NAPOJENÍ ZDRAVOTNICKÝCH SYSTÉMŮ NA ZÁKLADNÍ REGISTRY VEŘEJNÉ SPRÁVY: OCHRANA A KONTROLOVANÉ SDÍLENÍ OSOBNÍCH DAT

Jiří Kofránek, Ondřej Felix, Jiří Polák, Jiří Borej

Abstrakt

Propojení zdravotnických informačních systémů na základní registry veřejné správy umožní chránit i kontrolovaně sdílet citlivá osobní data. V článku je popsán princip tohoto propojení, které umožní nahrazení rodného čísla jako klíče k citlivým datům sadou tzv. agendových identifikátorů fyzické osoby (AIFO klíčů). Tím se zajistí bezpečnost citlivých dat a umožní se jejich kontrolované sdílení. Je zdůrazněna důležitost mezioborové spolupráce lékařů – informatiků a legislativců při budování informačních systémů veřejné správy.

Klíčová slova

ehealth, eGovernment, ochrana dat, základní registry, zdravotnické informační systémy

1 Úvod – sdílet a chránit

Zdravotnictví patří k oborům založeným na týmové spolupráci zdravotnického personálu. To vyžaduje oběh značného množství sdílených informací uvnitř nemocnic a poliklinik (vedení chorobopisu, indikovaná terapie, výsledky laboratorních a konziliárních vyšetření atd.) tak i mezi jednotlivými zdravotnickými zařízeními (lékařské zprávy, recepty, žádanky a výsledky vyšetření, záznamy do nejrůznějších specializovaných zdravotnických registrů aj.) i mimo zdravotnictví (lékařské informace, které dostává v písemné či elektronické formě pacient, nejrůznější zdravotnické výkazy pro statistiku, výkazy pro pojišťovny, ekonomické ukazatele aj.). Oběh elektronických dokumentů vyžaduje zabezpečit kompatibilitu přenášených dat. Zároveň se ale jedná o **sdílení vysoce citlivých osobních dat, které kladou vysoké požadavky na jejich ochranu** [2].

Pokud jsou tyto informace předávány a uchovávány v bezpečném síťovém prostředí nemocničních informačních systémů, je ochrana osobních dat zajištěna vlastním síťovým prostředím nemocnice a o zabezpečení kompatibility ukládaných a přenášených formátů dat se stará výrobce příslušného nemocničního informačního systému.

Složitější situace vzniká v případě, kdy chceme zdravotnické (a příslušné návazné ekonomické) informace přenášet mimo toto prostředí. Pak je kompatibilita datových formátů a především **ochrana citlivých osobních dat** ve zdravotnických informačních systémech nezbytnou podmínkou jejich funkčnosti. Proto například není možné sdílet lékařské informace na webových serverech bez zabezpečení ochrany před neoprávněným přístupem.

S problematikou sdílení a zároveň bezpečné ochrany dat se setkáváme např. v internetovém bankovnictví – bankovní účet chceme mít přístupný přes internet, zároveň ho chceme dostatečně chránit. K tomu, abychom se do spravování svého účtu dostali, potřebujeme v internetovém bankovnictví ověřit svoji identitu a s ní spojená práva k ovládání bankovního účtu – v závislosti na internetovém bankovnictví k tomu používáme různé prostředky – (pin, čipovou kartu, mobilní telefon apod.). Představa, že k ověření naši identity k účtu v bance by v internetovém bankovnictví stačilo rodné číslo, je absurdní – hrozba zneužití by zřejmě byla neadekvátně vysoká. Ve zdravotnictví je však rodné číslo dosud často používaným identifikátorem pro přístup k údajům ve zdravotnických databázích.

Program, který s námi v internetovém bankovnictví komunikuje – se v informatické hantýrce nazývá „front office", celé složitá struktura asistenčních služeb, která na pozadí ověřuje naši identitu, nastavuje práva k účtu a podle nich zprostředkuje nástroje k manipulaci s účtem, se nazývá „back office".

Obdobně, ve zdravotnických informačních systémech za nejrůznějšími „front office" programy komunikujícími s lékaři a dalšími zdravotnickými pracovníky stojí na pozadí „back office" – asistenční služby, které zařizují ověření identity a podle přístupových práv bezpečnou manipulaci s daty. Je zřejmé, že obdobně jako v internetovém bankovnictví, ve zdravotnických informačních systémech rodné číslo jako univerzální identifikátor do budoucna nestačí.

2 Citlivá a "necitlivá" data

Rozvoj informačních technologií, možnosti sdílení a propojování údajů v internetu, široké používání sociálních sítí, vyhledávacích služeb a na nich napojené zacílené reklamy vede k tomu, že z informačních sítí lze vhodnými vyhledávacími algoritmy získat i mnoho zneužitelných nedostatečně chráněných citlivých osobních dat. Proto v celé Evropské unii se stále více ozývaly požadavky na zpřísnění ochrany osobních údajů. Proto bylo v dubnu přijato nařízení **GDPR** (General Data Protection Regulation) podstatně zpřísňující ochranu osobních dat v informačních systémech. Týká se všech firem, institucí, jednotlivců a online služeb, které zpracovávají data uživatelů, s cílem dát evropským občanům větší kontrolu nad tím, co se s jejich daty děje. Toto nařízení začíná platit od 25. května 2018. Přináší přísná pravidla, která budou velmi nekompromisně vymáhána i za cenu astronomických pokut za jejich porušení. Tato nová přísná pravidla proto musí být důsledně implementována zejména v informačních systémech pracujících s citlivými zdravotnickými údaji pacientů.

Kdy jsou ve zdravotnických informačních systémech zapotřebí osobní údaje? Zdaleka ne vždy.

Existuje řada situací, kdy při zpracování zdravotnických dat citlivé údaje nejsou zapotřebí. Pokud např. zpracováváme údaje ze zdravotnických databází za účelem statistických šetření, výzkumu, ekonomických analýz, zdravotnického výkaznictví apod., pak si vystačíme s anonymizovanými údaji, kde **pacient je zastoupen bezvýznamovým**

identifikátorem, tj. nějakým jedinečným číslem, kterým tohoto pacienta identifikujeme, ale z kterého nelze bezprostředně určit jeho totožnost.

Jiná situace nastává, pokud provádíme **klinické vyšetření pacienta**. V těchto případech nám bezvýznamový identifikátor nestačí, protože potřebujeme ze zdravotnických databází vyhledat a do nich ukládat údaje o jeho zdravotním stavu, výsledcích vyšetření a zvoleném léčení. K tomu ale potřebujeme **jednoznačný identifikátor pacienta**.

Co ale má být tímto jednoznačným identifikátorem? Má jim být rodné číslo, číslo pojištěnce, číslo občanského průkazu nebo pasu, číslo sociálního pojištění nebo nějaký jiný identifikátor? Nic podobného! Klíčem k citlivým chráněným datům uloženým ve zdravotnických databázích musí být opět **bezvýznamový identifikátor pacienta**, tj. číslo, které ho jednoznačně identifikuje, ale které **bez dalších nástrojů nelze ztotožnit s daným pacientem**.

Nástrojem, který umožní ztotožnit číslo, které slouží v dané zdravotnické databázi identifikátorem pacienta, s jeho jménem, příjmením, datem narození, rodným číslem apod. – tedy s jednoznačným identifikátorem pacienta, slouží asistenční služby (tzv. „back office“) **eGovernmentu,** tvořený základními registry veřejné správy. Propojení zdravotnických databází se základními registry eGovernmentu umožní jak **ochranu** tak i **kontrolované sdílení** citlivých osobních dat o zdravotním stavu [1, 3, 4].

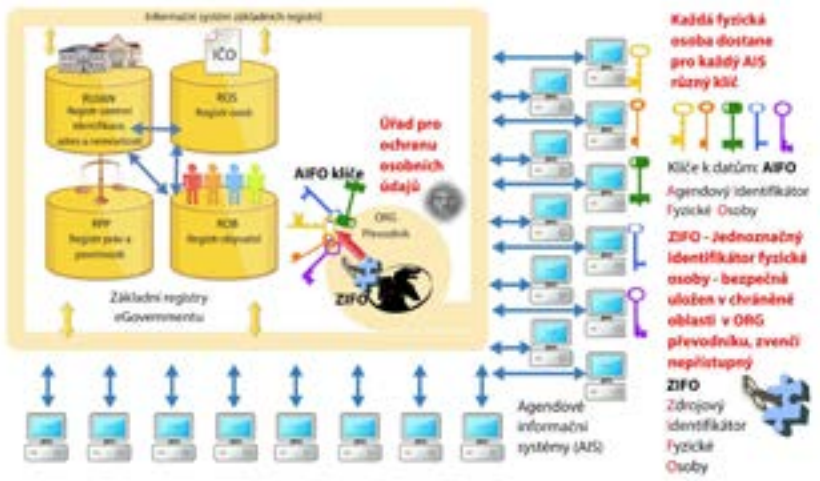
3 Jádro eGovernmentu – základními registry veřejné správy

Každá státní správa v té či oné formě vede tři základní údaje – o svých obyvatelích, o registrovaných právnických osobách (podnicích, institucích apod.) a o pozemcích a budovách, zkrátka o nemovitostech. Jádro eGovernmentu proto také tvoří databáze, které obsahují údaje o obyvatelích, právnických osobách a nemovitostech (Obr. 1).

První databází je **Registr obyvatel**. Obsahuje údaje o fyzických osobách – všech občanech ČR i všech cizincích s povolením k pobytu, azylantech nebo cizincích, kterým byla udělena doplňková ochrana, případně i údaje o dalších fyzických osobách, o kterých vedení v registru nařídí nějaký další právní předpis. Registr obyvatel tedy vede údaje o všech obyvatelích České republiky. A to žijících i mrtvých (registr obyvatel dnes obsahuje cca 16 miliónů údajů o zemřelých).

Druhou databází je **Registr osob** sloužící k evidenci právnických osob a jejich organizačních složek, organizací, institucí a organizačních složek státu i podnikajících fyzických osob – jinak řečeno všech těch entit, kterým bylo přiděleno IČO. Protože fyzické osoby mohou být majiteli či statutárními zástupci příslušných právnických osob či institucí, je Registr osob vzájemnými odkazy propojen s Registrem obyvatel.

Každá fyzická či právnická osoba má nějaké bydliště či adresu, případně může vlastnit nějakou nemovitost. Proto třetím základním registrem veřejné správy je **Registr územní identifikace, adres a nemovitostí**. Slouží k evidenci údajů o územních prvcích, údajů o územně evidenčních jednotkách, adresách, územní identifikaci a dalších údajích o územních prvcích, např. o tzv. „technickoekonomické atributy“ budov (počet podlaží, výměra, připojení na plyn, kanalizaci, vodu, způsob vytápění aj.).



Obrázek 1 – Základní registry veřejné správy tvoří jádro eGovernmentu. Na tyto registry jsou přes informační systém základních registrů napojeny další tzv. agendové informační systémy veřejné správy. Základní data o obyvatelích, fyzických osobách, adresách a nemovitostech i přístupových právech jsou uloženy na jednom místě a jakákoliv změna údajů (narození, úmrtí fyzické osoby, změna adresy právnické nebo fyzické osoby, vytvoření nebo zánik právnické osoby, změna přístupových práv k nějaké agendě atd.) je zapisována na příslušném místě pouze jednou. Změna údajů se pak projeví ve všech propojených informačních systémech. Každá fyzická osoba, která je uvedena v Registru obyvatel, má přidělen jednoznačný identifikátor fyzické osoby, tzv. Zdrojový identifikátor fyzické osoby (ZIFO), bezpečně uložený v tzv. ORG převodníku. V agendových informačních systémech je identifikátorem fyzické osoby tzv. Agendový identifikátor fyzické osoby (AIFO) – číslo, které identifikuje danou fyzickou osobu v daném agendovém informačním systému. V různých agendových informačních systémech má každá fyzická osoba různé identifikační klíče (různé AIFO). AIFO je ale pouhý číselný identifikátor – sám neobsahuje žádnou informaci o fyzické osobě. Pokud agendový informační systém potřebuje propojit data s nějakým jiným informačním systémem (např. dotazem na agendový informační systém občanských průkazů zjistit fotografii fyzické osoby), musí tak učinit pouze přes služby informačního systému základních registrů (které informačnímu systému, má-li na takový dotaz právo, např. poskytnou AIFO dané osoby v informačním systému občanských průkazů pro zjištění fotografie apod.). Převod AIFO jednoho informačního systému na AIFO jiného informačního systému se provádí (v souladu s přístupovými údaji v Registru práv a povinností) v ORG převodníku. Tímto způsobem je možné řídit přístupy k základním registrům i propojování jednotlivých agendových informačních systémů, a zároveň tyto přístupy monitorovat. Propojení informačních systémů se základními registry tak umožňuje důslednou ochranu dat i kontrolované sdílení dat.

Registr obyvatel, Registr osob a Registr územní identifikace, adres a nemovitostí jsou propojeny **vzájemnými odkazy**, což umožňuje vést základní údaje o fyzických osobách, právnických osobách a institucích, adresách a nemovitostech **na jednom místě**. Změna příjmení, změna adresy či třeba založení živnosti nějakou fyzickou osobou se projeví ve všech propojených odkazech, jak uvnitř základních registrů veřejné správy, tak i ve všech informačních systémech se základními registry propojených.

Protože k základním registrům veřejné správy jsou připojeny i další informační systémy, je nutno pečlivě hlídat i přístupová práva k údajům v nich obsažených. Proto existuje

ZÁZNAM O VYUŽÍVÁNÍ ÚDAJŮ V REGISTRU OSOB[1)]

(NA ZÁKLADĚ § 14 ZÁKONA Č. 111/2009 Sb., O ZÁKLADNÍCH REGISTRECH, VE ZNĚNÍ POZDĚJŠÍCH PŘEDPISŮ)

Identifikační údaje osoby, které je záznam poskytován:

Název nebo obchodní firma: Creative Connections s.r.o.

IČO: 48036713

Poř.č.	Agenda	Subjekt (OVM)	Datum a čas	Důvod/Účel
1.	A1000 - Zákon o Českém rozhlasu	45245053 - ČESKÝ ROZHLAS	25.01.2016 08:11:13	Aktualizace dat
2.	A1022 - Základní registr - registr osob	00007064 - Ministerstvo vnitra	03.04.2016 06:05:01	AIS3 - Roční výpis využití do DS subjektu
3.	A1022 - Základní registr - registr osob	00007064 - Ministerstvo vnitra	28.04.2016 18:08:56	AIS3 - Roční výpis využití do DS subjektu
4.	A1423 - Zákon o rozhlasových a televizních poplatcích	45245053 - ČESKÝ ROZHLAS	12.05.2016 19:11:41	Aktualizace dat
5.	A1201 - Veřejné rejstříky právnických a fyzických osob	00216800 - Městský soud v Praze	01.10.2016 00:39:14	Obchodní rejstřík - správa dat
6.	A1201 - Veřejné rejstříky právnických a fyzických osob	00216800 - Městský soud v Praze	03.10.2016 00:13:23	Obchodní rejstřík - správa dat
7.	A121 - Zjednodušené podnikání	47609108 - Ministerstvo průmyslu a obchodu	11.10.2016 22:32:11	Automatická kontrola údajů právnických osob
8.	A555 - Daňová kontrola vykonávaná územními finančními orgány	72080043 - Generální finanční ředitelství	14.10.2016 02:49:06	Automatická aktualizace dat

*Obrázek 2 – Díky monitorování přístupů a uchovávání tzv. „digitální stopy" o provedených transakcích je možné se dozvědět, **kdo, kdy a za jakým účelem** data o daném subjektu v základních registrech měnil nebo upravoval. Tak např. na obrázku je část záznamu o využívání údajů v registru osob pro subjekt Creative Connections s.r.o. – tento záznam se generuje automaticky a přichází do datové schránky.*

čtvrtý základní registr – **Registr práv a povinností**. Tento registr slouží jako zdroj údajů pro řízení přístupu uživatelů k údajům v jednotlivých základních registrech i k údajům v zvnějšku propojených informačních systémech. To znamená, že kdykoliv se někdo pokusí získat z registrů nějaký údaj, nebo ho dokonce změnit, bude systém posuzovat, zda to bude dovolené a jestli má na to právo ze zákona. V Registru práv a povinností jsou uchovávány záznamy, tzv. „digitální stopy" o provedených transakcích. Díky tomu bude mít každý občan možnost se dozvědět, **kdo, kdy** a **za jakým účelem** data o něm vedená v základních registrech měnil nebo upravoval (viz Obr. 2).

4 Klíče k osobním údajům – sada AIFO klíčů

Každá fyzická osoba, která je uvedena v Registru obyvatel, má přidělen jednoznačný identifikátor – tzv. **Zdrojový identifikátor fyzické osoby (ZIFO)**. Tento univerzální klíč ale není součástí Registru obyvatel. Zasluhuje si tu nejpřísnější ochranu. Proto je ukryt ve speciálním informačním systému – tzv. **ORG převodníku (převodníku identifikátorů)**. Org převodník spravuje Úřad pro ochranu osobních údajů a klíč ZIFO v něm pečlivě chrání. Odnikud zvnějšku (mimo Org převodník) není klíč ZIFO přístupný. ORG převodník není přímo napojen na základní registry – komunikuje s nimi pouze přes informační systém základních registrů.

Na informační systém základních registrů jsou **připojeny** další informační systémy – tzv. **agendové informační systémy**, které řeší nejrůznější agendy veřejné správy.

Toto uspořádání má tu výhodu, že základní data o obyvatelích, právnických osobách a institucích, adresách a nemovitostech i přístupových právech jsou **uloženy na jednom místě** a jakákoliv **změna** údajů (změna příjmení nebo narození či úmrtí fyzické osoby, změna adresy fyzické či právnické osoby apod.) se v informačních systémech **zapíše jen jednou** na příslušném místě, a všechny **ostatní propojené systémy** o tom **ihned vědí**. Občan nebo příslušná instituce (třeba matrika) tak např. může sám iniciovat změnu údajů v základních registrech (např. přestěhování, svatba apod.) a právně příslušný editor daného informačního systému pak provede změnu, která se okamžitě projeví ve všech propojených informačních systémech.

V informačních systémech veřejné správy je nutno zajistit nejen **sdílení a propojení** uložených dat, ale také i důslednou **ochranu osobních údajů**. K tomu slouží jednoduchý princip.

Každé fyzické osobě informační systém ORG vygeneruje **sadu klíčů**. Každá fyzická osoba pak má pro každý k základním registrům připojený agendový informační systém (ale i pro samotný Registr obyvatel) vygenerovaný různý klíč – tzv. **Agendový identifikátor fyzické osoby (AIFO)**.

Používání **rodného čísla** jako univerzálního identifikátoru fyzické osoby je tedy **nahrazeno sadou bezvýznamových identifikátorů – klíčů AIFO**, tj. čísel, které slouží jako identifikátory fyzické osoby v jednotlivých agendových informačních systémech (viz Obr. 1).

Podstatné je, že **AIFO klíče** se budou **pro jednotlivé agendy nebo skupiny agend lišit**, a neumožní tak při znalosti jednoho identifikátoru vyhledávat údaje o fyzické osobě v agendě jiné. Jediným místem, kde budou všechny tyto identifikátory uloženy, je právě Informační systém ORG.

Systém ORG provádí (v souladu s přístupovými údaji v Registru práv a povinností) **převod AIFO** jednoho informačního systému (např. Registru obyvatel) na AIFO jiného informačního systému – a tím **umožňuje řídit přístupy i propojování jednotlivých agendových informačních systémů.** Zároveň umožňuje **monitorovat** tyto přístupy a díky „paměťovým stopám" v Registru práv a povinností registrovat „kdo, kde, kdy a proč" se díval nebo měnil nějaké údaje v příslušném informačním systému.

Podstatné je, že v systému **ORG převodníku** ale **nejsou uloženy žádné další údaje fyzických osob**, takže ani znalost všech identifikátorů neumožňuje Úřadu ochranu osobních údajů (ani nikomu jinému) zjistit jejich přiřazení jednotlivým fyzickým osobám. Touto cestou může tedy realizace projektu základních registrů výrazně přispět k ochraně osobních údajů občanů.

Důležité je, že systém základních registrů veřejné správy jako jádro propojených agendových informačních systémů **není jen koncept, ale již fungující informační systém**. Do března minulého roku bylo např. přiděleno více než 262 miliónů různých AIFO klíčů,

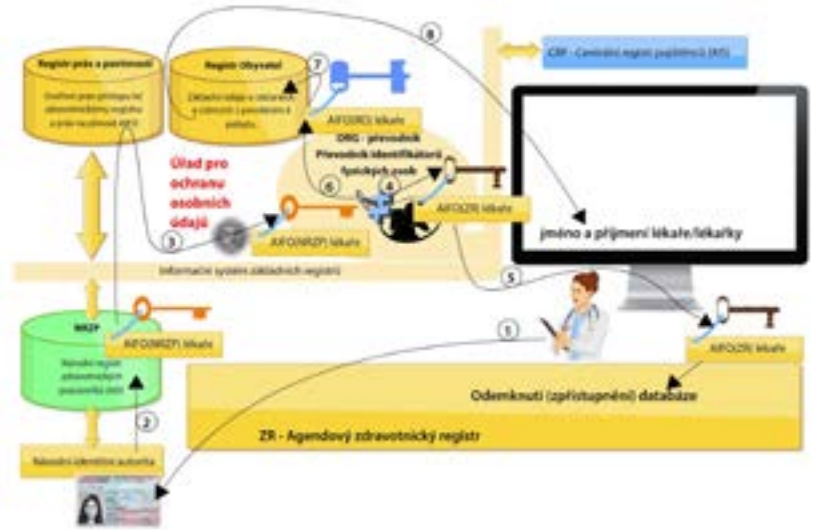
nyní odhadem to bude o více než sto miliónů více.

5 Propojení zdravotnických informačních systémů se základními registry eGovernmentu

Ukažme si (s určitým zjednodušením), **jak budovaný Národní zdravotnický informační systém bude spolupracovat se základními registry veřejné správy.**

Pokud zdravotnický pracovník, např. nějaký lékař či lékařka bude potřebovat pracovat s nějakým agentovým zdravotnickým registrem, nejprve musí prokázat, že k práci s daným zdravotnickým informačním systémem má právo přístupu (Obr. 3). Použije svůj přístupový identifikátor – třeba občanský průkaz s čipem – a **Národní identitní autorita zdravotnického pracovníka** identifikuje a nalezne jeho příslušný záznam v Národním registru zdravotnických pracovníků.

Národní registr zdravotnických pracovníků bude budován jako agendový informační systém – tj. každý zdravotnický pracovník v něm bude mít jedinečný AIFO klíč, a tento



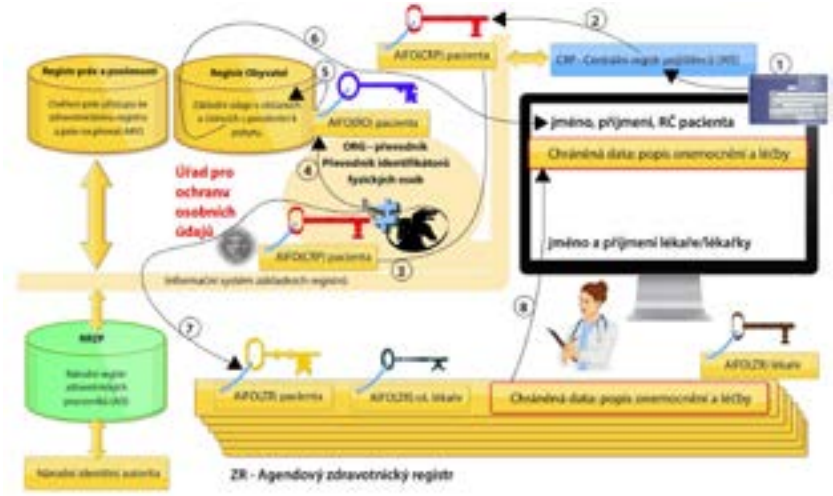
Obrázek 3 – Pro přístup k datům zdravotnického informačního systému (např. do nějakého agendového zdravotnického registru – třeba onkologického registru) bude nutno se nejprve identifikovat (1) pomocí přístupového identifikátoru (třeba pomocí občanského průkazu s čipem). Národní identitní autorita zdravotnického pracovníka identifikuje a vyhledá jeho záznam v Národním registru zdravotnických pracovníků (2) – vyhledá jeho AIFO klíč v tomto registru, pošle jej do informačního systému základních registrů, kde se nejprve v Registru práv a povinností ověří, zda daný zdravotnický pracovník má právo přístupu k agendovému registru, a pokud ano, klíč AIFO(NRZP) se pošle do ORG převodníku (3). ORG převodník zjistí odpovídající AIFO klíč lékaře AIFO(ZR) pro daný zdravotnický registr (4). Tímto klíčem zdravotnický pracovník zpřístupní údaje ve zdravotnické databázi (5). Zároveň ORG převodník vyhledá klíč zdravotnického pracovníka pro Registr obyvatel (6). Tímto AIFO(RO) klíčem se vyhledá (7) jméno a příjmení zdravotníka v Registru obyvatel (8).

AIFO klíč – AIFO(NRZP), bude poslán do informačního systému základních registrů.

Registr práv a povinností zjistí, že lékař/lékařka má k příslušnému agendovému zdravotnickému registru **právo přístupu** a poté ORG převodník pro tohoto zdravotnického pracovníka **vyhledá další AIFO klíče.** Jeden AIFO klíč je určen pro agendový zdravotnický registr – AIFO(ZR), a druhý AIFO klíč – AIFO(RO) je určen pro registr obyvatel.

AIFO klíč pro zdravotnický registr zdravotnickému pracovníku tento registr **zpřístupní**, a AIFO klíč pro registr obyvatel **vyhledá příslušné jméno a příjmení zdravotnického pracovníka v registru obyvatel.**

Nyní se musí zjistit identifikátor pacienta (obr 4). Pacient má např. u sebe kartičku pojištěnce – a podle čísla pojištěnce (nebo případně i z rodného čísla) v **Centrálním registru pojištěnců** (který bude také vybudován jako agendový registr) se zjistí agendový identifikátor pacienta pro centrální registr pojištěnců. Tento agendový identifikátor – AIFO(CRP) bude poslán do informačního systému základních registrů a na informační systém základních registrů připojený ORG převodník **vyhledá dva AIFO klíče pacienta – AIFO klíč pro zdravotnický registr** – AIFO(ZR) a AIFO klíč pro registr obyvatel – AFO(RO). První klíč bude identifikátor pro vyhledávání záznamů o daném pacientovi ve zdravotnickém registru, druhý identifikátor vygeneruje jméno, příjmení, rodné číslo pacienta (eventuálně, s využitím propojeného agendového systému občanských



Obrázek 4 – V Centrálním registru pojištěnců (který bude také vybudován jako agendový registr) se podle čísla pojištěnce (1) nebo z rodného čísla zjistí (2) agendový identifikátor pacienta pro centrální registr pojištěnců AIFO(CRP) . Tento agendový identifikátor bude poslán do informačního systému základních registrů a ORG převodník zjistí AIFO klíč pacienta pro Registr obyvatel (4), pomocí kterého se v Registru obyvatel vyhledá (5) jméno a příjmení pacienta (6). Zároveň ORG převodník podle AIFO(CRP) pacienta vyhledá AIFO klíč pacienta pro zdravotnický registr AIF(ZR). Pomocí tohoto klíče se v registru vyhledají zdravotnické záznamy o pacientovi (7). Tím se (dočasně) lékaři/lékařce zpřístupní chráněné zdravotnické záznamy o minulých vyšetřeních a léčbě (8).

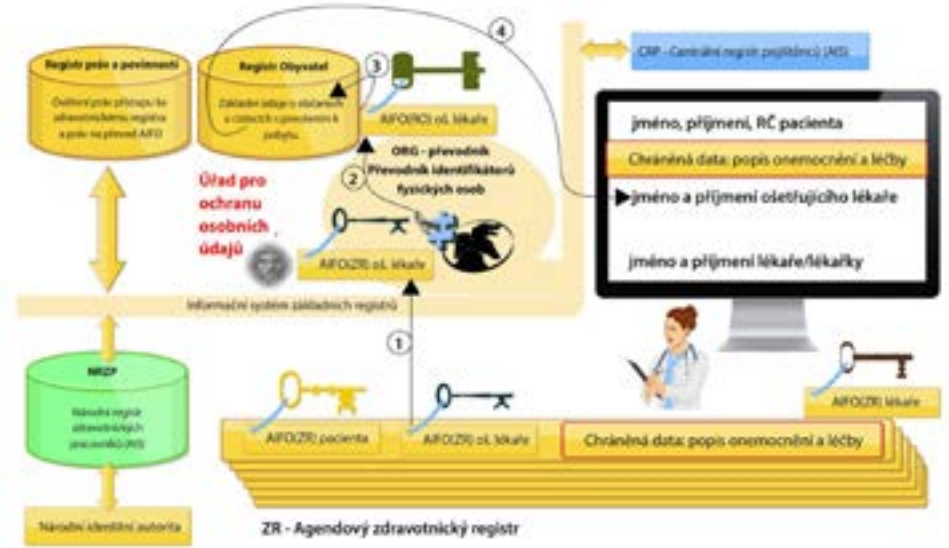
průkazů i fotografii pacienta).

Podle AIFO(ZR) pacienta se ve zdravotnickém registru **vyhledají záznamy o minulých vyšetřeních a léčbě pacienta** a také **agendový identifikátor ošetřujícího lékaře** AIFO(ZR), který provedl záznam (viz Obr. 5).

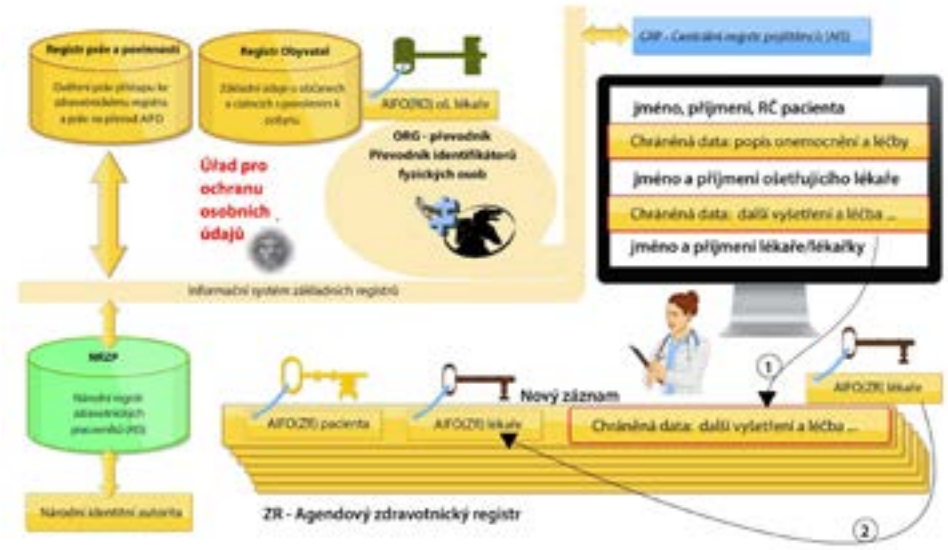
Aby se zjistilo jméno a příjmení ošetřujícího lékaře, musí se v ORG registru podle AIFO(ZR) **vyhledat jeho identifikátor pro registr obyvatel** – AIFO(RO). V registru obyvatel se podle tohoto identifikátoru nalezne **jméno a příjmení ošetřujícího lékaře.** Je nutno poznamenat, že registr obyvatel obsahuje záznamy i o zemřelých osobách, takže pokud ošetřující lékař již není na živu, z registru obyvatel nezmizí.

Pokud zdravotnický pracovník provede **další záznam do registru** (např. o provedených vyšetřeních a léčbě pacienta) – a tento záznam chce uložit jako **novou položku** do zdravotnického registru, **klíčem** k tomuto záznamu bude opět **AIFO(ZR) pacienta**, a jako ošetřující **lékař** bude v registru zdravotnický pracovník zapsán svým **AIFO(ZR) identifikátorem** (viz Obr. 6).

Ve zdravotnickém registru budou **pacienti i ošetřující lékaři zaznamenáni pouze jako čísla** – bezvýznamové identifikátory. Citlivá data budou tedy **anonymizována** – budou bez identifikace fyzické osoby. Vlastní zdravotnický registr tedy nebude obsahovat žádné citlivé osobní údaje (viz Obr. 7). Identifikovat pacienta (i ošetřujícího lékaře)



Obrázek 5 – Kromě záznamů o minulých vyšetřeních a léčbě pacienta zdravotnický registr obsahuje také AIFO klíč ošetřujícího lékaře, který provedl záznam (1). Aby se zjistilo jméno a příjmení ošetřujícího lékaře, musí se v ORG registru podle AIFO(ZR) ošetřujícího lékaře vyhledat (2) jeho AIFO pro registr obyvatel – AIFO(RO). V registru obyvatel se podle tohoto identifikátoru (3) nalezne jméno a příjmení ošetřujícího lékaře (4). Podstatné je, že Registr obyvatel obsahuje záznamy i o zemřelých osobách, takže pokud ošetřující lékař již není na živu, z registru obyvatel nezmizí.



Obrázek 6 – Záznam o provedených vyšetřeních a léčbě pacienta se ukládá jako nová položka do zdravotnického registru (1), klíčem k tomuto záznamu je opět agendový identifikátor pacienta pro daný zdravotnický registr AIFO(-ZR). Ošetřující lékař zapisuje svým AIFO(ZR) identifikátorem (2).

bude možné pouze při propojení s informačním systémem základních registrů, a toto propojení bude umožněno pouze oprávněným osobám. Toto oprávnění bude řízeno s využití registru práv a povinností a přístup registru bude monitorován.

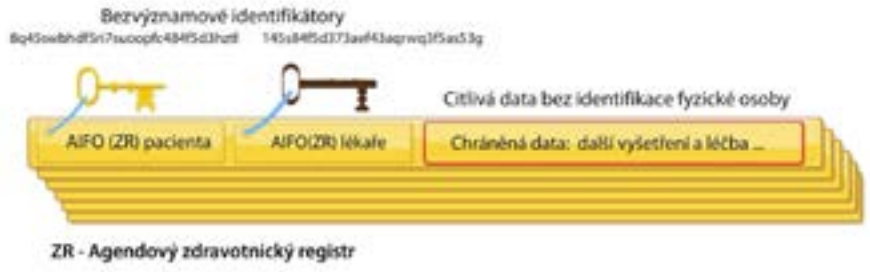
Propojení zdravotnických informačních systémů na základní registry eGovernmentu tedy umožňuje data zároveň **chránit proti zneužití i kontrolovaně sdílet.**

Národní zdravotnický systém je v současné době ve stádiu projektu a budování. **Základní registry** eGovermentu jsou však již dnes **funkční systém.**

6 Nezbytný předpoklad: legislativa

Pro občana platí, že činnosti, které nejsou legislativně upraveny, je dovoleno vykonávat libovolným způsobem. Ve veřejné správě je to naopak. Veřejná správa může vykonávat jen to, co ji zákon umožňuje. Ve veřejné správě je nutné veškerou činnost mít ošetřenou **legislativně** (veřejná správa může dělat jen ty činnosti, která má popsány v zákonech a nařízeních). Proto je důležité, že struktura i funkce základních registrů a jejich propojení na agendové informační systémy je **legislativně ošetřeno** zákonem č. 111/2009 Sb. pozdějšími předpisy.

Národní zdravotnický informační systém, napojený na základní registry eGovernmentu je zatím v projektu – **technologicky je napojení na jádro eGovernmentu vyřešeno**, toto napojení však musí být s dostatečnou přesností a jednoznačností popsáno i v legislativě,



Obrázek 7 – Ve zdravotnickém registru budou pacienti i ošetřující lékaři zaznamenáni pouze jako čísla – bezvýznamové identifikátory. Citlivá data budou tímto způsobem anonymizována – budou bez identifikace fyzické osoby. Vlastní zdravotnický registr tedy nebude obsahovat žádné citlivé osobní údaje. Identifikovat pacienta (i ošetřujícího lékaře) bude možné pouze při propojení s informačním systémem základních registrů. Toto propojení bude umožněno pouze oprávněným osobám, řízeno s využití registru práv a povinností a přístup registru bude monitorován.

a v nejbližší budoucnosti **bude nutno stávající legislativu upřesnit**.

Napojení na základní registry eGovernmentu není zamýšleno jen pro státem vytvářený Národní zdravotnický informační systém.

Služeb základních registrů budou moci využívat i **soukromí budovatelé zdravotnických informačních systémů** – jako poskytovatelé zdravotních služeb.

Projekt Národního informačního systému počítá i se službami pro soukromě budované zdravotnické informační systémy.

Podrobný aktuální popis funkce základních registrů je popsán v portálu správy základních registrů (*http://www.szrcr.cz*). Portál správy základních registrů [5] obsahuje mimo jiné i **podrobný popis pro správce a vývojáře informačních systémů** využívajících základní registry.

Vlastní technologie napojení zdravotnických informačních systémů na základní registry eGovernmentu však není závažným problémem. Hlavní problém při tvorbě Národního zdravotnického systému je **mezioborová komunikace**.

Zdravotnické informační systémy mají ulehčit práci zdravotníkům. Prvním problémem je mezioborové porozumění mezi zdravotníky a informatiky. Informační systémy musí vznikat v neustálém vzájemném dialogu. Bez určitého překryvu znalostí se to ale neobejde. Informatici musí pochopit potřeby zdravotníků a nabídnout efektivní informatické řešení jejich potřeb, zdravotníci musí pochopit možnosti a způsob fungování navrhovaného informatického řešení.

Národní zdravotnický systém musí být legislativně ošetřen – **to ovšem vyžaduje také mezioborové porozumění i mezi informatiky, zdravotníky a legislativci**, a konec konců i mezi **politiky**. Legislativci musí dobře pochopit strukturu a funkci navrhovaného informatického řešení a na základě tohoto pochopení legislativně dostatečně jednoznačně popsat procesy zaručující kontrolované sdílení i ochranu osobních údajů v budovaném národním zdravotnickém informačním systému. Zde jsou zatím bohužel ještě velké problémy.

Z **nedostatečné vzájemné komunikace a částečného nepochopení vznikají problémy,** které nakonec vedou i ke zbytečným sporům na půdě Poslanecké sněmovny i Senátu.

7 Závěr

1. Podstatné je, že **základní struktura eGovernmentu v ČR není jen koncept, ale fungující systém,** kde, obrazně řečeno, mozkem jsou registry veřejné správy, srdcem je legislativa, oběhem je komunikační infrastruktura veřejné správy a prsty jsou kontaktní místa veřejné správy s občany. Jedním z těchto míst jsou i zdravotnická zařízení a eGovernment, lze rozšířit i pro eHealth.
2. **Rodné číslo** je dobrý a v naši zemi tradiční koncept, který umožní **jednoznačně identifikovat občana jedním číslem**. Rodné číslo používáme v nejrůznějších dokladech – v občanském průkazu, pasu, řidičském průkazu, průkazu pojištěnce i jinde. Používání rodného čísla jako klíče k citlivým osobním datům je nebezpečné, protože podporuje možnost zneužití. Rodné číslo je totiž snadno získatelné, není chráněným údajem, a proto ho nelze používat jako univerzální klíč k osobním datům. Je možné i nutné ho **nahradit sadou AIFO klíčů**.
3. Při propojení agentových informačních systémů k informačnímu systému základních registrů je **přístup k osobním datům monitorován**. Proto je možné **zodpovědnost za eventuální úniky** dat snadno dohledat.
4. Díky monitorování můžeme dohledat informace o zacházení s osobními údaji konkrétní fyzické osoby – **zjistit „co, kdo, kdy a proč"** – což dává možnost, aby fyzická osoba (pacient) snadno získala informace o zacházení s jeho osobními údaji, v daném případě tedy o všech záznamech ve zdravotní dokumentaci a s nimi spojených vykazovaných nákladech.
5. Od 25. května 2018 začne v Evropské unii platit **nařízení GDPR** (General Data Protection Regulation) zpřísňující pravidla zacházení s osobními údaji. Propojení zdravotnických informačních systémů na základní registry eGovernmentu a příslušná legislativa, která toto propojení specifikuje, **umožní tato zpřísněná pravidla bez problémů splnit**.
6. **Klíčovým** pro další rozvoj zdravotnických informačních systémů je **vzájemná komunikace a multidisciplinární porozumění** mezi **informatiky, zdravotníky a legislativci**.

Literatura

[1.] Felix, O. (2012). Základní registry z pohledu architekta celého řešení. Informační bulletin, Úřad pro ochranu osobních údajů. vol. 13, 2012 (1), str. 2–6.

[2.] Kasal, P., Svačina, Š., Kofránek, J. (2008). Teze rozvoje eHealth v České republice: In MEDSOFT 2008, (Milena Ziethamlová, Ed.) Praha: Agentura Action M, Praha 2008, s. 23–35. ISBN 978-80-86742-22-9.

[3.] Kofránek, J. (2012). Jak propojit informační systémy veřejné správy a nevytvořit „velkého bratra". Informační bulletin, Úřad pro ochranu osobních údajů. vol. 13, 2012 (1), str. 25–30.

[4.] Kofránek, J. (2013) Jak informatizovat zdravotnictví a nevytvořit přitom velkého bratra. In MEDSOFT 2013, (Milena Zeithamlová, Ed.) Praha: Creative Connections, Praha 2013, s. 55-63, ISSN 1803-8115, dostupné z http://www.creativeconnections.cz/medsoft/2013/Medsoft_2013_Kofranek.pdf

[5.] Správa základních registrů. (2017) [online]. Dostupné z http://www.szrcr.cz [cit. 14.3.2017]

Kontakt

Doc. MUDr. Jiří Kofránek, CSc.
Oddělení biokybernetiky a počítačové podpory výuky, ÚPF 1. LF UK
Praha U nemocnice 5, 128 53 Praha 2
tel: 777686868
e-mail: *kofranek@gmail.com*

Ing. Ondřej Felix, CSc.
Digital Champion Czech Republic
Odbor Hlavního architekta eGovernmentu
Ministerstvo vnitra ČR Ministerstvo vnitra
nám. Hrdinů 1634/3, 140 21 Praha 4
tel: 974 817 402
Email: *ondrej.felix@me.com*

Ing. Jiří Polák, CSc.
výkonný ředitel České asociace manažerů informačních technologií (CACIO)
Vltavská 14 150 00
Praha 5
tel: 267 053 400
Email: *jiri.polak@cacio.cz*

ing. Jiří Borej
koordinátor Národní strategie elektronického zdravotnictví
Ministerstvo zdravotnictví ČR
Palackého nám. 4
128 01 Praha 2