DOI: 10.35191/MEDSOFT_2018_1_30_120_124


# DEFINICE SOUKROMÍ PACIENTA V ELEKTRONICKÝCH ZDRAVOTNÍCH ZÁZNAMECH

**Marek Mateják, Libor Seidl, Michal Potůček**

## Anotace

Elektronizace zdravotnictví je trend, který se už nedá zastavit. Výhody automatického zpracování a poskytování zdravotních záznamů často zastiňuje fakt, že se jedná i o údaje osobní a citlivé. Tedy jejich zpracování a sdílení by mělo být řízeno zabezpečeně, a to výhradně akceptováním všech souhlasů od pacienta = vlastníka těchto zdravotních dat. V neposlední řadě by pro každou podezřelou operaci nad účtem pacienta nebo s jeho osobními a citlivými údaji mělo být vždy možné zjistit čas a identitu přistupujícího uživatele.

## Klíčová slova

*pacientský souhlas, citlivé osobní zdravotní údaje, sdílení zdravotních záznamů, elektronické zdravotní záznamy*

## 1 Úvod

Definic, které je možné vztahovat na soukromí pacienta ve sdílených elektronických zdravotních záznamech, je spousta. Dovolíme si citovat některé z nich:

"Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě." Listina základních práv a svobod (článek 10, sekce 3). [1]

"Soukromí je ta sféra života člověka, do které nikdo včetně státu nesmí bez souhlasu člověka nebo bez výslovného dovolení zákona zasahovat ani o ni požadovat či získávat informace, a o které subjekt soukromí není povinen nikomu (ani státnímu orgánu) informace dávat, pokud mu to zákon neukládá. Člověk se soukromí může zříkat v momentě, kdy ho někomu dobrovolně zpřístupní, např. že o něm podá informaci. Přičemž soukromí přirozeně nezahrnuje to, co se odehrává na veřejnosti (př. účast hráče ve veřejně provozované hře)." Ústava a ústavní řád České republiky. [2]

"Každý občan tedy bude mít právo vědět a být informován zejména o tom, za jakým účelem se osobní údaje zpracovávají – znát období, po které budou údaje uchovávány, znát příjemce jeho osobních údajů, vědět, v čem spočívá logika automatizovaného zpracování osobních údajů a jaké mohou být důsledky takového zpracování přinejmenším v případech, kdy je zpracování založeno na profilování." Evropské obecné nařízení o ochraně osobních údajů (GDPR). [3]

Osobní údaje a jejich nakládání řeší také zákon č. 101/2000 Sb., o ochraně osobních údajů (dále jenom Zákon). V praxi se o dodržování tohoto zákona stará „Úřad pro ochranu osobních údajů se sídlem v Praze" pověřený tímto samotným zákonem. Od konce května 2018 bude platit také nařízení Evropského parlamentu a Rady (EU) 2016/679 (GDPR).

Obecně lze říct, že soukromí pacienta v elektronických zdravotních záznamech je tedy možné definovat jako ochranu jeho osobních a citlivých údajů. Pro bližší zkoumání je nutné tyto pojmy dobře definovat.

Zákon v §4a) definuje osobní údaje jako:

„Osobním údajem se 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," [4]

Dále Zákon §4b) definuje i citlivý osobní údaj jako

„Citlivým údajem se rozumí 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" [4]

Což znamená, že každý citlivý údaj je zároveň údajem osobním. Z hlediska informací se údajem myslí spíše skupina jednoho nebo více atributů. Do kategorie osobních údajů tak spadají všechny kombinace atributů, které lze považovat za klíč pro vyhledání konkrétní osoby. Tímto klíčem můžou být i biometrická data jako jsou otisky prstů, fotka obličeje, hlasový záznam atd., které se dnes běžně používají pro vyhledání osob. Osobním údajem je však i interní identifikátor v každém systému, který sám o sobě žádné informace o dané osobě neposkytuje.

Co není osobním údajem je údajem anonymním. Bohužel v praxi je tato černobílá definice ne vždy použitelná. Problémové jsou případy, kdy není možné na základě typů dat určit, zda je daná skupina atributů anonymním údajem nebo osobním údajem. Řešením může být správná a striktní strukturovanost údajů takovým způsobem, aby umožňovala v dostatečné míře definovat neklíčové atributy za každých okolností tak, aby mohli být považovány vždy za anonymní při oddělení od zbytku dat.

Bohužel česká legislativa v některých specifických případech umožňuje zpracování i sdílení osobních i citlivých dat i bez souhlasů subjektů osobních údajů, např. § 9 v Zákoně. Odstrašující případ nastal právě minulý rok, když se podařilo schválit novelu o Národním kontaktním místě pro elektronické zdravotnictví, která umožňuje sdílet citlivá zdravotní data nejenom bez souhlasu pacienta ale dokonce i bez toho, aby zaručovala dohledatelnost konkrétní nahlížející osoby. Jedná se o sedmou část senátního tisku ST153 z roku 2017, a to konkrétně o následující sekci:

„§ 69a Národní kontaktní místo pro elektronické zdravotnictví

(1) Národní kontaktní místo pro elektronické zdravotnictví je informační systém veřejné správy, který umožňuje oprávněným osobám nahlížet do zdravotnické dokumentace vedené v elektronické podobě.

(2) Oprávněnými osobami podle odstavce 1 jsou

a) poskytovatelé a poskytovatelé sociálních služeb, v případě, že poskytují zdravotní služby,

b) poskytovatelé zdravotnické záchranné služby a

c) národní kontaktní místa pro elektronické zdravotnictví zřízená ostatními členskými státy Evropské unie " [5].

V podstatě to znamená, že soukromí pacienta v zdravotních záznamech je zákonem chráněno jen částečně, protože zdravotničtí pracovníci i pracovníci „národních kontaktních míst" můžou mít možnost nahlížet na osobní data pacientů i bez jejich souhlasů.

Přitom je vždy možné i vhodné, aby pacient uděloval souhlas při vzniku nebo při přístupu na jeho osobní údaje. Souhlas může být přímo součástí těchto dat u správce dat, který tyto data zpracovává a sdílí. Nebo v případě, že se jedná o obecný souhlas, tak může být i na jiném nezávislém místě, kde ho může pacient definovat a odkud ho může nahlížející bezpečně použít. V určitých případech je dokonce možné udělovat i jednorázový omezený komunikační souhlas na nahlížení na osobní data přímo na místě, a to dokonce i pasivně při bezvědomí pacienta např. použitím elektronické občanky pacienta [6].

DOI: 10.35191/MEDSOFT_2018_1_30_120_124


## 2 Pacientské souhlasy k přístupům k osobním i citlivým údajům

Jedním ze souhlasů k nahlížení na data pacienta je souhlas se zastoupením. Tento souhlas mají automaticky rodiče nezletilých dětí. Bez něho by na tyto data nemohli nahlížet. I navzdory tomu, že se jedná o situaci velmi běžnou v praxi, tak v elektronických záznamech je to poněkud složitější. **Přidělování zákonných zástupců** je možné přes souhlas v účtu pacienta, kterému je přidáván daný zákonný zástupce. Tato na první pohled zbytečná operace je však nutná na zpřístupnění dat v účtu jiné osoby. Je to srovnatelné se souhlasem s dalšími disponenty účtu v elektronickém bankovnictví.

Souhlas s **nahlížením na osobní údaje pacienta** se může vázat na roli a specializaci zdravotnického pracovníka. Vždy by však měla být dohledatelná jak identita nahlížející osoby, tak to že se opravdu jedná o záchranáře, praktického lékaře, zubaře, gynekologa, pediatra nebo jiného specializovaného zdravotnického pracovníka při ošetřovaní pacienta. Souhlas by se tak vždy v elektronických záznamech měl přímo vázat na internetovou identitu přistupujícího uživatele. O identitu na internetu by se měli starat tzv. autorizační autority. V tomto případě však nepostačuje jednoduchá identita přistupujícího uživatele, ale je nutné mít i jeho role a specializace ve zdravotnictví definované na takové úrovni, jak podrobně mají být dané souhlasy specifikovatelné. **Přihlášením zdravotnického pracovníka u autorizační autority** by tedy měla být zaručena jeho identita role i specializace ve zdravotnictví v dostatečném rozsahu pro vyhodnocení pacientských souhlasů na jednotlivé operace s osobními i citlivými údaji. Nové trendy v elektronických zdravotních záznamech směrují na přeshraniční poskytování zdravotní péče založené na sdílení zdravotních dat definovaných pomocí mezinárodně uznávaných kódů nemocí (MKN-10), kódů pro vyšetření a laboratorní výsledky (LOINC) nebo rozsáhlých číselníků a klasifikací snažících se uchopit vše ve zdravotnictví (SNOMED CT). Tím by měl být zaručen automatický překlad odborných termínů do široké škály světových jazyků. Lékař v jiného státu nejenže může mít možnost se podívat do zdravotní dokumentace cizince, ale zároveň je možné mu danou dokumentaci alespoň částečně poskytnout v jeho jazyce. Souhlas pacienta by mohl být založený jenom na určitém stupni důvěry v cizí autorizační autority. Podobný princip už na internetu funguje v každém internetovém prohlížeči při navazováním důvěry s navštívenou internetovou doménou. Protokol HTTPS musí zohledňovat autorizační autoritu, která certifikáty pro danou doménu podepsala. Dalším příkladem pro využití důvěry institucí v garantování totožnosti a role uživatele v systému je EDUROAM [7], který umožňuje mezinárodně potvrzovat výzkumným a vzdělávacím institucím identitu svých studentů a zaměstnanců. Logicky právě poskytování identity zdravotnického pracovníka s rolemi a specializacemi ve zdravotnictví by měl být cíl Národního kontaktního místa pro elektronické zdravotnictví. Přihlášením by zdravotnický pracovník získal identitu, kterou by mohl využít každý správce zdravotních dat při posouzení, zda povolit přístup na pacientova data dle jeho vlastních souhlasů. Obecně je však možné systém vyvinout i bez centrální autorizační autority a to tak, že by autorizačními autoritami byli přímo poskytovatelé zdravotních služeb, kteří znají identitu, roli a specializaci svých zdravotnických pracovníků nejlépe.

Zápis nových osobních údajů pacienta zdravotnickým pracovníkem do systému správce dat by měl být také propojen **se souhlasem se zpracováním osobních údajů**, který by měl daný pacient udělit správci dat.

Souhlas může tedy nejen specifikovat uživatele, ale i operaci s daty. Běžně je však žádoucí, aby každý zdravotnický pracovník mohl zapisovat pacientům data. Taky je žádoucí, aby si jednotlivé záznamy uživatelé nemohli navzájem libovolně měnit. Vzhledem k tomu, že odbornost autora by měla mít zásadní vliv na důvěryhodnost a váhu záznamu, tak se nedoporučuje, aby si záznamy od specializovaných zdravotnických pracovníků mohl pacient editovat. Oprava záznamu by měla být umožněna jenom autorovi záznamu. Pacientovi by však mělo být umožněno omezit souhlas na nahlížení na dané záznamy. Dle GDPR musí mít pacient také právo být zapomenut, co může vést k tomu, že se pacientům umožní jednotlivé záznamy i mazat.

## 3 Elementární operace s osobními i citlivými údaji

Z pohledu souhlasů je nejdůležitější operace **nahlížení** na osobní údaje různých definovaných typů.

**Vytvoření** nových osobních údajů pacienta by mělo být vždy propojeno se souhlasem se zpracováním osobních údajů, který by měl mít daný správce dat od daného pacienta.

**Modifikace** osobních údajů pacienta je nutné pro možnosti editace chyb a oprav v záznamech – typicky jenom autorem daných dat.

**Mazání** osobních údajů pacienta je vhodné také povolit pro specifické opravy v záznamech dělané autorem nebo dokonce i vlastníkem daných dat.

## 4 Přístupy na osobní i citlivé údaje

Pro detailnější určení typu přístupu bohužel nestačí jenom znát identitu a roli přistupujícího uživatele. Přístup k záznamu je určen i vlastnostmi daného záznamu a souhlasů od pacienta, které se daného typu záznamu týkají. Typ přístupu je možné definovat jako množinu rolí přístupu. Elementární operaci s daným záznamem je možné uskutečnit pouze tehdy jeli povolena alespoň jednou rolí v daném typu přístupu. Příkladem pro role přístupů k osobním údajům pacienta ve vztahu k operaci nahlížení v elektronických zdravotních záznamech je Tabulka 1.

| | Role přístupu | Právo nahlížet |
|---|---|---|
| 1 | Autor dat | Autorství údajů |
| 2 | Vlastník dat | Vlastnictví údajů |
| 3 | Nahlížející zákonný zástupce | Potvrzení žádosti o zástup v nahlížení |
| 4 | Zapisující zákonný zástupce | Potvrzení žádosti o zástup v zapisovaní |
| 5 | Nahlížející záchranář | Souhlas s nahlížením na data pro pracovníky záchranné služby |
| 6 | Nahlížení povoleného zdravotnického pracovníka | „Souhlas s nahlížením na daný záznam pro specifikované zdravotnické pracovníky“ |
| 7 | Zapisující zdravotnický pracovník | Na základě této role přístupu není umožněno nahlížet na data. Pro nahlížení je nutno mít zároveň jinou roli přístupu. |
| 8 | Nahlížení dle komunikačního souhlasu | Vlastník musí poskytnout komunikační kód pro nahlížení na své zdravotní záznamy. |
| 9 | Zápis dle komunikačního souhlasu | Vlastník musí poskytnout komunikační kód pro zápis do svých zdravotních záznamů. |
| 10 | Správce kontaktních údajů | „Souhlasu se zpracováním kontaktních údajů správcem dat“ nebo komunikační souhlas od pacienta pro správu kontaktních dat. |

DOI: 10.35191/MEDSOFT_2018_1_30_120_124


| | Role přístupu | Právo nahlížet |
|---|---|---|
| 11 | Správce zdravotních údajů | „Souhlasu se zpracováním zdravotních údajů správcem dat" nebo komunikační souhlas od pacienta pro správu zdravotních dat. |
| 12 | Správce oprávnění a souhlasů | „Souhlasu se zpracováním zdravotních údajů správcem dat" nebo komunikační souhlas od pacienta pro změnu jeho souhlasů a oprávnění. |
| 13 | Správce veřejných dat | Na základě této role přístupu není umožněno nahlížet na osobní nebo citlivé údaje pacientů. |
| 14 | Odesílání záznamu do registrovaného poskytovatele zdravotních služeb | Adresováním osobních a citlivých údajů poskytovateli zdravotních služeb vlastníkem záznamu je udělen automatický souhlas zástupcům dané organizace na tyto data nahlížet. |
| 15 | Přijímání záznamu od registrovaného poskytovatele zdravotních služeb | Na základě této role přístupu není umožněno nahlížet na data. Pro nahlížení je nutno mít zároveň jinou roli přístupu. |
| 16 | Veřejné nahlížení na veřejná data | Na základě této role přístupu není umožněno nahlížet na osobní nebo citlivé údaje pacientů. Slouží jen pro data, která jsou veřejná. |

*Tabulka 1 – Role přístupů nahlížejícího uživatele k záznamům pacienta*

Speciálním případem je vytvoření dat při přístupu autor. Tuto variantu je nutné důkladně ošetřit, protože při vytváření dat je autorem vždy ten, kdo je vytváří. To znamená, že při neošetření takovéto podmínky by teoreticky mohlo dojít i k umožnění vytvářet data každému uživateli systému. To je samozřejmě nežádoucí, a proto by měl mít přístup autora vždy zakázanou operaci vytváření záznamů.

## 5 Identita přistupujícího uživatele k osobním i citlivým údajům

Sdílení osobních a citlivých dat by mělo vždy umožňovat zjistit identitu každého uživatele, který na data přistupuje. Proto je nutné všechny uživatele systému autorizovat ověřením jejich identity ještě předtím, než se s nimi začnou sdílet nějaké osobní nebo citlivé údaje na základě souhlasů. Online registrace, ověření telefonu nebo emailu bohužel identitu uživatele neověřuje, proto jsou nutné další kroky, kterých výsledkem je potvrzení, že se účet v systému patří konkrétní osobě s případnou konkrétní rolí, či dokonce specializací ve zdravotnictví. Typicky je vhodné rozlišit role jako zdravotnický pracovník, pracovník záchranné služby, lékař, farmaceut, vědec, laborant, operátor dané organizace atd. Pro efektivnější běh systému je možné do identity přihlášeného uživatele vkládat i tvrzení jako je jeho odbornost a specializace ve zdravotnictví (např. použitím Seznamu odborností podle vyhlášky MZ ČR č. 134/1998 Sb.); identifikace poskytovatele zdravotních služeb, pod kterou přistupuje; komunikační souhlas od pacienta (jednorázový dočasný klíč, který pacient vygeneroval danému uživateli) atd

## 6 Komunikační souhlas od vlastníka dat

Souhlas s nahlížením na data nemusí být vždy definován předem. V mnohých situacích je možné souhlas udělit přímo na místě. Tento komunikační souhlas je možné dosáhnout vzdáleným generováním jednorázových časově omezených datových klíčů, které můžou být spojeny buď s daty pacienta nebo s účtem přistupujícího. Jiným typem komunikačního souhlasu může být také umožnění použití fyzického klíče v osobním vlastnictví daného pacienta, např. čipové karty, USB-klíč, aplikace s privátním klíčem v mobilu atd.

## 7 Oprávnění a souhlasy u zdravotních záznamů

Každý zdravotní záznam by měl mít jednoznačně určeného autora, organizaci autora, vlastníka, zákonné zástupce vlastníka pro nahlížení a pro zápis, souhlasy s nahlížením, souhlasy se spravováním u správce dat atd. Ideálně by měl mít také tabulku práv pro jednotlivé operace s daty pro jednotlivé přístupy. Tuto tabulku je např. možné reprezentovat pomocí 64-bitové masky v případě, že se jedná o 16 typů přístupu (autor, vlastník, záchranář, …) pro 4 operace nad daty (nahlížej, vytvoř, modifikuj, zmaž). Databázové prostředí dokonce umožňují v podmínkách dotazů definovat i bitové operace, což umožňuje kontroly práv integrovat takovým způsobem, aby se při daném přístupu skutečně nepracovalo s daty, na které nemá přistupující právo.

## 8 Rozpad práv pod úrovní zdravotního záznamu

Některé atributy v entitách zdravotních záznamů je vhodné z hlediska práv na jednotlivé operace více omezit. Jedná se například o jednoznačné identifikátory, které nesmí mít hodnotu vyskytující se již pro jiný záznam. Toho lze dosáhnout jednoduše na úrovni databáze definováním jednoznačného indexu, který v případě nejednoznačnosti vrací chybu při vkládání nebo modifikaci záznamu.

Mohou být také definovány atributy, které je možné modifikovat i jiným zdravotnickým pracovníkem než autorem. A to například atributy definující současný stav daného zdravotního záznamu, tj. jestli je diagnóza / medikace / léčba / hospitalizace již aktivní / ukončená / neplatná atd. I když lékař nemůže modifikovat záznamy jiných lékařů, tak umožněním modifikace těchto vybraných atributů je možné efektivně uvést zdravotní dokumentaci do aktuálního konzistentního stavu.

## 9 Dotaz na existenci osobních nebo citlivých údajů

Na první pohled neškodný dotaz na osobní nebo citlivé údaje, jehož odpovědí je jenom jestli EXISTUJE / NEEXISTUJE v systému, může skrývat vážné bezpečnostní riziko. Pokud by se takový dotaz bez omezení umožnil veřejně, tak je možné hrubou silou zkoušet různé kombinace a tímto způsobem lze nepřímo získat i informace, na které není umožněno přímo nahlížet. Proto je vhodné dotazy tohoto typu patřičně zabezpečit nebo dokonce postavit na úroveň nahlížení na takto dotazovaná data.

## 10 Logování přístupů na osobní a citlivé údaje

Robustní systém logování sice sám o sobě nezabrání neoprávněným přístupům na osobní údaje, ale v takovém případě umožňuje zjištění, kdo a kdy neoprávněně přistupoval. Měl by tedy subjektům osobních údajů umožnit dopátrání se identity uživatelů, který na data přistupovali. Přehled přístupů na data tak vytváří důvěru mezi správcem a vlastníkem dat, dle které může pacient coby vlastník svých osobních údajů sdílet svá zdravotní data napříč široce dostupnou zdravotní péčí.

DOI: 10.35191/MEDSOFT_2018_1_30_120_124


| | Role přístupu | Příklad logování přístupů |
|---|---|---|
| 1 | Autor dat | Přihlášení a odhlášení uživatele do/ze systému je nutné logovat vždy. Mělo by se také logovat zmazání dat jejich autorem a případně i jejich modifikace. |
| 2 | Vlastník dat | Přihlášení, odhlášení, změnu práv a souhlasů je nutné logovat vždy. Je možné logovat také mazání dat i modifikaci dat, v případě, že je vlastníkovy umožněna. |
| 3 | Nahlížející zákonný zástupce | Nahlížení zákonného zástupce stejně jako nahlížení vlastníka dat není potřeba logovat u každého zdravotního záznamu. |
| 4 | Zapisující zákonný zástupce | Je možné logovat mazání dat i modifikaci dat, v případě, že je zákonnému zástupci vlastníka umožněna. |
| 5 | Nahlížející záchranář | Je nutné logovat nahlížení na zdravotní záznam pracovníkem záchranný služby. |
| 6 | Nahlížení povoleného zdravotnického pracovníka | Je nutné v logovat nahlížení na zdravotní záznam zdravotnickým pracovníkem. |
| 7 | Zapisující zdravotnický pracovník | Je možné logovat vytvoření zdravotního záznamu registrovaným zdravotnickým pracovníkem. |
| 8 | Nahlížení dle komunikačního souhlasu | Je nutné logovat použití komunikačního souhlasu i nahlížení na zdravotní záznam dle komunikačního souhlasu na nahlížení. |
| 9 | Zápis dle komunikačního souhlasu | Je možné logovat zápis zdravotní záznam dle komunikačního souhlasu na zápis. |
| 10 | Správce kontaktních údajů | Nahlížení, vytvoření, modifikace i zmazání osobních či zdravotných dat správcem dat by mělo být logované vždy, pokud je to umožněno. |
| 11 | Správce zdravotních údajů | Nahlížení, vytvoření, modifikace i zmazání osobních či zdravotných dat správcem dat by mělo být logované vždy, pokud je to umožněno. |
| 12 | Správce oprávnění a souhlasů | Změnu práv a souhlasů správcem dat je nutné logovat vždy, pokud je to umožněno. |
| 13 | Správce veřejných dat | Administraci veřejných dat není potřeba uvádět do uživatelských logů pacientů. |
| 14 | Odesílání záznamu do registrovaného poskytovatele zdravotních služeb | Adresování zdravotního záznamu registrovanému poskytovateli zdravotních služeb je nutné logovat. |
| 15 | Přijímání záznamu od registrovaného poskytovatele zdravotních služeb | Změnu a zmazání dat registrovaným poskytovatelem zdravotních služeb je vždy nutné logovat. Vytvoření dat touto cestou je možné taky logovat. |
| 16 | Veřejné nahlížení na veřejná data | Nahlížení na veřejné data není potřeba logovat. |

*Tabulka 2 – Příklad nastavení logování dle rolí přístupu uživatele k záznamu pacienta*

Z důvodu ochrany osobních údajů zaznamenaných logováním by se měla dostupnost záznamu v logu přístupů na osobní údaj omezit jenom na subjekt daného osobního údaje.

Z hlediska výkonu není vhodné logovat podrobně úplně všechny operace, protože samotné logování tak může mít vyšší nároky než správa samotných dat. Kromě vybraných náhledů, vytváření, modifikace a mazání by se však určitě měli logovat operace typu přihlášení uživatele do systému, změna souhlasů a oprávnění, potvrzení provozního řádu systému atd. Obvyklý postup je, že formu i rozsah logování si určuje sám správce dat. Teoreticky je možné to ponechat i na vlastníkovi dat, kde např. bitovou maskou je možné nadefinovat při kterém typu přístupu a při které operaci se udělá zápis do logu. Logy z principu nemůžou být modifikovatelné, což je v mnohých případech zabezpečeno již na hardwarové úrovni. Existuje tak řešení, které neumožňuje ani privilegovaným účtům správců dat po sobě zamést stopy při neoprávněném nahlížení na data pomocí standardních služeb systému.

## 11 Diskuze

Elektronické zpracování zdravotních dat může nejen usnadnit skladování a poskytování zdravotních záznamů ošetřujícím lékařům. Je to taky klíč k personalizované medicíně, která může umožnit téměř automaticky řešit interakci i dávkování léků, a to dokonce i v závislosti na genetickém profilu pacienta [8]. Zpracování dat může být umožněno použitím simulačních modelů [9–12] vybudovaných využitím sofistikovaných softwarových knižnic [13–17]. Příkladem může být i využití přepočtů přenosu krevních plynů [18–19] na základě naměřených dat u pacienta v různých stavech a diagnózách [20–21]. To vše však vyžaduje nejenom vhodnou formalizaci dat a jejich relací [22], ale zároveň možnosti jak s danými daty pracovat bez toho aby se jakkoli narušilo soukromí pacienta definované jeho souhlasy. Celý systém elektronických zdravotních záznamů [23] je přitom dokonce možné vytvořit tak, aby nemohl být zneužit k vyšším cílům ani samotnými správci dat [24].

## Literatura

[1.] ČESKÁ REPUBLIKA. „Listina základních práv a svobod." In Sbírka zákonů, Česká republika. 1992, roč. 1993, částka 1, usnesení předsednictva České národní rady č. 2. Dostupné z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=22426. ISSN 1211-1244, článek 10, sekce 3

[2.] V. Pavlíček, „Ústava a ústavní řád České republiky": komentář. 2. díl., Práva a svobody. 2. dopl. a podstatně rozšíř. vyd. Praha: Linde, 2003. 1164 s. Zákony – komentáře. s. 113

[3.] Evropská Unie, „General Data Protection Regulation", popis, 2017, Dostupné z: https://www.gdpr.cz/gdpr/prava/

[4.] ČESKÁ REPUBLIKA. Zákon č. 101/2000 Sb., o ochraně osobních údajů, In: Sbírka zákonů České republiky, 2015. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/.

[5.] ČESKÁ REPUBLIKA. "Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci", 2017, změna §69a v 372/2011 Sb., o zdravotních službách, Dostupné z: http://www.senat.cz/xqw/webdav/pssenat/original/84517/70927

DOI: 10.35191/MEDSOFT_2018_1_30_120_124


*[6.] J. Prusa, „E-identity: Basic building block of e-Government," in IST--Africa Conference, 2015, 2015, pp. 1–10.*

*[7.] M. Sánchez, G. López, O. Cánovas, and A. F. Gómez-Skarmeta, „A proposal for extending the eduroam infrastructure with authorization mechanisms," in 5th International Workshop on Security in Information Systems (submitted 2007).*

*[8.] M. Mateják, J. Potůček, and J. Douša, „Genetic Data of Patient in Pharmacology," International Journal on Biomedicine and Healthcare, vol. 4, pp. 46–49, 2016.*

*[9.] M. Mateják and J. Kofranek, „Physiomodel-an integrative physiology in Modelica," in Engineering in Medicine and Biology Society (EMBC), 2015 37th Annual International Conference of the IEEE, 2015, pp. 1464–1467.*

*[10.] M. Mateják and J. Kofránek, „Rozsáhlý model fyziologických regulací v Modelice," presented at the Medsoft 2010, 2010.*

*[11.] M. Mateják and J. Kofránek, „HumMod – Golem Edition – Rozsáhlý model fyziologických systémů," presented at the Medsoft 2011, 2011.*

*[12.] M. Mateják, J. Kofránek, and J. Rusz, „Akauzální" vzkříšení" Guytonova diagramu," presented at the Medsoft 2009, 2009.*

*[13.] M. Mateják, F. Ježek, M. Tribula, and J. Kofránek, „Physiolibrary 2.3-An Intuitive Tool for Integrative Physiology," IFAC-PapersOnLine, vol. 48, pp. 699–700, 2015.*

*[14.] M. Mateják, T. Kulhánek, J. Šilar, P. Privitzer, F. Ježek, and J. Kofránek, „Physiolibrary – Modelica library for Physiology," presented at the 10th International Modelica Conference, Lund, Sweden, 2014.*

*[15.] M. Mateják, M. Tribula, F. Ježek, and J. Kofránek, „Free Modelica Library of Chemical and Electrochemical Processes," in 11th International Modelica Conference, Versailles, France, 2015, pp. 359–366.*

*[16.] M. Mateják, „Physiolibrary – fyziológia v Modelice," presented at the Medsoft 2014, 2014.*

*[17.] M. Mateják, „Physiology in Modelica," MEFANET Journal, vol. 2, pp. 10–14, 2014.*

*[18.] M. Mateják, „Adairove viazanie O2, CO2 a H+ na hemoglobín „ presented at the Medsoft 2015, 2015.*

*[19.] M. Mateják, T. Kulhánek, and S. Matoušek, „Adair-based hemoglobin equilibrium with oxygen, carbon dioxide and hydrogen ion activity," Scandinavian Journal of Clinical & Laboratory Investigation, pp. 1–8, 2015.*

*[20.] M. Mateják, B. Nedvědová, A. Doležalová, J. Kofránek, and T. Kulhánek, „Model ECMO oxygenátoru," presented at the Medsoft 2012, 2012.*

*[21.] M. Mateják, „Simulovanie ketoacidózy," presented at the Medsoft 2013, 2013.*

*[22.] M. Mateják, „Formalization of Integrative Physiology," Charles University in Prague, 2015.*

*[23.] M.Mateják, J. Potůček, J. Kofránek, „Nová generácia elektronických zdravotných záznamov" presented at the Medsoft 2016, 2016.*

*[24.] J. Kofránek, O. Felix, and J. Polák, „Jak informatizovat zdravotnictví a nevytvořit přitom velkého bratra," Sborník MEDSOFT 2013, 55, vol. 63, 2013.*

**Kontakty:**

**Marek Mateják**

**Libor Seidl**

**Michal Potůček**

Institut pro podporu elektronizace zdravotnictví z.ú.
Českomoravská 2408/1a Praha – Libeň
PSČ 190 00