Kórházi kockázatminimalizálás információbiztonsági elvek alapján

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

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. Egy kórház esetében a kár végső esetben emberéletbe is kerülhet. Ezt természetesen egyetlen egészségügyi intézmény sem tekintheti elfogadható kockázatnak.

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 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 even result in the loss of life. Naturally there is no healthcare institution that can take this as an acceptable risk.

BEVEZETÉS

A Kenézy Gyula Kórház életében (a továbbiakban: Kórház) – más fordulópontok mellett – elérkezett az az időszak, amikor az információbiztonsági rendszer már nem bevezetési, hanem üzemeltetési állapotában működik. A rendszer átesett egy tanúsításon, immár a napi rutin részévé vált. Az IME-ben 2013-ban megjelent cikkünkben [1] áttekintettük a szabvány követelményeinek jelentős részét, néhány pontot azonban – terjedelmi okokból – csak érintettünk. Hogy teljesebb képet kapjunk egy információbiztonsági rendszer elemeiről, az azokkal kapcsolatos teendőkről, ezért most ezeket mutatjuk be részletesen.

MIÉRT VAN SZÜKSÉG INFORMÁCIÓBIZTONSÁGI RENDSZERRE?

A kórház speciális helyzete (egy városban három nagy szakellátó intézmény) azt eredményezte, hogy az egészségügyben általánosnak tekinthető bizonytalanság-érzet halmozottan jelentkezett a dolgozók körében. A bizonytalan munkaerő könnyebben fárad, hamarabb lesz fásult, gyorsabban csökken a koncentrációs képessége. Ennek egyenes következménye a magasabb hibaszázalék, és a több betegpanasz. A betegpanasz pedig általában drága mulatság.

A közép és felső vezetéstől indultak a következő kérdések:

- Miért következtek be ezek a hibák?
- Milyen incidensekkel kell még számolnunk?
- Mi a bekövetkezés valószínűsége?
- Hogyan tudunk ezekre felkészülni?
- Mit tehetünk az elkerülésük érdekében?

Megszületett a kórház stratégiai célja: minimalizálni a fentiek kockázatát! Ehhez természetesen valamilyen eszközre van szükség, és a célnak kiválóan megfelel egy kifejezetten kockázatkezelési szabvány (kvázi szabálygyűjtemény). Egy olyan szabvány, ami túlmutat az informatikai biztonságon, és ami mindenkinek ajánlott, aki adatokat rögzít/használ/tárol.

A DOKUMENTÁCIÓS RENDSZER

Az MSZ ISO/IEC 27001:2006 azon kevés szabványok egyike, amelyiknek egyik fejezete (a 4.3.1. fejezet) tételesen és részletesen felsorolja, hogy milyen kézikönyvre, szabályzatokra, eljárásokra, utasításokra van szükség.

A dokumentációs rendszernek tartalmaznia kell:

- dokumentált nyilatkozatokat az információbiztonsági szabályzatról és a szabályozási célokról;
- információbiztonság alkalmazási területét;
- információbiztonságot támogató eljárásokat és intézkedéseket;
- kockázatfelmérés módszertanának leírását;
- kockázatfelmérési jelentést;
- kockázatjavítási tervet;
- szervezet által igényelt dokumentált eljárásokat, amelyek biztosítják az információbiztonsági folyamatok eredményes tervezését, működtetését és ellenőrzését, és leírják az intézkedések hatékonysága mérésének módját;
- az alkalmazhatósági nyilatkozatot.

Azért, hogy értehetőbb legyen:

- Információbiztonsági Kézikönyv (esetleg integrálva a minőségirányítási kézikönyvvel)
- Információbiztonság politika (esetleg integrálva a minőségpolitikával)
- Iratkezelési szabályzat, egészségügyi dokumentáció kezelési szabályzat
- Adatvédelmi szabályzat, fizikai és környezeti biztonság szabályzat
- Működésfolytonossági tervek, használható vészforgatókönyvek

- Kockázatcsökkentési tervek – Mi a cél, milyen intézkedést hozunk a csökkentés érdekében? Ki a felelős a betartásáért/betartatásáért? Milyen szabályozó dokumentummal akarjuk elérni a javulást? Hogyan, milyen rendszerességgel ellenőrizzük a betartást; mérjük a javulást?
- Alkalmazhatósági nyilatkozat – mely szabványpont alkalmazható a kórház működésére, és készült-e arra a pontra valamilyen szabályozó dokumentum?

KOCKÁZATI TÉNYEZŐK ELEMZÉSE ÉS KEZELÉSE

A kockázati elemzést ki kell terjeszteni valamennyi folyamatra. 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 szinten (lásd alább) kerül besorolásra – vészforgatókönyvet kell kidolgozni (szorosan együttműködve az érintett szervezeti egységgel), majd azokat rendszerezni és rendszeresen felülvizsgálni, illetve tesztelni (tervezetten és randomszerűen) kell.

Kockázati tényezőket kell keresnünk:
- a kórház folyamataiban (a gyógyítással összefüggő és a kisegítő folyamatokban egyaránt),
- az ingatlanokban / az infrastruktúrában,
- a használt műszerekben / eszközökben
- a munkaerőben
- a dokumentációban (papír és elektronikus egyaránt)

A fentiek közül a leggyakoribb a folyamatok az infrastruktúra és a dokumentáció kockázatelemzése.

Azt, hogy egy folyamatot/eszközt milyen részletességgel lehet/kell kockázati tényezőkre bontani, cikkünkk már idézett első részben olvashattuk, a lázmérő példáján levezetve. A kockázati osztályokat egyébként mi határozzuk meg: magunkat osztályozzuk, magunknak osztályozunk, de aztán viselnünk kell a következményeit!

A kockázati tényezők elemzése során a következőket kell mérlegelnünk:
- milyen gyakorisággal következik be az esemény?
- mekkora kárt okoz a bekövetkezése?
- mit tehetek ellene?
- mennyibe kerül az óvintézkedés?

A kockázat mértéke egy egyszerű képlet segítségével kerülhet meghatározásra:

Kockázat mértéke = Valószínűség * Kárérték

A kórház a kockázat mértékét a következő skálák szerint határozza meg:

Bekövetkezés valószínűség	Okozott kár
• évente vagy ritkábban • negyedévente – félévente • havonta • hetente • naponta	• 100 eFt alatt • 500 eFt alatt • 1 millió Ft alatt • 10 millió Ft alatt • 100 millió Ft alatt • Kritikus súlyosságú kockázat

Ettől természetesen el lehet térni, a helyi sajátosságoknak megfelelően.

A kockázatok okának kiderítésére létezik egy roppant egyszerű eszköz; az „5 miért” módszere. A módszer célja, hogy eljussunk a probléma alapjához, amit talán első pillantásra nem vettünk észre, amire esetleg nem is gondoltunk volna. A módszer alkalmazása mindössze annyi, hogy ötször feltesszük a „Miért?” kérdést ugyanazzal a problémával kapcsolatban, és az újabb miért az előző válaszra kérdez rá (persze előfordulhat, hogy a probléma mélységétől függően, többször, vagy kevesebbszer kell a kérdést feltennünk). Természetesen ezzel még nincs megoldva a probléma, de megtaláltuk az okot. Lényeges pont, hogy ne álljunk meg az első kérdés után, mert akkor csak tüneti kezelést végeztünk.

Egy egyszerű példa az 5 miért módszerre:

Indító probléma: Betegpanasz érkezett, miszerint egy adott műtétet meg kellett ismételni.
- Miért kellett megismételni a műtétet? Adott eszköz nem állt rendelkezésre.
- Miért nem állt rendelkezésre az eszköz? A műtéti raktár a protokoll alapján készíti elő a tálcákat, és a kérdéses eszköz nem szerepelt a protokollban.
- Miért nem szerepelt az eszköz a protokollban? Mert csak az az operatőr használja azt az eszközt, aki éppen a műtétet végezte. (egyedi igény)
- Miért használ az operatőr protokolltól eltérő eszközt? Mert csak azzal az eszközzel tudja eredményesen elvégezni a műtétet.
- Miért csak azzal az eszközzel tud eredményesen műteni? Mert ennek a műszernek a használatára lett kiképezve.

Ennek a problémának több megoldási lehetősége is van:
- Az eszközt felvesszük az adott műtéttípushoz tartozó protokoll eszközlistájára (ugyanakkor felmérjük, hogy mekkora készlettel kell rendelkeznünk, hogy zökkenőmentes legyen a műtétek rendje)
- Elküldjük az operatőrt olyan továbbképzésre, ahol megtanulhatja és begyakorolhatja a protokoll szerinti eszközökkel történő operálást.

Milyen kockázati tényezők merülhetnek fel a dokumentáció elemzése során?

Rendelkezésre állás:
- Nem áll rendelkezésre, mert elfelejtettük elkérni.
- Nem áll rendelkezésre, mert nem bocsájtják rendelkezésünkre.
- Nem áll rendelkezésünkre, mert postázási hiba folytán elkeveredett.
- Nem áll rendelkezésünkre, mert saját cégen belül nem megfelelő az iratkezelés.
- Nem áll rendelkezésünkre véletlen iratkezelési hiba folytán.

- Nem áll rendelkezésünkre váratlan katasztrófahelyzet bekövetkezése miatt.
- Nem áll rendelkezésünkre, mert nincs rendszerezve.
- Nem áll rendelkezésre, mert az egységekből nem érkezik be az irodába.
- Nem áll rendelkezésünkre, mert nem készült el időben.
- Nem áll rendelkezésre, mert nincs folyamatosan vezetve.

Megbízhatóság:
- Megbízhatatlan tartalmi hiányosság miatt.
- Megbízhatatlan, mert hibás, téves adatokat tartalmaz.
- Megbízhatatlan, frissítési, nyomonkövetési hiányosságok miatt.
- Megbízhatatlan, megváltozik a gyakorlat és nem követi a dokumentáció.
- Megbízhatatlan, nem a szabályban rögzítettek szerint van vezetve.

Titkosság:
- Titkossága sérült postázási probléma miatt.
- Titkosság sérült nem megfelelő iratkezelés miatt.
- Titkosság, hozzáférési probléma, tiszta asztal elv megsértése.

Végső soron, a kapott eredményt milyen kockázati szintbe soroljuk be:
- 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.

Az ingatlanok/infrastruktúra elemzése során bejutási pontokat, zónatérképeket kell létrehoznunk. Mire kell odafigyelnünk?
- A bejutási pontok felmérése esetén meg kell határoznom, hogy melyek
  - nyitottak (folyamatosan szabad „áramlás" biztosítanak)
  - zárhatóak (átjárhatóságuk írásos szabályokhoz kötött – pl. időtartam, munkakör)
  - megszüntetendő (teljes mértékben lezárandó)
- A zónatérképek kialakításánál figyelembe kell vennem, hogy
  - Kinek (munkakör, vagy akár személy szerint) van joga az adott épületben / épületrészben / helyiségben tartózkodni és milyen feltételekkel.

A legszemléletesebb (és leglátványosabb) térképet az épületek tervrajzai segítségével tudjuk elkészíteni. Mit tegyünk azonban, ha nem áll rendelkezésre tervdokumentáció? (Hiszen ezek általában korlátozott példányszámban találhatók meg a kórházban – régebbi, vagy korábban más tulajdonában lévő épület esetében hiányosan, vagy egyáltalán nem áll rendelkezésre. Másolásuk pedig körülményes – általában kórházon belül nem is oldható meg –, és költséges.) Dolgozzunk abból, amink van. Ezek lehetnek akár:
- a menekülési útvonalak meghatározásánál használt rajzok,
- az épületek tervezését megelőző skiccek, vázlatok,
- nem-tervezői szoftverrel rajzolt alaprajzok,
- végső soron egy hagyományos lista (felsorolás) az adott épület helyiségeiről, és nagyobb egységeiről, kiegészítve az egyéb adatokkal.

Nem szabad elfeledkeznünk arról, hogy a bejutási pontok meghatározása és a zónatérképek kialakítása során nem csak a betegellátó osztállyal kell foglalkoznunk, hanem a járóbeteg-ellátó egységekkel, a raktárakkal, a szociális helyiségekkel, a kiszolgáló egységek irodáival/műhelyeivel, az épületek folyosóival, alagútjaival, az olyan helyiségekkel, ahol nincs feltétlenül állandó dolgozói jelenlét (pl. gőzközpont, kazánház) és az intézményhez tartozó külső területtel (pl. parkolók).

Amiről nem szabad elfeledkeznünk – életszerű, használható megoldásokat találjunk.
- hiába szereljük fel a legmodernebb számzárral, kártyaleolvasóval ellátott bejáratot, ha a hely annyira forgalmas, ha az ott dolgozók inkább kitámasztják az ajtót,
- hiába építünk be behatolás, tűz- és robbanásbiztos, ugrókóddal ellátott ajtót gipszkarton falba,
- a vészkijáratok valóban csak a menekülési útvonalon meghatározott irányba legyenek „egy mozdulattal" nyithatóak; a túloldalról vagy zárjuk le, vagy csak kulccsal/kártyával legyenek nyithatók (hamarosan azt fogjuk tapasztalni, hogy csökken a „csak egy kis időre eltűnt dolgozók/betegek" száma, illetve ritkulni fognak az illetéktelen behatolások, vagy akár a lopások – hiszen kiiktattunk egy olyan bejutási lehetőséget, ami nem feltétlenül van szem előtt),

Ha már az infrastruktúránál tartunk, fel kell mérnünk az üzembiztonságot veszélyeztető tényezőket, és azokat minimalizálni kell. Ezek a következők:
- Tisztában vagyunk-e azzal, hogy a kórház hány betápról kapja a szolgáltatótól az áramot (és miért csak egyről)?
- Tudjuk-e hogy mekkora területet és mennyi időre tud ellátni a generátorunk? Vajon az áramszünet bekövetkezése után mennyi idővel kapcsol be és miért csak akkor? Mikor teszteltük ezt utoljára?
- Vajon mikor ellenőriztük utoljára a falakon futó kábelcsatornákat? Mindenütt a helyén van a csatorna takarólemeze? Hiába szerezzük be a legmodernebb, legbiztonságosabb rack-szekrényeket, ha mögöttük csupaszon lógnak a vezetékek, vagy ha a szekrény nincs megfelelően rögzítve.

ÉRTÉKLELTÁR

Mi tekinthető az információbiztonsági szabvány szempontjából vagyonnak/értéknek: „Bármi, ami a szervezet számára érték." A rendszer célja: „a szervezet vagyontárgyai megfelelő védelmének elérése és fenntartása. Minden vagyontárgyat vegyenek számba és legyen megnevezett gazdájuk. A gazdát azonosítani kell minden vagyontárgyhoz, és ki kell jelölni a felelősséget a megfelelő intézkedések fenntartásáért. Az egyes intézkedések bevezetését a gazda átháríthatja, ha helyénvaló, de a gazda marad felelős a vagyontárgyak védelméért."

Újabb tisztázandó információbiztonsági fogalom: a gazda.

A vagyontárgy gazdája felelős a következőkért:

- annak biztosításáért, hogy az információ feldolgozó eszközhöz kapcsolódó információ és vagyontárgy megfelelően legyen osztályozva;
- a hozzáférési korlátozás és osztályozás meghatározásáért és időnkénti átvizsgálásáért, figyelembe véve a vonatkoztatható hozzáférés-ellenőrzési szabályzatot.

Gazda szerepet lehet kijelölni:

- a működési folyamatra;
- a tevékenységek meghatározott csoportjára;
- egy alkalmazásra, vagy
- egy meghatározott adatcsoportra.

Sokféle típusú vagyontárgy van, beleértve a következőket:

- információ: adatbázisok és adatgyűjtők, szerződések és megállapodások, rendszerdokumentáció, kutatási információ, használói kézikönyv, oktatási anyag, üzemeltetési vagy támogatási eljárások, működési folytonossági tervek, tartalék megállapodások, audit-kísérődokumentáció és archivált információ;
- szoftver vagyontárgyak: alkalmazási szoftver, rendszerszoftver, fejlesztési eszközök és segédprogramok;
- fizikai vagyontárgyak: számítógép-berendezés, kommunikációs berendezés, eltávolítható adathordozók és más berendezések;
- szolgáltatások: számítógépes és kommunikációs szolgáltatások, általános közszolgáltatások, pl. fűtés, világítás, energia és légkondicionálás;
- emberek és képesítésük, jártasságuk és tapasztalatuk;
- nem kézzelfogható dolgok, mint hírnév és a szervezet arculata.

Az előző részben felsoroltuk, hogy egy kórház esetében pontosan milyen jellegű eszközök tartoznak a leltárba. Most kitérünk arra, hogy milyen adatokat is kell ezekről az eszközökről nyilvántartanunk.

- az eszköz azonosítója (ez lehet a gyári szám, és/vagy a helyi gazdasági rendszerben szereplő egyéb egyértelmű azonosító)
- az eszköz megnevezése (gyártmány, típus, kategória – pl. HP, LaserJet 1100, asztali nyomtató)
- felhasználó / gazda (ez lehetőleg konkrét személy, de az eszköz jellegéből adódóan (pl. hálózati nyomtató) lehet csoport is)
- tulajdonos (az eszköz a kórház tulajdona, vagy egyéb (bérelt, alapítványi, esetleg a dolgozó saját tulajdona))
- felhasználás helye (a helyiség pontos megnevezése – amennyiben nem köthető egyetlen helyiséghez, akkor a lehetséges felhasználási helyek)

A papír és elektronikus formában tárolt információ esetében a fentieken túl azt is nyilván kell tartanunk, hogy az adott információ

- milyen jellegű (nyilvános, belső használatú, titkos)
- milyen adathordozón tároljuk (munkaállomás, szerver, mobil adathordozó)

Értelemszerűen a különböző hibafokozatok más és más megoldást igényelnek. Az 1. ábra bemutat néhány ilyen fogalmat és azok kapcsolatát.

1. ábra
Példa az előforduló hibafokozatokra és súlyosságuk kapcsolatára

HUMÁN ERŐFORRÁS

Az előző részben részleteztük, hogy miként jelent kockázatot a dolgozó alkalmazása előtt, alatt és után. Azonban mindegyik bekezdéshez van még mit hozzátennünk.

Alkalmazás előtti kockázat

Képzeljük el, hogy meghirdetünk egy állást, amire valaki lead egy pályázatot. Elbíráljuk az anyagot és nem ő nyeri el az állást. Néhány héttel/hónappal később azonban kiértesítjük, hogy egy másik munkahelyre viszont ideálisnak tartjuk, úgyhogy felvételt nyert. A pályázó ezután bepereli a kórházat, mondván, visszaéltünk az adataival, ugyanis nem(csak) arra és annyi időre használtuk fel, amire (az az álláshirdetés, amire eredetileg leadta pályázatát) és ameddig (a pályázat elbírálási határideje – ezt általában nem határozzuk meg, de következtetni lehet rá) ő feljogosított bennünket. A pert megnyerte, a kártérítésre igényt tarthat.

Alkalmazás ideje alatti kockázat

Minden vezető számára ismerős a szituáció: reggel betelefonál valamelyik beosztott, és valamilyen váratlan eseményre hivatkozva szabadnapot kér. Ez önmagában nem

gond, de vajon utána néztünk-e annak, hogy adott időintervallumon belül melyik dolgozónk hányszor kért szabadnapot? Ha valaki gyakran él ezzel a lehetőséggel, fokozott kockázati tényezőnek minősíthető, ugyanis szinte biztos, hogy készül valamire. (Ilyenkor utasítható az informatika, hogy figyeljék a hálózati forgalmat és a naplófájlokat.)

Alkalmazás utáni kockázat

A dolgozó valamilyen formában távozott, majd néhány héttel/hónappal később jelentkezik nálunk, hogy kártérítésre tart igényt, mivel a kórházban töltött szolgálati idő alatt maradandó egészségkárosodást/krónikus betegséget szerzett. Nehéz helyzetbe kerülhetünk, hiszen az ellenkezőjét kell bebizonyítanunk, úgy, hogy a bíróság nekünk adjon igazat. Pedig, mindössze annyit kellett volna tennünk, hogy az utolsó munkanapok egyikén egy alapos ”záró üzemorvosi” vizsgálatot végeztetünk, melyben rögzítjük a dolgozó akkori egészségi állapotát.

KÖVETKEZTETÉSEK

Egy rendszert csak akkor nem kell fejleszteni, ha azt már nem használjuk. Ugyanez igaz az egészségügy valamennyi (gyógyító és kiszolgáló) területére. Mivel folyamatosan új műszerekkel, eszközökkel, anyagokkal, technológiákkal, eljárásokkal szembesülünk, így a rendszer fejlesztésének belső oka adott. Külső okként megemlíthető a szabványrevízió, mely napjainkban zajlik és nemcsak az információbiztonsági, hanem valamennyi közismert szabványt (beleértve az ISO 9001-est is) érinti. Ha már egy kórház megszerzett egy tanúsítványt, nem engedheti meg magának azt a luxust, hogy elveszítse, és esetleg évekkel később újraépítse. Jelen és az ezt követő írásainkkal a rendszerek folyamatos fejlesztésében, az átállás megkönnyítésében kívánunk segítséget nyújtani más kórházaknak.

KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretnénk köszönetet mondani Lelkes Péternek (EMT Zrt.) és Siklósi Imrének (Tequa-Zert Kft.) a konzultációs lehetőségért, és az építő jellegű kritikáért.

IRODALOMJEGYZÉK

[1] Guba Tamás, Lampé Zsolt: Információbiztonsági kérdések egy megyei kórházban – rendszerkiépítési és tanúsítási tapasztalatok IME – Az egészségügyi vezetők szaklapja, 2013/7. szám16-20
[2] MAGYAR SZABVÁNY MSZ ISO/IEC 27001 Informatika. Biztonságtechnika. Az információbiztonság irányítási rendszerei, Követelmények Kiadó: Magyar Szabványügyi Testület (Hivatkozási szám: MSZ ISO/IEC 27001:2006)
[3] MAGYAR SZABVÁNY MSZ ISO/IEC 17799 Informatika. Biztonságtechnika. Az információbiztonság irányítási gyakorlatának kézikönyve, Kiadó: Magyar Szabványügyi Testület (Hivatkozási szám: MSZ ISO/IEC 17799:2006)

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.