai Osztály.

Információbiztonsági incidensek kezelése

Tudatosítani kell a dolgozókban, hogy joguk és munkaköri kötelességük a napi munka által feltárt biztonsági rések, hibák, illetve a bármilyen formában észlelt illetéktelen behatolások észlelésének jelentése a közvetlen felettes, vagy a helyi IBIR felelős felé.

Követelményeknek való megfelelés

A kiépített rendszernek természetesen meg kell felelni a szabvány és a hatályos jogszabályok előírásainak egyaránt. Emellett az IBIR-nek illeszkednie kell a már régóta működő ISO 9001-es rendszerhez is. Ennek megvalósítása érdekében:

- felül kell vizsgálni valamennyi (tanúsított és előkészített) MIR-t, azokat össze kell csiszolni, illetve hozzá kell igazítani az IBIR-hez;
- a belső auditokat célszerű egyszerre elvégezni – összevonni az auditterveket és a belső audit kérdésjegyzékeket.

ÖSSZEGZÉS

Ahogy a fentiekből is kitűnik, egy működőképes IBIR bevezetése és üzemeltetése nem egyszerű és gyors folyamat. Azonban megéri a ráfordított időt és erőforrást, mert egy egészségügyi intézményben a nem várt esemény bekövetkezése és az elhárítás között eltelt idő a beteg állapotára, életére is hatással lehet, így a hasznossága nem vitatható.

IRODALOMJEGYZÉK

[1] MAGYAR SZABVÁNY MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei. Követelmények.
Kiadó: Magyar Szabványügyi Testület (Hivatkozási szám: MSZ ISO/IEC 27001:2006)

A SZERZŐK BEMUTATÁSA

Guba Tamás 1998-ban végzett a nyíregyházi Egészségügyi Főiskolán, szervezői szakon. Pályafutását a Kenézy Kórházban kezdte, mint rendszeradminisztrátor, majd egy kórház-informatikai cégnél rendszerszervező volt. 2003-tól Debrecenben, a VESZ-nél fogja össze a minőségirányítást, a finanszírozást, kontrollingot és az informatikát. 2009 óta foglalkozik (ismét a Kenézy Kórházban) minőségirányítással, valamint taktikai és stratégiai szintű vezetői döntéstámogatással. Ugyancsak 2009-től, mellékállásban végzi különböző ISO szabványok (főként MIR és IBIR) rendszerének kiépítését és üzemeltetését.

Dr. Lampé Zsolt Tibor orvos, egészségügyi szakmenedzser. 1987-ben végzett a Debreceni Orvostudományi Egyetemen. 1991-ben tette le szemészeti szakvizsgáját. 1987 és 1999 között a Debreceni Orvostudományi Egyetem Szemészeti Klinikáján dolgozott klinikai orvos, majd egyetemi tanársegéd beosztásban. 1999 és 2001 között az Országos Egészségbiztosítási Pénztár egészségügyi főigazgató-helyettese, orvos szakmai vezetője, majd főigazgatója volt. 2007-ben a Kenézy Gyula Kórház és Rendelőintézet orvosigazgatója lett. 2008-tól jelenleg is a Kórház ügyvezető igazgatója.

Negyed évszázad a vesék védelmében

A Budapesti Nephrológiai Iskola egy egyhetes, angol nyelvű, nemzetközileg is elismert (29 európai/US CME kreditpont, illetve 50 OFTEX creditpont értékű) nephrológiai kurzus, amit a 25 éves Magyar Vesealapítvány szervezett.

A Semmelweis Egyetemen megrendezett esemény egyike a világ legrégebbi és legismertebb nephrológiai kurzusainak, mely 61 országból érkező résztvevőt vonzott az elmúlt évek során. A huszadik alkalommal megrendezett jubileumi eseményre 2013. augusztus 26. és 31. között került sor, amire a szervezők több különleges programmal is készültek.

Az egyhetes program során kiváló nemzetközi előadók segítségével áttekintették a nephrológia, hipertonológia, dialízis és a transzplantáció legfrissebb ismereteit. Az idei előadók között szerepelt a Nemzetközi Nephrológiai Társaság jelenlegi és előző elnöke, valamint az Európai Vese Szövetség – Európai Dialízis és Transzplantációs Társaság jelenlegi és előző két elnöke is.

A témakörök a molekuláris kérdésektől egészen a betegágy melletti feladatokig terjedtek, magukba foglalva a tudományos újdonságoktól a klinikai tapasztalatokig szinte mindent. A workshopok során lehetőség nyílt kiscsoportos közvetlen megbeszélésekre, ahol a résztvevők bemutathatták saját tapasztalataikat és feltehették kérdéseiket. A programnak része volt a legmodernebb dialízis és kutató központok meglátogatása is.

A 2013-as Budapesti Nephrológiai Iskolát a 11. Nemzetközi Bor és Egészség Szimpóziummal együtt, valamint a 8. Vese Világnaphoz csatlakozóan tartották meg.

A Nemzetközi Bor és Egészség Szimpóziumot augusztus 26-án rendezték meg, melyen a világ egyik legnevesebb nefrológusaként számon tartott Eberhard Ritz beszélt a bor egészségre és a vesére gyakorolt hatásáról. A bort már Hippokratész, az orvostudomány megalapítója is használta nyugtató és sebgyógyító céllal, a hasmenés, az alvási zavarok és a vizenyőképződés ellenszereként. Azóta számtalan tudományos kutatás készült a bor és az alkoholfogyasztás hatásairól. Vizsgálatokkal igazolható, hogy a mértékletes borfogyasztás javíthatja a szívbetegek, a magas vérnyomással küszködők és a cukorbetegek életkilátásait és a krónikus veseelégtelenség kialakulásának rizikóját is csökkenti, a kulcskérdés persze mindig a mennyiség.