NAJVYŠŠÍ KONTROLNÝ ÚRAD SLOVENSKEJ REPUBLIKY

Číslo poverenia: 1049/01
Zo dňa: 23. 09. 2014

Počet výtlačkov: 2
Výtlačok číslo: 1
Počet strán: 12
Počet príloh: 0

P R O T O K O L

o výsledku kontroly
hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií
vo vybraných nemocniciach SR

Fakultná nemocnica s poliklinikou Žilina

Žilina november 2014

Zhrnutie

NKÚ SR v spolupráci so Švajčiarskym federálnym kontrolným úradom vykonal v marci 2013 rizikovú analýzu informačno-komunikačného prostredia vo vybraných nemocniciach SR. Riziková analýza ukázala nedostatky v oblasti činnosti organizácie, informačných technológií, vnútorného kontrolného systému, aplikačného programového vybavenia, prevádzky informačno-komunikačných technológií a v iných oblastiach. Identifikované boli nedostatky predovšetkým v oblasti implementácie informačných systémov, procesoch vnútorného kontrolného systému, povedomia o informačnej bezpečnosti, stanovenie zodpovednosti a nezlučiteľnosti rolí, kľúčových aplikácií a databázových systémov. Z tohto dôvodu NKÚ SR do plánu kontrolnej činnosti na rok 2014 zahrnul kontrolu hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií vo vybraných nemocniciach, ktorej účelom bolo preveriť stav dodržiavania všeobecne záväzných právnych predpisov, hospodárnosti, správy a ochrany aktív v oblasti informačno-komunikačných technológií vo vzťahu k zabezpečeniu a ochrane aktív informačno-komunikačných technológií na základe výsledkov rizikovej analýzy.

Kontrola bola vykonaná v súlade so zákonom o NKÚ SR a boli uplatňované medzinárodné štandardy najvyšších kontrolných inštitúcií ISSAI.

Predmetom kontroly bola správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií, dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií, dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy, prevádzka informačných systémov verejnej správy a kontrola bezpečnosti informačných systémov verejnej správy.

Hodnotiacimi kritériami bola relevantná legislatíva SR, vrátane súvisiacich právnych predpisov, týkajúcich sa jednotlivých oblastí predmetu kontroly a platných v konkrétnom kontrolovanom období.

Základom pre výber kontrolovaných údajov boli účtovné a finančné výkazy, dokumentácia k vedeniu a nakladaniu s majetkom štátu a výstupy z informačných systémov. Z dôvodu rozsiahlej údajovej základne výber vzorky bol realizovaný neštatistickou metódou na základe kvalifikovaného úsudku kontrolóra.

Preverením prírastkov a úbytkov dlhodobého hmotného a dlhodobého nehmotného majetku v oblasti informačno-komunikačných technológií v kontrolovanom období nebol zistený rozdiel medzi požadovaným a skutočným stavom. Nadobudnutý majetok bol obstaraný v súlade so zákonom o verejnom obstarávaní a bol zaradený do evidencie majetku nemocnice. Kontrolou vyraďovania neupotrebiteľného majetku neboli zistené nedostatky.

Novelizáciou zákona o informačných systémoch verejnej správy sa nemocnica stala povinnou osobou v zmysle uvedeného zákona. Z tohto dôvodu bola nemocnica povinná vypracovať koncepciu rozvoja informačného systému verejnej správy. Nemocnica nevypracovaním koncepcie rozvoja informačného systému verejnej správy nekonala v súlade so zákonom informačných systémoch verejnej správy.

Preverením vybraných štandardov pre informačné systémy verejnej správy bolo zistené, že nemocnica nemala vypracovanú internú smernicu pre zálohovanie údajov a smernicu pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušili bezpečnostnú politiku. Taktiež nemocnica nezabezpečila vypracovanie plánov na zachovanie kontinuity pozostávajúce z havarijných plánov a plánov na obnovu

činnosti. V rozpore so štandardami pre informačné systémy verejnej správy nemocnica nemala menované osoby zodpovedné za informačnú bezpečnosť a správu jednotlivých aktív nemocnice. Dodávatelia, ktorí vykonávali pre nemocnicu činnosti vyplývajúce zo zmluvných vzťahov, neboli poučení o schválenej bezpečnostnej politike nemocnice. Povinnosti zamestnancov nemocnice vyplývajúce z bezpečnostnej politiky neboli uvedené v pracovných zmluvách. Nebol dodržaný štandard pre tvar e-mailových adries používateľov informačného systému verejnej správy.

Nedodržaním vyššie uvedených štandardov pre informačné systémy verejnej správy nemocnica porušila zákon o informačných systémoch verejnej správy.

Kontrolou vybraných ustanovení zákona o ochrane osobných údajov bolo zistené, že nemocnica neviedla evidenciu všetkých informačných systémov, v ktorých spracúvala osobné údaje. V čase, keď nemocnica nemala osobu poverenú dohľadom nad ochranou osobných údajov, neoznámila Úradu na ochranu osobných údajov SR prevádzkovanie informačných systémov, v ktorých spracúvala osobné údaje.

Nemocničný informačný systém pozostával zo šiestich modulov, ktorých prevádzku zabezpečoval odbor informatiky. Prístup tretích strán do nemocničného informačného systému bol realizovaný na základe dvoch zmlúv, ktorými bola zabezpečená podpora prevádzky troch modulov. Kontrolou týchto zmlúv bolo zistené, že v rozpore so štandardami pre informačné systémy verejnej správy neboli v zmluvách uvedené bezpečnostné požiadavky pre poskytovanie služieb vyplývajúcich z uvedených zmlúv.

Kľúčové komponenty nemocničného informačného systému (servre, aktívne prvky siete LAN, záložné zdroje,...) mala nemocnica umiestnené v priestoroch na to určených (serverovňa). Serverovňa sa nachádzala na prízemí a nebola dostatočne oddelená fyzickými prostriedkami od ostatných priestorov, čo bolo v rozpore so štandardami pre informačné systémy verejnej správy.

Odporúčania na riešenie zistených nedostatkov:

- zaviesť interný predpis odboru informatiky do systému riadenia kvality nemocnice (schváliť ho vedením nemocnice ako smernicu),
- zaradiť oddelenie informatiky do procesu skončenia pracovného pomeru zamestnancov, z dôvodu aktualizácie prístupových práv do nemocničného informačného systému.

Podľa poverenia predsedu Najvyššieho kontrolného úradu Slovenskej republiky (ďalej len „NKÚ SR“) č. **1049/01** zo dňa 23. 09. 2014 vykonali:

Ing. Juraj Podolák, vedúci kontrolnej skupiny
Mgr. Ľubica Grochalová dos Santos, členka kontrolnej skupiny

Kontrolu hospodárenia a ochrany aktív v oblasti informačno-komunikačných technológií vo vybraných nemocniciach SR, ktorej účelom bolo preveriť stav dodržiavania všeobecne záväzných právnych predpisov, hospodárnosti, správy a ochrany aktív v oblasti informačno-komunikačných technológií vo vzťahu k zabezpečeniu a ochrane aktív informačno-komunikačných technológií na základe výsledkov rizikovej analýzy.

Kontrola bola vykonaná v čase od 02.10.2014 do 28.11.2014 vo

Fakultnej nemocnici s poliklinikou Žilina
Vojtecha Spanyola 43, 012 07 Žilina
IČO 17335825

za kontrolované obdobie rokov 2012-2014a v prípade potreby objektívneho zhodnotenia kontrolovanej skutočnosti aj predchádzajúce obdobie.

Kontrola bola vykonaná v súlade so zákonom NR SR č. 39/1993 Z. z. o Najvyššom kontrolnom úrade Slovenskej republiky v znení neskorších predpisov a so štandardami, ktoré vychádzajú zo základných princípov kontroly (ISSAI 100 – 999) v rámci medzinárodných štandardov najvyšších kontrolných inštitúcií.

Predmetom kontroly bolo:
- správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií,
- dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií,
- dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy,
- prevádzka informačných systémov verejnej správy,
- bezpečnosť informačných systémov verejnej správy.

Počas výkonu kontroly bolo zistené:

1. Správa majetku štátu, hospodárenie a nakladanie s majetkom štátu v oblasti informačno-komunikačných technológií

Dňa 01.01.1992 bola zriaďovacou listinou Ministerstva zdravotníctva Slovenskej republiky (ďalej len „MZ SR“) zriadená Nemocnica s poliklinikou Žilina ako štátna príspevková organizácia s právnou subjektivitou. Na základe rozhodnutia MZ SR č. 19514-4/2009-OP s účinnosťou od 01.10.2009 došlo k zmene názvu na Fakultná nemocnica s poliklinikou Žilina(ďalej „FNsP Žilina“ alebo „nemocnica“).

FNsP Žilina poskytuje špecializovanú ambulantnú a ústavnú zdravotnú starostlivosť, vrátane ústavnej pohotovostnej služby, stacionáre, úkony jednodňovej starostlivosti, centrálny príjem, spoločné vyšetrovacie a liečebné zložky, oddelenie liečebnej výživy a stravovania

a spolupracuje so vzdelávacími ustanovizňami, ktoré poskytujú stredoškolské, vysokoškolské a ďalšie vzdelávanie zdravotníckych pracovníkov.

Štatutárnym orgánom FNsP Žilina je riaditeľ, ktorý je oprávnený konať v mene organizácie vo všetkých veciach. Zodpovedá za realizáciu zdravotnej starostlivosti a za plnenie úloh vo FNsP Žilina.

Na zabezpečovanie svojich úloh bol FNsP Žilina zverený do jej správy hmotný aj nehmotný majetok s ktorým hospodári a nakladá ako správca majetku.

FNsP Žilina ako správca majetku štátu je v zmysle ustanovenia § 3 ods. 2 zákona č. 278/1993 Z. z. o správe majetku štátu v znení neskorších predpisov (ďalej len „zákon č. 278/1993 Z. z.“) oprávnená a povinná tento majetok užívať na plnenie úloh v rámci predmetu činnosti alebo v súvislosti s ním, nakladať s ním podľa tohto zákona, udržiavať ho v riadnom stave, využívať všetky právne prostriedky na jeho ochranu a dbať, aby nedošlo najmä k jeho poškodeniu, strate, zneužitiu alebo zmenšeniu. Podľa ustanovenia § 3 ods. 9 zákona č. 278/1993 Z. z. je FNsP Žilina povinná viesť o majetku štátu účtovníctvo v rozsahu a spôsobom ustanoveným zákonom č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov (ďalej len „zákon č. 431/2002 Z. z.“).

Správnosť stavu a pohybu vykázaného majetku nemocnice bola preverená porovnaním údajov v účtovnom výkaze súvaha a údajov zachytených v hlavnej knihe, s dôrazom na kontrolu stavu a pohybu na účtoch v účtovej triede 0 - Dlhodobý majetok. Preverením stavu a pohybu (prírastky a úbytky) na účtoch dlhodobého majetku neboli zistené rozdiely.

Kontrolou prírastkov dlhodobého hmotného majetku (ďalej len „DHM“) a dlhodobého nehmotného majetku (ďalej len „DNM“) v oblasti informačno-komunikačných technológií (ďalej len „IKT“) bolo zistené, že v kontrolovanom období mala nemocnica:

- prírastky DHM na účte 022 21 –Samostatné hnuteľné veci, nákup pre ostatné účely sume 11 832,00 eur za obstaranie pracovnej stanice s tromi monitormi,
- prírastky DNM na účte 013 21 – Softvér nad 2 400,00 €, nákup pre ostatné účely v sume 7 430,00 eur za obstaranie softvéru webovej stránky.

Kontrolou inventárnych kariet nadobudnutého DHM a DNM v oblasti IKT bolo zistené, že uvedený majetok mala nemocnica zaradený v evidencii majetku a porovnaním účtovného stavu neboli zistené rozdiely.

Postup a proces vyraďovania a likvidácie neupotrebiteľného majetku FNsP Žilina bol upravený v Smernici pre vyraďovanie neupotrebiteľného dlhodobého hmotného majetku, drobného hmotného majetku, osobných ochranných pracovných prostriedkov a pomôcok a ostatného hmotného majetku v správe FNsP Žilina (ďalej len „smernica pre vyraďovanie neupotrebiteľného majetku“). Uvedená smernica bola vypracovaná v súlade s ustanovením § 13b zákona č. 278/1993 Z. z., ktorý upravoval nakladanie s neupotrebiteľným majetkom štátu.

FNsP Žilina v kontrolovanom období vyradila 51 kusov DHM v oblasti IKT z dôvodu, že boli zastarané, alebo ich oprava by bola nerentabilná.

O neupotrebiteľnosti majetku štátu rozhodoval riaditeľ nemocnice ako štatutárny orgán správcu majetku štátu a nariadil jeho likvidáciu. Rozhodnutia o neupotrebiteľnosti majetku obsahovali zákonné náležitosti v zmysle ustanovenia § 13b ods. 2 zákona č. 278/1993 Z. z. Vyraďovacia komisia vyhotovila zápisy o vyradení majetku, ktoré boli schválené riaditeľom nemocnice v súlade so smernicou pre vyraďovanie neupotrebiteľného majetku a následne bol vyradený majetok zlikvidovaný.

Kontrolná skupina preverila vyradenie 15 kusov počítačových staníc. Kontrolou vyraďovacieho procesu a účtovných zápisov o vyradení majetku z účtovnej evidencie nebol zistený nesúlad medzi požadovaným a skutočným stavom.

Inventarizácia majetku, záväzkov a rozdielu majetku a záväzkov za obdobie rokov 2012 a 2013 bola vo FNsP Žilina vykonaná v súlade s ustanovením § 29 a § 30 zákona č. 431/2002 Z. z. na základe príkazov riaditeľa nemocnice.

Čiastkovými inventarizačnými komisiami boli vyhotovené inventúrne súpisy a následne boli vypracované inventarizačné zápisy. Inventúrne súpisy a inventarizačné zápisy obsahovali náležitosti v zmysle ustanovenia § 30 ods. 2 a ods. 3 zákona č. 431/2002 Z. z.

Podľa predloženej dokumentácie inventarizáciou neboli zistené inventarizačné rozdiely. Inventarizácie pokladne boli v priebehu rokov 2012 a 2013 vykonané v súlade s ustanovením § 29 ods. 3 zákona č. 431/2002 Z. z. štyrikrát ročne.

V roku 2013 bola vykonaná mimoriadna inventúra z dôvodu výmeny pracovníkov zodpovedných za inventár na deviatich pracoviskách nemocnice.

2. Dodržiavanie všeobecne záväzných právnych predpisov pri hospodárení s finančnými prostriedkami v oblasti informačno-komunikačných technológií

Obstarávanie tovarov, služieb a stavebných prác mala FNsP Žilina v kontrolovanom období upravené smernicou o verejnom obstarávaní č. SM-01, ktorá bola s účinnosťou od 13.06.2014 nahradená smernicou o verejnom obstarávaní č. SM-04.

Kontrolná skupina preverila dodržiavanie hospodárnosti pri vynakladaní finančných prostriedkov na obstaranie DHM a DNM v oblasti IKT na dvoch verejných obstarávaniach, ktoré nemocnica realizovala v kontrolovanom období, čím bola vykonaná 100 % kontrola.

- softvér webovej stránky 6 191,67 eur bez DPH,
- pracovná stanica s tromi monitormi – 9 860,00 eur bez DPH.

V obidvoch prípadoch išlo o zákazky s nízkymi hodnotami, pri ktorých nemocnica dodržala postupy v zmysle zákona č. 25/2006 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon č. 25/2006 Z. z.“) a vnútornej smernice o verejnom obstarávaní účinnej v kontrolovanom období. Na predloženie cenových ponúk boli v obidvoch verejných obstarávaniach oslovení viacerí dodávatelia, pričom uspel ten, ktorý predložil najnižšiu cenovú ponuku.

Kontrolou bolo zistené, že obidve zákazky boli uvedené v súhrnnej správe o zákazkách s nízkou hodnotou s cenami vyššími ako 1000,00 eur na webovej stránke nemocnice v zmysle ustanovenia § 102 ods. 4 zákona č. 25/2006 Z. z.

3. Dodržiavanie všeobecne záväzných predpisov pre oblasť informačných systémov verejnej správy

Novelizáciou zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 275/2006 Z. z.“) sa FNsP Žilina s účinnosťou od 01.02.2010 stala povinnou osobou v zmysle uvedeného zákona. Z tohto dôvodu bola nemocnica povinná vypracovať koncepciu rozvoja informačného systému verejnej správy.

Kontrolnej skupine NKÚ SR bola predložená Koncepcia riadenia odboru informatiky a správy systému (ďalej len „koncepcia“), ktorú vypracoval vedúci odboru informatiky a správy systémov (ďalej len „odbor informatiky“).Predložená koncepcia, vychádzajúc

z reálnych potrieb nemocnice, detailne popisovala činnosti zabezpečované odborom informatiky pre jednotlivé oddelenia nemocnice:

- oddelenie spracovania poisťovní,
- oddelenie revízie zdravotných činností,
- oddelenie aplikácií, štatistiky a NIS,
- oddelenie technológií a sieti,
- oddelenie eHealth.

Predložená koncepcia nedefinovala ciele, organizačné, technické a technologické nástroje a architektúru informačných systémov nemocnice, čím nemožno z pohľadu zákona č. 275/2006 Z. z. považovať tento dokument za koncepciu rozvoja informačných systémov.

Z uvedeného dôvodu FNsP Žilina nedodržala ustanovenie §3 ods. 4 písm. a) zákona č. 275/2006 Z. z., podľa ktorého povinné osoby sú povinné vypracovať koncepciu rozvoja informačných systémov.

Bezpečnostnú politiku FNsP Žilina tvorili bezpečnostný projekt, ktorý bol vypracovaný vo februári 2014 a smernica, ktorou boli upravené práva a povinnosti všetkých zamestnancov nemocnice v oblasti ochrany a bezpečnosti majetku, informácií a ďalších hodnôt, ktoré nemocnica vlastní alebo spravuje (ďalej len „bezpečnostná smernica“). Vedenie nemocnice bezpečnostnú smernicu schválilo dňa 31.03.2014.

Bezpečnostný projekt v súlade s vyhláškou Úradu na ochranu osobných údajov Slovenskej republiky č. 164/2013 Z. z. (ďalej len „vyhláška č. 164/2013 Z. z.“), ktorou bol zadefinovaný rozsah a dokumentácia bezpečnostných opatrení, pozostával z bezpečnostného zámeru vypracovaného v januári 2014, analýzy bezpečnosti so stavom k 15.02.2014 a návrhu bezpečnostnej smernice vypracovanej k 01.03.2014.

Kontrolou dokladov tvoriacich bezpečnostnú politiku bolo zistené, že bezpečnostná politika nemocnice bola zadefinovaná v súlade so štandardami pre informačné systémy verejnej správy, avšak nie všetky bezpečnostné opatrenia uvedené v bezpečnostnej politike boli v podmienkach nemocnice realizované.

V oblasti riadenia informačnej bezpečnosti FNsP Žilina nezabezpečila realizáciu a dodržiavanie schválenej bezpečnostnej politiky v celom rozsahu aj tým, že nevypracovala interné smernice pre zálohovanie údajov (určenie skupín údajov, v akom rozsahu, akým spôsobom a s akou periodicitou sa budú zálohovať v prevádzkovej a archivačnej zálohe). Uvedená skutočnosť bola v rozpore s ustanovením § 29 písm. b) výnosu Ministerstva financií Slovenskej republiky č. 55/2014 Z. z. o štandardoch pre informačné systémy verejnej správy (ďalej len „výnos MF SR č. 55/2014 Z. z.“).

V rozpore s ustanovením § 29 písm. c) výnosu MF SR č. 55/2014 Z. z. nemocnica neurčila osobu zodpovednú za informačnú bezpečnosť (bezpečnostného správcu). Táto povinnosť pre nemocnicu vyplývala aj zo schválenej bezpečnostnej smernice.

FNsP Žilina nemala určené konkrétne zodpovednosti za jednotlivé aktíva nemocnice - správcov aktív nemocnice mal menovať bezpečnostný správca. Neurčením správcov aktív nemocnica nedodržala ustanovenie§ 29 písm. f) výnosu MF SR č. 55/2014 Z. z.

Kontrolou personálnej bezpečnosti bolo zistené, že poučenie zamestnancov o schválenej bezpečnostnej politike nemocnica realizovala na prevádzkových schôdzach jednotlivých oddelení nemocnice. Každý zamestnanec svojím podpisom potvrdil, že bol oboznámený so schválenou bezpečnostnou politikou. Osoby (dodávatelia), ktoré vykonávali pre nemocnicu činnosti vyplývajúce zo zmluvných vzťahov, neboli o schválenej bezpečnostnej politike poučení, čo bolo v rozpore s ustanovením § 30 písm. a) výnosu MF SR č. 55/2014 Z. z.

Kontrolou bolo ďalej zistené, že povinnosti vyplývajúce z bezpečnostnej politiky neboli uvedené v pracovných zmluvách zamestnancov, čím došlo k porušeniu ustanovenia § 30 písm. c) výnosu MF SR č. 55/2014 Z. z.

FNsP v Žiline nemala vypracovanú internú smernicu upravujúcu postup pre disciplinárne konanie vo vzťahu k zamestnancovi alebo vo vzťahu k tretej strane, ktorí porušili bezpečnostnú politiku, čím nedodržala ustanovenie § 30 písm. d) výnosu MF SR č. 55/2014 Z. z.

Manažment rizík pre oblasť informačnej bezpečnosti bol zadefinovaný v bezpečnostnom zámere (súčasť bezpečnostného projektu) a následne zapracovaný aj v bezpečnostnej smernici, podľa ktorej nemocnica zabezpečí vypracovanie plánov na zachovanie kontinuity pozostávajúce z havarijných plánov a plánov na obnovu činnosti. Ku dňu ukončenia výkonu kontroly nemocnica nemala vypracované plány na zachovanie kontinuity, čím nedodržala ustanovenie § 31 písm. f) výnosu MF SR č. 55/2014 Z. z.

Výkon kontroly bezpečnostnej politiky v podmienkach nemocnice podľa bezpečnostnej smernice zabezpečoval bezpečnostný správca. Keďže FNsP Žilina nemala vymenovaného bezpečnostného správcu, nevykonávala kontrolu bezpečnosti, čím nepostupovala v súlade s ustanovením § 32 písm. a) výnosu MF SR č. 55/2014 Z. z.

Zo schválenej bezpečnostnej smernice vyplývalo, že o každom bezpečnostnom incidente musí byť bez zbytočného odkladu informovaný bezpečnostný správca a všetci správcovia dotknutých aktív. Keďže nemocnica nemala vymenovaných správcov jednotlivých aktív a taktiež nemala vymenovaného bezpečnostného správcu, bol z tohto pohľadu manažment bezpečnostných incidentov nefunkčný.

FNsP Žilina pri osobných e-mailových adresách zamestnancoch pred deliacim znakom @ používala len priezvisko používateľa, čo bolo v rozpore s ustanovením § 26 písm. a) výnosu MF SR č. 55/2014 Z. z., podľa ktorého štandardom pre tvar e-mailových adries používateľov informačných systémov verejnej správy je používanie celého mena a priezviska zamestnanca.

Nedodržaním vyššie uvedených štandardov pre informačné systémy verejnej správy FNsP Žilina súčasne porušila ustanovenie § 3 ods. 4 písm. i) zákona č. 275/2006 Z. z., podľa ktorého povinné osoby, ktoré sú správcami, sú povinné zabezpečovať, aby bol informačný systém verejnej správy v súlade so štandardami informačných systémov verejnej správy.

Kontrolou boli preverené aj vybrané ustanovenia zákona č. 122/2013 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (ďalej len „zákon č. 122/2013 Z. z.“).Bezpečnostná smernica v oblasti ochrany osobných údajov bola vypracovaná v súlade s vyhláškou č. 164/2013 Z. z.

Podľa ustanovenia bodu 5.13.4.1 písm. j) bezpečnostnej smernice bola zodpovedná osoba (osoba poverená dohľadom nad ochranou osobných údajov) povinná spracovať metodický pokyn pre poučenie oprávnených osôb. Na vybranej vzorke zamestnancov bolo zistené, že vybraní zamestnanci boli poučení o právach a povinnostiach pri spracúvaní osobných údajov v súlade so zákonom č. 122/2013 Z. z. Z poučenia oprávnených osôb boli vypracované záznamy, ktoré tvorili súčasť osobného spisu každého zamestnanca. Poučenie oprávnených osôb bolo realizované aj napriek tomu, že zodpovedná osoba nevypracovala interný metodický pokyn pre poučenie oprávnených osôb.

FNsP Žilina nevypracovaním interného predpisu pre poučenie oprávnených osôb nekonala v súlade s bezpečnostnou smernicou, ktorou boli okrem iného upravené povinnosti

pri ochrane osobných údajov, čím nedodržala ustanovenie § 29 písm. b) výnosu 55/2014 Z. z., podľa ktorého štandardom pre riadenie informačnej bezpečnosti je zabezpečenie realizácie a dodržiavanie schválenej bezpečnostnej politiky.

Kontrolnej skupine bolo predložené poverenie na výkon dohľadu na dodržiavanie zákonných ustanovení pri spracúvaní osobných údajov, podľa ktorého v čase od 01.11.2005 do 30.06.2014 mala nemocnica poverenú zodpovednú osobu.

FNsP Žilina prevádzkovala ku dňu ukončenia výkonu kontroly 20 informačných systémov, v ktorých spracúvala osobné údaje[1]. Keďže nemocnica mala v kontrolovanom období zodpovednú osobu poverenú dohľadom nad ochranou osobných údajov, mala povinnosť v zmysle ustanovenia § 43 ods. 1 zákona č. 122/2013 Z. z. viesť evidenciu informačných systémov, ktoré nepodliehajú oznamovacej povinnosti alebo osobitnej registrácií.

Kontrolou evidencie informačných systémov bolo zistené, že nemocnica evidovala len päť informačných systémov[2] z celkového počtu 20 informačných systémov, ktoré podliehali evidencii.

Neevidovaním 15 informačných systémov[3] FNsP Žilina nepostupovala v súlade s ustanovením § 43 ods. 1 zákona č. 122/2013 Z. z.

V čase od 01.07.2014 do ukončenia výkonu kontroly nemala nemocnica zodpovednú osobu poverenú dohľadom nad ochranou osobných údajov. Z uvedeného dôvodu mala nemocnica oznamovaciu povinnosť voči Úradu na ochranu osobných údajov Slovenskej republiky (ďalej len „úrad na ochranu osobných údajov“) na všetky informačné systémy, v ktorých spracúvala osobné údaje s výnimkou informačných systémov, v ktorých sú spracúvané osobné údaje na základe zákona, priamo vykonateľného právne záväzného aktu Európskej únie alebo medzinárodnej zmluvy, ktorou je Slovenská republika viazaná.

FNsP Žilina úradu na ochranu osobných údajov neoznámila prevádzku žiadneho informačného systému spracúvajúceho osobné údaje, čím porušila ustanovenie § 34 ods. 1 zákona č. 122/2013 Z. z.

4. Prevádzka informačných systémov verejnej správy

Informačný systém FNsP Žilina (ďalej len „IS FNsP“) pozostával zo šiestich modulov, ktorých prevádzku zabezpečoval odbor informatiky:

- NIS MEDEA – komplexný nemocničný informačný systém pre lôžkové oddelenia, spoločné vyšetrovacie a liečebné zložky a ambulancie,
- FONS – modul pre vykazovanie činností/bodovanie pre zdravotné poisťovne, ktorý je prepojený s modulom NIS MEDEA,
- VEMA – modul pre spracovanie miezd, personalistiky a dochádzky,

[1] Personalistika a mzdy, Plánovanie a organizácia práce, Poskytovanie zdravotnej starostlivosti, Ekonomika – úhrada za poskytnutú zdravotnú starostlivosť, Ekonomika – všeobecná ekonomika, Plánovanie a organizácia dopravy a dopravných služieb, Ochrana osobných údajov, Knižnica, Registratúra, Civilná ochrana, Bezpečnosť a ochrana zdravia pri práci, Hospodárska mobilizácia, Majetok – evidencia, Stravovanie – zamestnanci, Nemocničná lekáreň (vnútorná), Kamerové systémy, Riadenie procesov, kvality a výkon auditu, Vybavovanie sťažností, žiadostí a petícií, Evidencia a ukladanie zmlúv, Verejné obstarávanie

[2] Poskytovanie zdravotnej starostlivosti, Hospodárska mobilizácia, Bezpečnosť a ochrana zdravia pri práci, Personalistika a mzdy, Ekonomika – úhrady za poskytnutú zdravotnú starostlivosť.

[3] Plánovanie a organizácia práce, Ekonomika – všeobecná ekonomika, Plánovanie a organizácia dopravy a dopravných služieb, Ochrana osobných údajov, Knižnica, Registratúra, Hospodárska mobilizácia, Majetok – evidencia, Stravovanie – zamestnanci, Nemocničná lekáreň (vnútorná), Riadenie procesov, kvality a výkon auditu, Vybavovanie sťažností, žiadostí a petícií, Evidencia a ukladanie zmlúv, Verejné obstarávanie, Kamerové systémy

- L.E.A. UAFALAN – ekonomický informačný systém na vedenie komplexnej agendy fakturácie a účtovníctva,
- HIS – hospodársky informačný systém, ktorý umožňoval sledovať hospodárenie jednotlivých nákladových stredísk nemocnice,
- IMA-DIM – analytická evidencia a odpisovanie dlhodobého hmotného a dlhodobého nehmotného investičného majetku a evidencia a spotreba drobného investičného majetku.

Činnosti súvisiace s prevádzkou IS FNsP uvedené v bezpečnostnej smernici boli definované aj v internom predpise odboru informatiky, ktorý okrem iného definoval:

- kľúčové komponenty IS FNsP,
- základné zásady bezpečnej prevádzky IS FNsP,
- zálohovanie údajov,
- preventívne opatrenia,
- práva a povinnosti užívateľov,
- prístupové heslá,
- práva a povinnosti vedúcich pracovníkov oddelení v oblasti bezpečnosti IS FNsP.

Interný predpis odboru informatiky nebol oficiálnym dokumentom nemocnice, t.j. nebol schválený vedením nemocnice ako smernica, ktorá by bola záväzná pre všetkých zamestnancov.

Z tohto dôvodu odporúčame FNsP Žilina zaviesť interný predpis odboru informatiky do systému riadenia kvality a schváliť ho vedením nemocnice ako smernicu.

Nepretržitú prevádzku jednotlivých modulov IS FNsP zabezpečoval odbor informatiky. V prípade havarijných situácií obnovu informačných systémov pre moduly L.E.A. UAFALAN, HIS a IMA-DIM realizoval odbor informatiky z prevádzkových (archivačných) záloh. Pre moduly NIS MEDEA, FONS a VEMA obnova databáz bola zabezpečená dodávateľsky na základe uzatvorených zmlúv.

Preverením štandardov pre informačné systémy verejnej správy pre oblasť zálohovania a archivovania nebol zistený nesúlad medzi požadovaným a skutočným stavom. Zálohovanie databáz pre jednotlivé moduly IS FNsP sa vykonávali v pravidelných intervaloch definovaných interným predpisom odboru informatiky. Zálohy boli archivované v uzamykateľných priestoroch odboru informatiky a taktiež v druhej budove gynekologicko-pôrodného a neonatologického oddelenia.

V oblasti aktualizácie IKT bolo zistené, že v Supervíznej zmluve č. ST201013 zo dňa 10.06.2010 v znení neskorších dodatkov, ktorou bola zabezpečená podpora prevádzky modulov NIS MEDEA a FONS treťou stranou, nebola zo strany dodávateľa určená osoba zodpovedná za informačnú bezpečnosť. Táto skutočnosť bola v rozpore s ustanovením § 42 písm. c) výnosu MF SR č. 55/2014 Z. z.

5. Bezpečnosť informačných systémov verejnej správy

Identifikácia používateľa a následná autentizácia pri vstupe do IS FNsP boli definované v bezpečnostnom projekte a následne zapracované aj v bezpečnostnej smernici. Politiku hesiel taktiež upravoval interný predpis odboru informatiky, podľa ktorého pre vstup do NIS MEDEA bolo potrebné zadať osobné číslo zamestnanca a heslo. Prístupové heslá

užívateľov museli mať minimálne osem znakov, užívateľ bol povinný svoje prístupové heslo meniť najmenej jeden krát za šesť mesiacov, prípadne častejšie na výzvu zamestnanca odboru informatiky.

Prístupové práva zamestnancov nemocnice do ISFNsP prideľoval, menil a odnímal poverený zamestnanec odboru informatiky na základe žiadosti vedúceho útvaru nemocnice, v ktorom zamestnanec pôsobil. Bol pritom rešpektovaný bezpečnostný princíp "najmenších privilégií" - zamestnanec mal pridelené len také privilégiá, ktoré potreboval pre plnenie svojich pracovných povinností, a nie vyššie. Zamestnanci odboru informatiky, poverení správou jednotlivých modulov IS FNsP, viedli evidenciu pridelených, zmenených a odňatých prístupových práv užívateľov jednotlivých modulov IS FNsP.

Vedúci zamestnanci nemocnice boli zodpovední za včasné podanie žiadosti o zrušenie, prípadne modifikáciu prístupových práv podriadených zamestnancov, ktorým končil pracovný pomer, resp. ktorým sa zmenilo pracovné zaradenie. Vedúci zamestnanci boli povinní rozhodnúť o súboroch podriadených zamestnancov, ktorým sa skončil pracovný pomer. Pokiaľ tak neurobili, vedúci odboru informatiky bol oprávnený tieto súbory považovať za nepotrebné a odstrániť ich.

Kontrolou bolo zistené, že odbor informatiky nebol súčasťou procesu ukončenia pracovného pomeru zamestnancov nemocnice, čím nebolo zabezpečené okamžité zrušenie ich prístupových práv do IS FNsP. Odbor informatiky zabezpečoval aktualizáciu používateľov IS FNsP tak, že v pravidelných intervaloch žiadal vedúcich zamestnancov oddelení nemocnice o predloženie zoznamov zamestnancov ich úsekov, ktoré následne porovnával s užívateľmi zavedenými v IS FNsP.

Z uvedeného dôvodu odporúčame FNsP Žilina, aby odbor informatiky zaradila do procesu skončenia pracovného pomeru zamestnancov nemocnice.

Prístup tretích strán do IS FNsP Žilina bol realizovaný na základe dvoch zmlúv, ktorými bola zabezpečená podpora prevádzky modulov NIS MEDEA, FONS a VEMA:

- Supervízna zmluva č. ST201013zo dňa 10.06.2010 v znení neskorších dodatkov,
- Licenčná zmluva č. 2/210/025/2003 zo dňa 24.01.2003 v znení neskorších dodatkov pre modul VEMA.

Kontrolou predložených zmlúv bolo zistené, že FNsP Žilina v týchto zmluvách neuviedla bezpečnostné požiadavky pre poskytovanie služieb vyplývajúcich z uvedených zmlúv, čo bolo v rozpore s ustanovením § 43 písm. b) výnosu MF SR č. 55/2014 Z. z.

Kľúčové komponenty v oblasti IKT (servre, aktívne prvky siete LAN, záložné zdroje,...) mala nemocnica umiestnené v priestoroch na to určených (serverovňa).
Serverovňa sa nachádzala na prízemí, pričom na oknách serverovne neboli namontované zábrany. Uvedená skutočnosť bola v rozpore s ustanovením § 35 písm. b) výnosu č. MF SR č. 55/2014 Z. z., podľa ktorého zabezpečený priestor má byť oddelený od ostatných priestorov fyzickými prostriedkami najmä stenami a zábranami.

Protokol o výsledku kontroly vypracovali dňa 27.11.2014

Ing. Juraj Podolák
vedúci kontrolnej skupiny

Mgr. Ľubica Grochalová dos Santos
členka kontrolnej skupiny

S obsahom protokolu o výsledku kontroly bol oboznámený dňa 28.11.2014

MUDr. Štefan Volák
riaditeľ nemocnice