ÚŘAD PRO OCHRANU OSOBNÍCH ÚDAJŮ
Pplk. Sochora 27, 170 00 Praha 7
tel.: 234 665 111, fax: 234 665 444
posta@uoou.cz, www.uoou.cz

Čj. UOOU-12026/17-14
Praha 2. května 2018

Protokol o kontrole

Kontrolní orgán:

Úřad pro ochranu osobních údajů, se sídlem Pplk. Sochora 27, 170 00 Praha 7, IČ 70837627, (dále jen „Úřad“).

Pravomoc kontrolního orgánu k výkonu kontroly vyplývá z § 2 odst. 2 a 3 a z § 29 odst. 1 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů.

Kontrolující:

Mgr. et. Mgr. Božena Čajková – inspektorka Úřadu, průkaz inspektora č. [redacted],

Mgr. Iva Tomášková – pověřená zaměstnankyně Úřadu, průkaz pověřeného zaměstnance č. [redacted],

Ing. Radek Loub – pověřený zaměstnanec Úřadu, průkaz pověřeného zaměstnance č. [redacted],

(dále jen „kontrolující“).

Kontrolovaná osoba:

Nemocnice [redacted], se sídlem [redacted], zastoupená [redacted], předsedou představenstva,

(dále jen „kontrolovaný“).

Předmět kontroly:

Předmětem kontroly je dodržování povinností správce osobních údajů stanovených zákonem č. 101/2000 Sb. v souvislosti se zpracováním osobních údajů subjektů údajů – pacientů kontrolovaného.

První kontrolní úkon:

Oznámení o zahájení kontroly čj. UOOU-12026/17-5, doručené kontrolovanému dne 11. ledna 2018.

Poslední kontrolní úkon:

Vyjádření kontrolovaného čj. UOOU-12026/17-13, doručené Úřadu dne 3. dubna 2018.

I. <u>Přehled podkladů:</u>

Protokol o kontrole se opírá o následující podklady a dokumenty, které byly pořízeny před zahájením kontroly a v jejím průběhu, popř. o dokumenty a skutečnosti, které jsou kontrolnímu orgánu známy z jeho úřední činnosti.

1. Podnět [redacted], čj. UOOU-12026/17-1, 1 list, s přílohami:
   a. Stížnost proti postupu poskytovatele při poskytování zdravotních služeb, 11 listů;
   b. Žádost o vyjádření a zaslání podkladů, 1 list;
   c. Záznam z místního šetření, 3 listy;
   d. Vyjádření kontrolovaného ze [redacted], 3 listy;
   e. Soupis nahlížení do zdravotní dokumentace [redacted], 1 list;
   f. Směrnice – Elektronická zdravotnická dokumentace, 4 listy;
   g. Sdělení Krajského úřadu ze [redacted], 1 list;
   h. Sdělení kontrolovaného ze [redacted], 1 list;
   i. Sdělení kontrolovaného ze [redacted], 2 listy;
   j. Sdělení kontrolovaného ze [redacted], 5 listů;
   k. Emailová komunikace ze [redacted], 1 list;
   l. Emailová komunikace [redacted], 2 listy.
2. Protokol z ústního jednání ze dne 24. ledna 2017, čj. UOOU-12026/17-6, 2 listy, s přílohami:
   a. Podnět [redacted], 1 list;
   b. Souhlas se zněním protokolu, 1 list.
3. Vyjádření kontrolovaného, doručené Úřadu dne 12. února 2018, čj. UOOU-12026/17-7, 7 listů, s přílohami:
   a. Vnitřní předpis – Bezpečnost informačních a komunikačních technologií, včetně prezenčních listin, 25 listů;
   b. Vnitřní předpisy – Ochrana osobních údajů, Elektronická zdravotnická dokumentace, včetně prezenčních listin, 12 listů;

c. Vnitřní předpis – Informace o zdravotním stavu pacienta, nahlížení, výpisy a kopie zdravotnické dokumentace, Podíl pacientů a jejich blízkých na zdravotní péči, Mlčenlivost zdravotnického pracovníka, včetně prezenčních listin, 12 listů;
d. Interní bezpečnostní audit [redacted], 8 listů.

4. Vyjádření kontrolovaného – potvrzení o absolvování elektronického školení [redacted], doručené Úřadu dne 12. února 2018, čj. UOOU-12026/17-8, 22 listů, s přílohami:
   a. Pracovní smlouvy a náplně zaměstnanců, 16 listů;
   b. Vnitřní předpis – Sledování spokojenosti pacientů, Postup při vyřizování stížností, pochval, 4 listy;
   c. Přístupy ke zdravotnické dokumentaci stěžovatelky [redacted], 2 listy;
   d. Záznam z ústního jednání – pokusný pacient, 2 listy;
   e. Záznam z ústního jednání – pokusný pacient (historie editace záznamu, historie pacienta v okně ambulance), 2 listy;
   f. Záznam z ústního jednání – PrintScreen – pokusný pacient (změna, smazání), 4 listy.
5. Protokol z ústního jednání a místního šetření ze dne 15. března 2018, čj. UOOU-12026/17-12, 2 listy, s přílohami:
   a. Žádost [redacted] o zaslání podkladů, 1 list;
   b. Souhlas se zněním protokolu, 2 listy.
6. Vyjádření kontrolovaného, doručené Úřadu dne 3. dubna 2018, čj. UOOU-12026/17-13, 1 list, s přílohami:
   a. PrintScreen – číselník - důvod nahlížení do EZD [redacted], 1 list;
   b. Popis opatření zakládajícího nutnost zadání důvodu práce s elektronickou zdravotnickou dokumentací pacienta, 1 list;
   c. Odpověď kontrolovaného na žádost [redacted], 3 listy;
   d. Příkaz předsedy představenstva k mimořádné kontrole používání uživatelských práv a k rozšíření auditu ze [redacted], 2 listy.

II. <u>Kontrolní zjištění:</u>

Kontrola byla zahájena na základě podnětu [redacted] (dále jen [redacted] ze dne [redacted]. Podezření [redacted] na porušení zákona č. 101/2000 Sb. vyplynulo z jeho šetření ve věci poskytování zdravotních služeb dle zákona č. 372/2011 Sb., o zdravotních službách a podmínkách jejich poskytování, ve znění pozdějších předpisů. [redacted] konkrétně poukázal na možné nahlížení a pozměňování obsahu v elektronické zdravotnické dokumentaci (dále jen „EZD“) pacientky (stěžovatelky) neoprávněnými osobami. Při vyřizování uvedené stížnosti [redacted] od kontrolovaného vyžádal výpisy z nemocničního informačního systému (dále jen „NIS“), které dokládají nahlížení do EZD pacientky prostřednictvím aplikačního software NIS [redacted] a aktivitu jednotlivých osob ve vztahu k EZD stěžovatelky.

Vzhledem k tomu, že stěžovatelka dle svého tvrzení nebyla ošetřována jinde než na oddělení [redacted], vzbudily dle [redacted] předložené záznamy a z nich vyplývající vstupy [redacted], [redacted] a [redacted] (za období od roku [redacted] podezření na porušení povinností při zpracovávání osobních údajů stěžovatelky.

Kontrolní zjištění č. 1.

Kontrolující předně posuzovali, zda informace, které kontrolovaný v souvislosti s vedením zdravotnické dokumentace (dále jen „ZD“) pacientů zpracovává, jsou osobními údaji, případně citlivými údaji ve smyslu § 4 písm. a) a b) zákona č. 101/2000 Sb., podle kterých se osobním údajem rozumí *„jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu“.* Citlivým údajem je potom *„osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, členství v odborových organizacích, náboženství a filozofickém přesvědčení, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektu údajů a genetický údaj subjektu údajů; citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů“.*

Dále bylo zjišťováno, zda kontrolovaný s osobními, příp. citlivými údaji, které zpracovává v souvislosti s vedením ZD pacientů, nakládá tak, že toto jeho jednání lze posoudit jako zpracování osobních údajů podle § 4 písm. e) zákona č. 101/2000 Sb., podle kterého je zpracováním osobních údajů *„jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Zpracováním se rozumí zejména shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace“.*

Kontrolovaný vede ZD pacientů na základě zákona č. 372/2011 Sb., přičemž v § 53 odst. 1 tohoto zákona je ZD definována tak, že se jedná o soubor informací vztahujících se ke konkrétnímu pacientovi. Rozsah zdravotnické dokumentace je pak vymezen v odst. 2 citovaného ustanovení, a to tak, že s ohledem na účel vedení zdravotnické dokumentace jsou jejím obsahem zejména identifikační údaje pacienta, kterými jsou jméno, příjmení, datum narození, rodné číslo, příp. číslo pojištěnce veřejného zdravotního pojištění a adresa místa trvalého pobytu. ZD dále obsahuje informace o zdravotním stavu pacienta, o průběhu a výsledku poskytovaných zdravotních služeb a o dalších významných okolnostech souvisejících se zdravotním stavem pacienta a s postupem při poskytování zdravotních služeb.

Základním kritériem pro posouzení toho, zda je určitá informace osobním údajem či nikoli, je možnost zjištění identity fyzické osoby na základě dané informace či s její pomocí. Osobním údajem je tedy každá informace, pokud je osoba, která touto informací disponuje, schopna přiřadit ji ke konkrétní fyzické osobě.

Vzhledem k výše uvedeným údajům, které kontrolovaný v souvislosti s vedením ZD shromažďuje, kontrolující konstatují, že kontrolovaný je schopen identifikovat jednotlivé pacienty, jejichž ZD je povinen na základě zákona č. 372/2011 Sb. vést.

Jak bylo řečeno výše, kromě identifikačních údajů jsou obsahem ZD také informace o zdravotním stavu pacienta, přičemž tyto informace jsou uvedeny v zákoně č. 101/2000 Sb. ve výčtu citlivých údajů.

Kontrolující na základě výše uvedeného konstatují, že kontrolovaný zpracovává **osobní a citlivé údaje** ve smyslu § 4 písm. a) a b) zákona č. 101/2000 Sb.

Zákon č. 372/2011 Sb. dále upravuje povinnosti kontrolovaného při vedení ZD, tj. požadavky na přesnost a aktuálnost záznamů, nakládání se zdravotnickou dokumentací v případě zániku oprávnění k poskytování zdravotních služeb nebo zániku poskytovatele zdravotnických služeb jako takového a dále také podmínky pro nahlížení do zdravotnické dokumentace a pořizování výpisů nebo kopií. Kontrolovaný proto uvedené osobní a citlivé údaje zejména shromažďuje, ukládá na nosiče informací, dále uchovává, doplňuje, zpřístupňuje a likviduje.

Popsané úkony kontrolovaného s osobními a citlivými údaji naplňují definici **zpracování osobních údajů** dle § 4 písm. e) zákona č. 101/2000 Sb.

Kontrolní zjištění č. 2.

Kontrolující následně posoudili postavení kontrolovaného ve vztahu k § 4 písm. j) zákona č. 101/2000 Sb., tedy zda je správcem osobních údajů zpracovávaných v ZD pacientů, přičemž správcem osobních údajů je dle citovaného ustanovení *„každý subjekt, který určuje účel a prostředky zpracování osobních údajů, provádí zpracování a odpovídá za něj“.*

Kontrolovaný je [redacted] a mezi jejíž primární činnosti patří komplexní poskytování zdravotnických služeb. Kontrolovaný je tak poskytovatelem zdravotních služeb ve smyslu § 2 odst. 1 zákona č. 372/2011 Sb.

Kontrolovaný vede ZD pacientů na základě zákona č. 372/2011 Sb., který stanoví účel, způsob a prostředky tohoto zpracování. Vedení ZD ve stanoveném rozsahu a stanovenými prostředky je tak povinností kontrolovaného.

V obdobných případech se má dle Úřadu za to, že správce osobních údajů byl určen zvláštním zákonem, kterým je mu předmětné zpracování uloženo, v tomto případě i včetně prostředků a způsobů zpracování.

Kontrolující s ohledem na výše uvedené konstatují, že kontrolovaný je v postavení **správce osobních údajů** podle § 4 písm. j) zákona č. 101/2000 Sb., neboť účel, způsob a prostředky předmětného zpracování osobních údajů mu byly stanoveny zvláštními právními předpisy, kontrolovaný toto zpracování provádí a odpovídá za něj.

Kontrolní zjištění č. 3.

S ohledem na předchozí kontrolní zjištění kontrolující dále hodnotili, zda je pro zpracování osobních a citlivých údajů v souvislosti s vedením ZD pacientů kontrolovaného dán právní titul, jak je požadován v § 5 odst. 2 a ve vztahu k citlivým údajům v § 9 zákona č. 101/2000 Sb. (obě citovaná ustanovení shodně jako primární právní titul uvádí souhlas subjektu údajů, resp. výslovný souhlas se zpracováním citlivých údajů, a dále taxativně vymezují situace, kdy lze zpracování realizovat i bez souhlasu).

Jak bylo uvedeno již výše, kontrolovaný vede ZD pacientů, neboť je to jeho povinností podle zákona č. 372/2011 Sb. Kontrolovaný tak postupuje v souladu s § 5 odst. 2 písm. a) zákona č. 101/2000 Sb., neboť předmětné zpracování osobních údajů realizuje za účelem splnění své právní povinnosti.

Právním titulem pro zpracování citlivých údajů (informací o zdravotním stavu pacientů) je pak poskytování zdravotních služeb podle zvláštního zákona ve smyslu § 9 písm. c) zákona č. 101/2000 Sb.

Kontrolující konstatují, že kontrolovaný v obecné rovině **splnil** požadavky § 5 odst. 2 a § 9 zákona č. 101/2000 Sb., neboť osobní a citlivé údaje pacientů v ZD zpracovává na základě zákonem předpokládaných právních titulů.

S ohledem na zaměření této kontroly se kontrolující blíže nezabývali dalšími parametry předmětného zpracování osobních údajů, které kontrolovanému vyplývají zejména z § 5 odst. 1 zákona č. 101/2000 Sb. (v kombinaci s příslušnými právními předpisy upravujícími povinný rozsah ZD a dobu jejího uchování).

Kontrolní zjištění č. 4.

S ohledem na obsah podnětu, na jehož základě je kontrola vedena, se kontrolující zaměřili na to, zda a do jaké míry kontrolovaný plní povinnosti spojené se zajištěním bezpečnosti osobních a citlivých údajů zpracovávaných v ZD pacientů, jak je jeho povinností podle § 13 odst. 1 až 4 zákona č.101/2000 Sb. Současně bylo hodnoceno plnění souvisejících povinností, které vyplývají zaměstnancům kontrolovaného na základě § 14 citovaného zákona.

Při hodnocení plnění povinností kontrolovaného v oblasti zabezpečení osobních údajů se kontrolující zaměřili na následující aspekty:

1. <u>Úroveň zabezpečení osobních údajů (fyzické zabezpečení, zabezpečení EZD a NIS)</u>

Dle § 54 odst. 1 zákona č. 372/2011 Sb. může být ZD vedena v listinné nebo elektronické podobě nebo v kombinaci obou těchto podob.

Kontrolovaný zpracovává ZD jak v listinné podobě, tak elektronicky (EZD). ZD v listinné podobě [redacted] (podklad č. 3).

Způsob vedení EZD je u kontrolovaného upraven ve Směrnici Elektronická zdravotnická dokumentace (podklad č. 1f). Na základě této směrnice je základním NIS [redacted]. Určená pracoviště kontrolovaného dále využívají tyto NIS:

- [redacted]
- [redacted]
- [redacted]
- [redacted]

Ze shromážděných podkladů (podklady č. 1j, 1f, 2, 3, 5) vyplývají následující zjištění:

Lékařům je v rámci [redacted] umožněno nahlížet do EZD všech pacientů kontrolovaného. Důvodem takto nastaveného přístupu je dle kontrolovaného zejména řádné zajištění poskytování zdravotních služeb na náležité odborné úrovni, včetně zajištění případné návaznosti poskytované péče, neboť nelze předem predikovat okruh osob (lékařů), které budou v budoucnu z legitimních důvodů potřebovat nahlédnout do EZD pacienta.

Uživatelé se přihlašují do [redacted] pod svým přístupovým jménem a heslem, které jim přiděluje administrátor [redacted]. Bezprostředně po prvním přihlášení je pak každý uživatel povinen změnit heslo a dále jej užívat tak, aby nedošlo k jeho zpřístupnění. [redacted]

V případě nečinnosti uživatele dojde [redacted] k automatickému odhlášení a pro další práci v [redacted] je vyžadováno opětovné přihlášení.

Rozsah údajů, ke kterým může přihlášený uživatel přistupovat, se odvíjí od zastávané funkce či pozice v organizační struktuře kontrolovaného (vedoucí pracovník či řadový lékař) a od specializace lékaře (příslušnosti k určitému oddělení). Některé části EZD jsou zpřístupněny pouze lékařům a zdravotnickým pracovníkům oddělení, na kterém je pacient ošetřován.

[redacted]

2. Technicko-organizační opatření k zajištění ochrany osobních údajů

Pravidla pro vedení ZD jsou obecně stanovena v § 53 a násl. zákona č. 372/2011 Sb. Za účelem zajištění ochrany osobních a citlivých údajů pacientů přijal dále kontrolovaný technicko-organizační opatření, která zdokumentoval ve vnitřních předpisech, a to zejména:

- Směrnice – Elektronická zdravotnická dokumentace (podklad č. 1f), kterou kontrolovaný upravil způsob vedení EZD, povinnosti uživatelů (zaměstnanců kontrolovaného) při práci s NIS za účelem zajištění bezpečnosti a integrity dat, včetně pravidelných kontrol přístupových oprávnění do NIS;

- Směrnice – Bezpečnost informačních a komunikačních technologií (podklad č. 3a), která obsahuje opatření k zajištění důvěrnosti, dostupnosti a integrity informací vytvářených, zpracovávaných, ukládaných, přenášených, zálohovaných a archivovaných v prostředcích informačně komunikačních technologií kontrolovaného;

- Směrnice – Informace o zdravotním stavu pacienta, nahlížení, výpisy a kopie ZD, podíl pacientů a jejich blízkých na zdravotní péči, mlčenlivost zdravotnického pracovníka (podklad č. 3c), ve které je upraven postup při předávání informací o zdravotním stavu pacientů, nahlížení do ZD a pořizování kopií, mlčenlivost zdravotnických pracovníků;

- Směrnice – Sledování spokojenosti pacientů, postup při vyřizování stížností, pochval (podklad č. 4b), kterou kontrolovaný upravil vyřizování připomínek občanů, stížností a pochval;

- Směrnice – Ochrana osobních údajů (podklad č. 3b), která obsahuje pravidla pro zachování důvěrnosti a utajení dat a informací a ochranu osobních údajů pacientů a zaměstnanců kontrolovaného.

3. Logování

Vzhledem k tomu, že v [redacted] dochází k automatizovanému zpracování osobních a citlivých údajů pacientů, se kontrolující dále zaměřili na skutečnost, zda kontrolovaný pořizuje elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje v EZD pacientů zaznamenány nebo jinak zpracovány (tzv. logy), jak je jeho povinností dle § 13 odst. 4 písm. c) zákona č. 101/2000 Sb.

Kontrolou bylo zjištěno, že práce s EZD pacientů je zaznamenána v logu, z něhož je patrné, kdo a kdy k EZD přistupoval. Součástí logu je také obecný důvod tohoto přístupu (příjem z oddělení, práce s dokumentací, přesun na propuštění, viz podklad č. 1e). V některých případech však odůvodnění nahlížení do EZD není uvedeno vůbec. Z toho vyplývá, že práce s EZD je v [redacted] umožněna i v situaci, kdy uživatel žádný důvod svého přístupu k EZD neuvede. Toto zjištění bylo ověřeno i v rámci kontrolního šetření, kdy při práci s EZD nebylo uvedení důvodu vyžadováno (podklad č. 2).

4. Kontrolní mechanismy

Kontrolující dále zjišťovali, jakým způsobem je u kontrolovaného zjišťováno, zda odpovědní zaměstnanci dodržují interní předpisy v oblasti ochrany osobních údajů, neboť důsledná interní kontrola, včetně případného vyvození odpovědnosti konkrétních zaměstnanců, je nedílnou součástí opatření, která je každý správce osobních údajů povinen přijmout na základě § 13 odst. 1 zákona č. 101/2000 Sb.

Kontrolou bylo zjištěno, že vedoucí pracovníci oddělení jsou oprávněni provádět namátkové kontroly dodržování povinností v oblasti zajištění bezpečnosti přístupu k ZD/EZD. Dalším nástrojem kontroly je dále kontrola vykázaných dokladů (podklad č. 3).

V [redacted] byl u kontrolovaného proveden interní bezpečnostní audit, jehož předmětem byla mimo jiné úroveň zabezpečení prostor, v nichž dochází k práci se ZD na jednotlivých odděleních, a přihlašování a odhlašování zaměstnanců z PC. Obě tyto oblasti byly vyhodnoceny jako zcela splněné (viz podklad č. 3d).

Kontrolovaný plánuje další namátkovou kontrolu dodržování bezpečnostních opatření v průběhu [redacted] (po proškolení zaměstnanců ve vztahu k obecnému nařízení o ochraně osobních údajů a kybernetické bezpečnosti, podklad č. 3).

Kontrolovaný nicméně neprovádí pravidelné kontroly zaměřené na přístupy k EZD za pomoci logů (tj. ověření oprávnění práce s EZD zaznamenané v logu ve vztahu k reální náplni práce daného zaměstnance v daném okamžiku či období).

5. Proškolování zaměstnanců

Kontrolující se zabývali i tím, jakým způsobem jsou zaměstnanci kontrolovaného seznamováni s interními předpisy, které upravují jejich povinnosti v oblasti ochrany osobních údajů. Seznámení s povinnostmi v této oblasti, stejně jako pravidelné (opakované) proškolení je opět nedílnou součástí opatření, která je kontrolovaný povinen vyhodnotit a v přiměřené míře přijmout na základě § 13 odst. 1 zákona č. 101/2000 Sb.

Kontrolou bylo zjištěno, že zaměstnanci jsou s výše popsanými interními předpisy seznámeni, což stvrzují podpisem na prezenční listině konkrétního předpisu (viz podklady č. 3a, 3b, 3c, 4b).

Dále jsou proškolováni v oblasti systému řízení bezpečnosti informací [redacted], jehož cílem je zabránit neoprávněnému nakládání s informacemi ve všech jejich formách a zajistit jejich dostupnost a integritu nezbytnou k poskytování komplexní zdravotní péče (podklad č. 4).

Shrnutí

Kontrolující konstatují, že kontrolovaný přijal pouze některá z opatření, která je jako správce osobních údajů je povinen na základě § 13 zákona č. 101/2000 Sb. aplikovat. Nedostatky byly shledány zejména v případě nastavení přístupu k EZD.

K nastavení rozsahu přístupových oprávnění uživatelů informačních systémů kontrolující obecně konstatují, že na základě zákona č. 101/2000 Sb. je povinností správce každého

informačního systému (jehož obsahem jsou osobní údaje) definovat pro každou roli/ funkci nezbytný rozsah přístupu a současně zajistit, že daný uživatel nebude mít přístup k osobním údajům, které pro výkon své činnosti nepotřebuje.

Kontrolující jsou toho názoru, že v obecné rovině platí výše uvedené východisko pro veškeré správce osobních údajů, tedy i zdravotnická zařízení. Je jistě organizačně i technicky možné nastavit přístupová oprávnění tak, aby byl pracovníkům zařazeným na určité oddělení umožněn přístup pouze k osobním údajům pacienta, který je zde skutečně ošetřován.

Úřadu nicméně nepřísluší s ohledem na rozsah jeho zákonných kompetencí hodnotit, zda je pro řádný výkon zdravotnické péče nezbytný způsob nastavení přístupových oprávnění, jaký zvolil kontrolovaný [redacted]. V takové situaci je však povinností kontrolovaného přijmout jiná opatření, která zajistí splnění požadavků zákona č. 101/2000 Sb. v oblasti rozsahu přístupových oprávnění jednotlivých osob, které se podílí na zpracování osobních údajů.

Dle kontrolujících patří mezi základní opatření v uvedeném smyslu závazné interní předpisy, auditní záznamy (logy) umožňující dohledat identitu konkrétní osoby a podrobnosti ohledně její činnosti s osobními údaji a v neposlední řadě i důsledná kontrolní činnost. Co se týče rozsahu logů, pak je nutno odkázat na výše citovanou zákonnou povinnost upravenou v § 13 odst. 4 písm. c) zákona č. 101/2000 Sb. Ke kontrolní činnosti je pak třeba uvést, že pro řádné zajištění povinnosti zabezpečit zpracovávané osobní údaje mají být odpovědní zaměstnanci nejen seznámeni se svými povinnostmi, ale musí si být současně vědomi toho, že dodržování stanovených požadavků je předmětem pravidelných kontrol, jejichž závěry se případně projeví i v pracovně právní oblasti. V rámci kontrol lze pak pracovat právě i s auditními záznamy (tj. ověřit reálnou existenci důvodu práce s EZD zaznamenanou v logu).

Kontrolou bylo zjištěno, že kontrolovaný přijal, jako hlavní nástroje pro zajištění ochrany osobních a citlivých údajů, interní předpisy upravující zásady a oprávnění zaměstnanců při práci s EZD (resp. veškeré interní předpisy upravující bezpečnostní opatření ve vztahu k informacím). Zaměstnanci kontrolovaného jsou s obsahem těchto předpisů seznámeni, přičemž dodržování stanovených postupů je jejich pracovně právní povinností.

Z logů, které kontrolovaný pořizuje v rámci NIS, je možné dohledat čas přístupu a osobu přistupující k EZD, nikoli však dostatečně konkrétní důvod tohoto přístupu. Logování v tomto rozsahu proto není dostatečné pro naplnění zákonné povinnosti dle § 13 odst. 4 písm. c) zákona č. 101/2000 Sb., resp. zamýšleného významu logů. To je patrné také ze skutečnosti, že kontrolovaný nebyl schopen doložit popis a odůvodnění přístupů k EZD stěžovatelky za požadované období (viz Kontrolní zjištění č. 5.), neboť uvedení této informace (důvodu nahlížení do EZD) nebylo při práci v [redacted] konkrétně vyžadováno.

Ohledně interní kontroly plnění povinností stanovených zaměstnancům kontrolovaného bylo zjištěno, že tyto kontroly byly zaměřeny (v souvislosti se zabezpečením osobních a citlivých údajů) na fyzické uložení a zabezpečení ZD a přihlašování a odhlašování zaměstnanců z PC (viz podklad č. 3d). Kontrola logů z hlediska oprávněnosti přístupů k ZD pacientů u kontrolovaného nebyla provedena. Kontrolovaný by nicméně (s ohledem na popsanou absenci některých informací v logu [redacted] ani v rámci takové kontroly nemohl účinně kontrolovat plnění

povinnosti stanovené ve Směrnici Elektronická zdravotnická dokumentace, tedy zákazu přistupovat k EZD pacientů, kteří nejsou ošetřováni na oddělení, na kterém lékař působí.

Z výše uvedených důvodů kontrolující konstatují, že kontrolovaný **porušil** povinnosti, které mu v souvislosti se zabezpečením osobních údajů vyplývají z § 13 odst. 1 zákona č. 101/2000 Sb., neboť auditní záznamy (logy) pořizované v [redacted] v rámci přístupů do EZD pacientů neumožňují určit a ověřit, z jakého důvodu bylo k EZD přistupováno. Kontrolovaný dále neprováděl pravidelné kontroly přístupů k EZD, které (při stávajícím nastavení NISA) představují účinný prostředek pro dodržování povinností vyplývajících zaměstnancům z přijatých interních předpisů.

K tomu kontrolující dále doplňují, že v průběhu kontroly kontrolovaný systém [redacted] upravil. Do pracovního postupu tzv. vkládání pacienta do okna bylo předřazeno okno s povolenými variantami přístupu a uživatel je povinen vybrat důvod práce s EZD pacienta (podklady č. 6a a 6b).

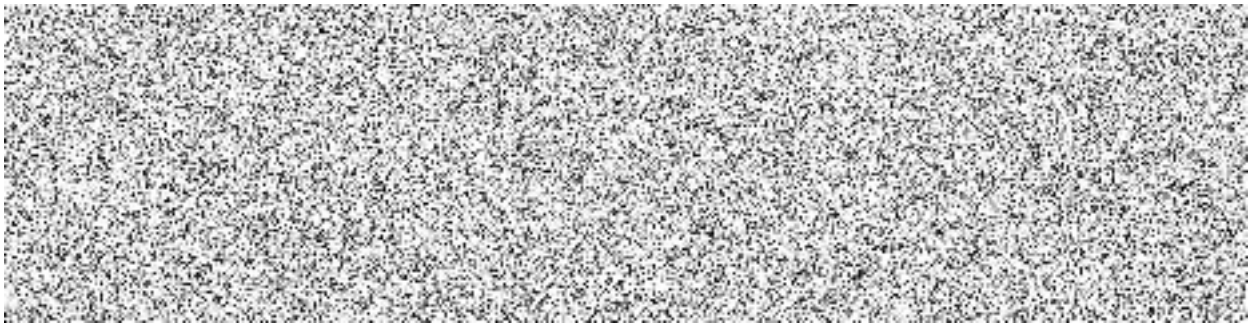
S účinností od [redacted] byl dále vydán Příkaz předsedy představenstva k mimořádné kontrole používání uživatelských práv a k rozšíření auditu, jehož předmětem je provedení namátkových kontrol a vytvoření systému pro provádění pravidelných kontrol logů (podklad č. 6d).

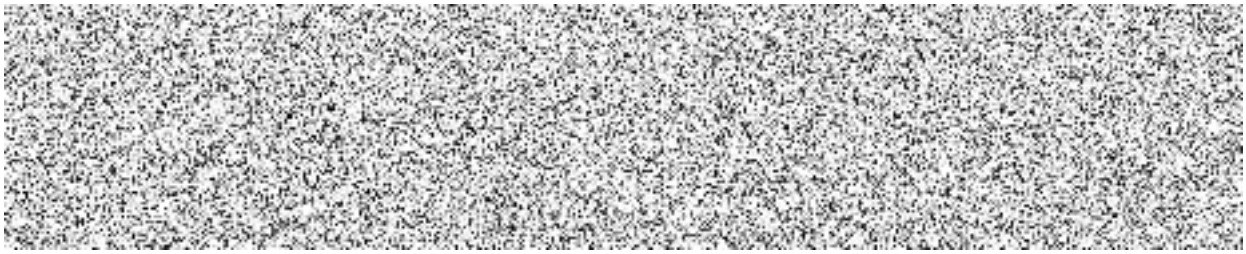
Kontrolovaný dále (na základě vyhodnocení stížnosti) připravuje propojení NISA s personálním informačním systémem (konkrétně propojení systému docházky se systémem logování) tak, že dokud zaměstnanec nebude evidován v docházkovém systému, nebude se moci přihlásit do [redacted]. Kontrolovaný také připravuje propojení [redacted] a proškolování zaměstnanců v rámci e-learningu - pokud zaměstnanec školení neabsolvuje, budou mu omezena přístupová oprávnění do [redacted] (podklad č. 3).

Kontrolní zjištění č. 5.

Kontrolující se dále zaměřili na zpracování osobních údajů stěžovatelky, tedy na údajné neoprávněné přístupy do EZD pacientky (stěžovatelky), včetně akcí „změna“ či „smazání“ zapsaných v logu z těchto přístupů.

V této souvislosti byla kontrolujícím při místních šetřeních demonstrována ukázka práce v NIS z pohledu lékaře (podklady č. 2 a 5). Z těchto ukázek a dalších podkladů vyplývá následující:



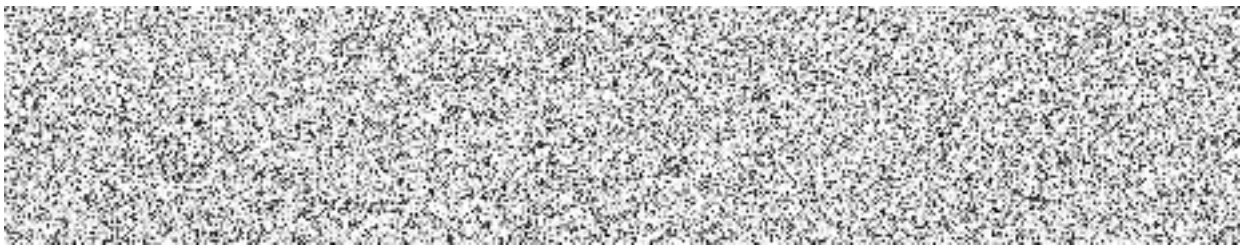


Kontrolující si dále vyžádali výpis přístupů k EZD stěžovatelky v době od [redacted], a to včetně popisu jednotlivých přístupů (kdo a kdy přistupoval, důvody přístupu, činnost s EZD).

Ve svém vyjádření (podklad č. 3) kontrolovaný zaslal popis jednotlivých přístupů k EZD stěžovatelky [redacted]. K tomu dále uvedl, že již není možné detailně prověřit jednotlivé přístupy za celé požadované období, neboť vzhledem k velkému časovému rozestupu si jednotliví lékaři již nejsou vědomi, zda k EZD stěžovatelky přistupovali, příp. z jakého důvodu.

Z uvedeného přehledu vyplývá, že k EZD pacientky dne [redacted] přistupovali zaměstnanci kontrolovaného (5 lékařů a 2 zdravotní sestry). Všichni tito zaměstnanci mají oprávnění k přístupu do [redacted] v rámci plnění svých pracovních povinností (viz také podklad č. 4a).

Dne [redacted] pak dle kontrolovaného (na základě vyjádření jednotlivých lékařů) došlo pravděpodobně k situaci, kdy se lékařka „překlikla“ a přidala EZD stěžovatelky do okna svého oddělení namísto skutečně vyhledávaného pacienta (např. z důvodu podobného příjmení či rodného čísla). Lékařka pak již s EZD stěžovatelky dále nepracovala a stěžovatelka zůstala zařazena mezi pacienty tohoto oddělení po celý den. [redacted]



Kontrolující s ohledem na uvedené konstatují, že výše popsaná zjištění dokládají a doplňují závěr kontrolního zjištění č. 4, tedy že nastavení přístupových oprávnění k [redacted] nelze považovat za odpovídající požadavkům v § 13 zákona č. 101/2000 Sb. Kontrolovaný, jako správce osobních údajů, neměl v důsledku tohoto nastavení (v kombinaci s absencí některých informací v logu) možnost ověřit a zkontrolovat oprávnění zaměstnanců přistupovat k EZD pacientů. Nemohl tedy zjistit a ověřit, zda se tak v případě stěžovatelky stalo pouze v důsledku pochybení zaměstnanců („překliknutí“) anebo v důsledku porušení zákazu nahlížet na pacienty, kteří nejsou v péči daného oddělení.

Kontrolovaný dále uvedl, že dne [redacted] nahlédla do EZD stěžovatelky zdravotní sestra pod přístupovými údaji lékaře, čímž se dopustila porušení pracovní kázně. Z hlediska zákona

č. 101/2000 Sb. tak porušila § 14 tohoto zákona, podle kterého je povinností zaměstnanců zpracovávat osobní údaje pouze za podmínek a v rozsahu stanoveném kontrolovaným jakožto správcem osobních údajů. Porušení § 14 zákona č. 101/2000 Sb. nicméně není přestupkem dle zákona č. 101/2000 Sb. a Úřad ho neprojednává. Projednání pochybení v této oblasti (pokud nenaplní skutkovou podstatu přestupku dle jiného zákona či trestného činu) je tak v působnosti správce. Kontrolovaný z tohoto pochybení zaměstnankyně vyvodil důsledky v rovině pracovněprávní (podklad č. 3).

Kontrolní zjištění č. 6.

Vzhledem k tvrzení stěžovatelky v řízení před [redacted] (viz podklad č. 1a), že informace o podané stížnosti byly známy také neoprávněným osobám (zaměstnancům kontrolovaného), se kontrolující zaměřili i na postup kontrolovaného při vyřizování stížností, včetně dodržování povinnosti mlčenlivosti zaměstnanců ohledně osobních údajů, které kontrolovaný v rámci této agendy zpracovává.

Obdobně jako v případě ZD je kontrolovaný i při vyřizování stížností a žádostí pacientů v postavení správce osobních údajů dle § 4 písm. j) zákona č. 101/2000 Sb., přičemž tyto osobní a případně i citlivé údaje zpracovává z titulu poskytovatele zdravotních služeb, v souladu s postupy upravenými v zákoně č. 372/2011 Sb.

K tvrzení stěžovatelky, že po podání předmětné stížnosti byla vystavena psychickému tlaku ze strany svých kolegů (lékařů), neboť zaměstnanci vyřizující stížnost údajně porušili povinnost mlčenlivosti a s obsahem stížnosti seznámili i neoprávněné osoby, kontrolovaný uvedl, že žádného porušení si není vědom (podklady č. 2 a 3).

Dle vyjádření kontrolovaného (podklad č. 3) nebyl obsah předmětné stížnosti zpřístupněn neoprávněným zaměstnancům. Vzhledem ke skutečnosti, že obsahem stížnosti byla nespokojenost stěžovatelky se zdravotními službami poskytovanými v souvislosti s porodem, byla stížnost zaslána k vyjádření dotčeným lékařům, aby bylo možné záležitost náležitě prošetřit. Jednalo se tak o standardní postup, kdy byl obsah stížnosti zpřístupněn pouze zainteresovaným osobám.

Na základě § 51 zákona č. 372/2011 Sb. jsou zaměstnanci kontrolovaného vázáni mlčenlivostí o všech skutečnostech, o kterých se dozvěděli v souvislosti s výkonem práce. Tato povinnost je u kontrolovaného dále zvlášť upravena v pracovní smlouvě (viz podklad č. 4a) a trvá i po skončení pracovního poměru.

Pravidla pro vyřizování stížností proti postupu poskytovatele zdravotních služeb obecně upravuje § 93 a násl. zákona č. 372/2011 Sb. Kontrolovaný dále upřesnil postup pro vyřizování stížností ve směrnici Sledování spokojenosti pacientů, postup při vyřizování stížností, pochval (podklad č. 4b). Na základě této směrnice je vyřizováním stížností pověřen člen představenstva kontrolovaného, který je v rámci šetření stížnosti oprávněn přizvat si ke spolupráci další zaměstnance kontrolovaného, příp. též sestavit 3 nebo 5ti člennou radu odborníků (mimo stěžovaného a osoby zainteresované na stížnosti).

Případné zpřístupnění či zveřejnění informací z obsahu stížnosti (de facto i samotné existence předmětné stížnosti) ze strany zaměstnanců kontrolovaného oprávněných stížnost vyřizovat by bylo nutné posuzovat jako porušení povinnosti mlčenlivosti dle § 15 zákona č. 101/2000 Sb., za které by odpovídal konkrétní zaměstnanec.

V daném případě ovšem nebylo zjištěno a prokázáno, že by se s obsahem stížnosti seznámili jiní zaměstnanci kontrolovaného, než kteří byli dle zákonných i interních předpisů v posuzované věci zainteresováni. Ostatně tvrzení stěžovatelky v tomto směru je pouze obecné, neuvádí, kteří zaměstnanci kontrolovaného měli s informacemi disponovat, případně v jakém rozsahu jim byl obsah stížnosti znám, ani jak s nimi měli nakládat.

Výše uvedené lze shrnout tak, že kontrolovaný přijal pravidla pro postup při vyřizování stížností pacientů a jeho zaměstnanci jsou při výkonu zdravotní péče vázáni povinností mlčenlivosti. V souvislosti s vyřízením předmětné stížnosti tedy **nebylo zjištěno porušení** žádné povinnosti stanovené zákonem č. 101/2000 Sb.

III. <u>Poučení o opravném prostředku:</u>

Proti kontrolnímu zjištění uvedenému v protokolu o kontrole může kontrolovaná osoba podat kontrolnímu orgánu ve lhůtě 15 dnů ode dne doručení protokolu o kontrole námitky. Námitky se podávají písemně, musí z nich být zřejmé, proti jakému kontrolnímu zjištění směřují, a musí obsahovat odůvodnění nesouhlasu s tímto kontrolním zjištěním.

Pokud kontrolující inspektor nevyhoví námitkám ve lhůtě 7 dnů ode dne jejich doručení, vyřídí je předsedkyně Úřadu ve lhůtě 30 dnů ode dne jejich doručení.

Podpisová doložka:

Mgr. et Mgr. Božena Čajková	inspektorka	……..
titul jméno příjmení	funkce	podpis
Mgr. Iva Tomášková	pověřený zaměstnanec Úřadu	……..
titul jméno příjmení	funkce	podpis
Ing. Radek Loub	pověřený zaměstnanec Úřadu	……..
titul jméno příjmení	funkce	podpis