Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic

INFORMACIJSKI
POOBLAŠČENEC

Namen dokumenta:	Smernice podajajo odgovor na najpogosteje zastavljena vprašanja z vidika zahtev Zakona o varstvu osebnih podatkov, s katerimi se srečujejo osebe, ki so v bolnišnicah odgovorne za vzdrževanje in delovanja informacijskih sistemov, obenem pa je njihov namen poenotiti zahteve in prakso v okviru inšpekcijskih nadzorov.
Ciljne javnosti:	Pravni oddelki in oddelki za informatiko v bolnišnicah
Status:	javno
Verzija:	1.0
Datum verzije:	15. 2. 2008
Avtorji:	Informacijski pooblaščenec v sodelovanju s skupino za bolnišnične informacijske sisteme pri Združenju zdravstvenih zavodov Slovenije
Ključne besede:	smernice, zdravstvo, zdravstveno stanje, zavarovanje, informacijski sistem, sledljivost

VSEBINA

O smernicah Informacijskega pooblaščenca (IP)

Namen smernic IP je podati skupne praktične napotke za upravljavce zbirk osebnih podatkov (OP) na jasen, razumljiv in uporaben način in s tem odgovoriti na najpogosteje zastavljena vprašanja s področja varstva osebnih podatkov, s katerimi se srečujejo posamezni upravljavci zbirk OP. S pomočjo smernic naj bi upravljavci dobili priporočila, kako naj v praksi zadostijo zahtevam Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 – uradno prečiščeno besedilo; v nadaljevanju ZVOP-1-UPB1).

Pravno podlago za izdajo smernic Pooblaščencu daje 49. člen ZVOP-1-UPB1, ki med drugim določa, da Pooblaščenec daje neobvezna mnenja, pojasnila in stališča o vprašanjih s področja varstva osebnih podatkov in jih objavlja na spletni strani ali na drug primeren način ter pripravlja in daje neobvezna navodila in priporočila glede varstva osebnih podatkov na posameznem področju.

Oglejte si tudi:

- *Mnenja IP*:
  http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/

- *Brošure IP*:
  http://www.ip-rs.si/publikacije/prirocniki/

Smernice IP so objavljene na spletni strani:

http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/smernice/

Uvod

Zakonodajalec se pri pripravi zakonskih okvirov seveda ne more do podrobnosti opredeliti glede svojih zahtev, saj morajo biti zakonski okviri hkrati zelo konkretni in tudi dovolj široki, obenem pa tehnološko nevtralni, kar pa lahko v praksi pomeni različne interpretacije glede zahtev, ki jih posamezen zakonski akt postavlja. Zakon o varstvu osebnih podatkov daje splošen okvir in usmeritve, ki jih nato zapolnjujejo področne zakonodaje in praksa, ki mora biti tudi zaradi pravne varnosti čim bolj enotna in jasna.

V praksi se je tako pojavila potreba po pripravi smernic za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic. Zahteve ZVOP-1-UPB1 glede zavarovanja OP v tovrstnih ustanovah so poleg običajnih zahtev za zavarovanje OP še toliko bolj rigorozne, saj se v zdravstvenih ustanovah obdelujejo tudi občutljivi osebni podatki, ki že zaradi svoje subtilne narave terjajo višje standarde zavarovanja.

Cilj IP je, da Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic postanejo uporaben pripomoček tako za osebe, ki so odgovorne za delovanje informacijskih sistemov v bolnišnicah, kot za osebe, pri upravljavcu odgovorne za posamezne zbirke osebnih podatkov. Enotna interpretacija zakonskih obveznosti je vsekakor v interesu upravljavcev zbirk OP in vseh, ki morajo v praksi postaviti in zagotavljati minimalne standarde za zavarovanje OP, katerih izvajanje bodo državni nadzorniki preverjali v okviru inšpekcijskih postopkov.

Ureditev zavarovanja osebnih podatkov v Zakonu o varstvu osebnih podatkov

Zavarovanje OP je urejeno v 24. členu ZVOP-1-UPB1, ki določa naslednje:

(1) Zavarovanje osebnih podatkov obsega organizacijske, tehnične in logično-tehnične postopke in ukrepe, s katerimi se varujejo osebni podatki, preprečuje slučajno ali namerno nepooblaščeno uničevanje podatkov, njihova sprememba ali izguba ter nepooblaščena obdelava teh podatkov tako, da se:

1. varujejo prostori, oprema in sistemsko programska oprema, vključno z vhodno-izhodnimi enotami;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. preprečuje nepooblaščen dostop do osebnih podatkov pri njihovem prenosu, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
4. zagotavlja učinkovit način blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov;
5. omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov.

(2) V primeru obdelave osebnih podatkov, ki so dostopni preko telekomunikacijskega sredstva ali omrežja, morajo strojna, sistemska in aplikativno programska oprema zagotavljati, da je obdelava osebnih podatkov v zbirkah osebnih podatkov v mejah pooblastil uporabnika osebnih podatkov.

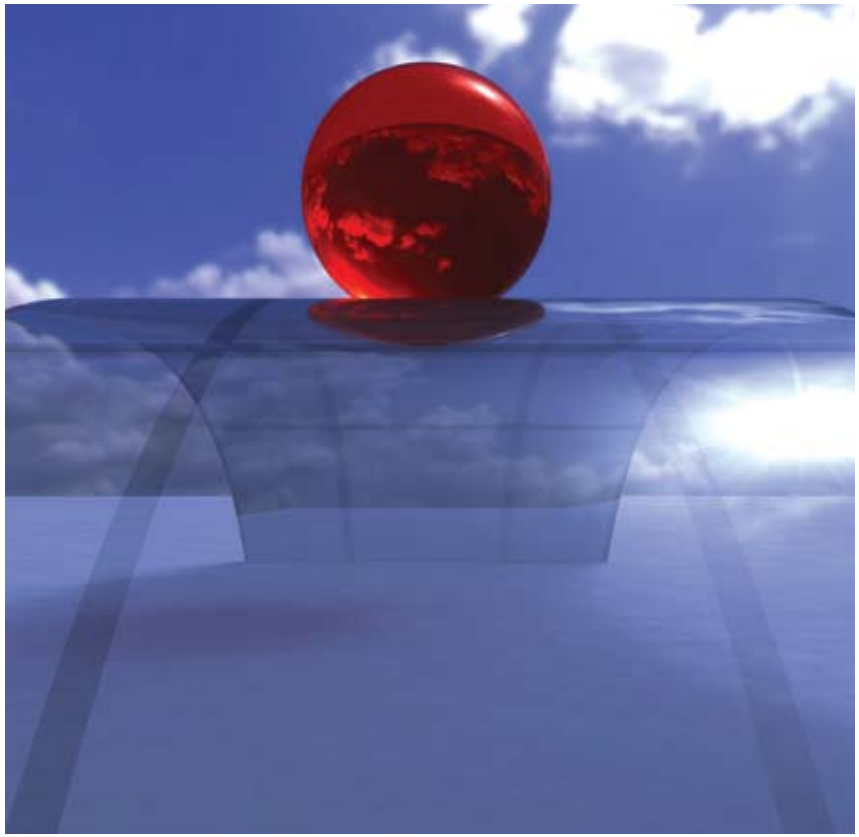
(3) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.

(4) Funkcionarji, zaposleni in drugi posamezniki, ki opravljajo dela ali naloge pri osebah, ki obdelujejo osebne podatke, so dolžni varovati tajnost osebnih podatkov, s katerimi se seznanijo pri opravljanju njihovih funkcij, del in nalog. Dolžnost varovanja tajnosti osebnih podatkov jih obvezuje tudi po prenehanju funkcije, zaposlitve, opravljanja del ali nalog ali opravljanja storitev pogodbene obdelave.

Zavarovanje občutljivih OP je posebej urejeno urejeno v 14. členu ZVOP-1-UPB1, ki določa naslednje:

(1) Občutljivi osebni podatki morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih, razen v primeru iz 5. točke 13. člena tega zakona .

(2) Pri prenosu občutljivih osebnih podatkov preko telekomunikacijskih omrežij se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.



Način dela in prijave v HIS (hospitalni informacijski sistem)

Vprašanje: *Proces zdravljenja pacientov v bolnišnici je organiziran tako, da v njegove osebne podatke v informacijskem sistemu velikokrat vpogleda več članov zdravstvenega tima hkrati, saj posamezen primer obravnava ekipa ljudi, sestavljena iz različnih strokovnih profilov. Ker je pri tem v informacijski sistem prijavljen samo eden od članov tima, sistem za sledenje vpogledom prikazuje stanje, kot da je v podatke vpogledal samo on, čeprav jih je v resnici videlo več ljudi. Kako glede na opisan potek dela v praksi zagotoviti spoštovanje 24. člena ZVOP-1?*

Ali naj se ustrezno prilagodi programsko opremo in interna pravila tako, da bo za delo s programom nujna hkratna prijava vseh navzočih članov tima?

Pojasnilo - opis dela:

- *Ambulante (urgenca):*
  - ambulantni tim: administratorka, sestra, zdravnik (dodatno še lahko specializant, sekundarij). Prijavljena administratorka - delajo (gledajo) vsi. Ali je potrebno, da se na začetku dela v program prijavijo vsi člani tima? Ali se lahko na začetku dela definira in v program zapiše samo tim (npr. poimensko zdravnik, sestra, administratorka) in se prijavi v program uporabnik "amb1"?
  - urgentni tim: sestre (2-4), zdravnik(-i). Prijavljena je sestra, delajo (gledajo) vsi. Isto velja za intenzivne terapije.

- *Hospital (oddelki):*
  - tim na oddelku: sestre (4-5), lastni računalnik - ena prijavljena, delajo (gledajo) vse, zdravniki, lastni računalnik - prijavljen zdravnik, dela zdravnik.
  - oddelčne pisarne: administratorke (3-4), zdravnik(-i), prijavljena administratorka - delajo (gledajo) vsi.

Odgovor:
Uvodoma je potrebno pojasniti namen (ratio) določbe, ki narekuje, da mora biti zavarovanje urejeno tako, da omogoča poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, uporabljeni ali drugače obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov. Omenjena določba, ki opredeljuje t.i. sledljivost obdelave osebnih podatkov, je izjemnega pomena predvsem za odkrivanje nepooblaščenih vstopov v zbirke osebnih podatkov in posledično zlorabe tako pridobljenih osebnih podatkov (npr. javno razkritje ipd.). Izvajanje sledljivosti je namreč tisti ukrep, s katerim naj bi se ugotovilo, kdo je zlorabil določene OP; kot primer praktičnega scenarija si lahko predstavljamo, da v javnost "pricurljajo" podatki o zdravstvenem stanju neke medijsko izpostavljene osebnosti, npr. da ima določen politik AIDS. Kako bomo ugotovili, kdo je odgovoren za nepooblaščeno razkritje takšnih podatkov? Pooblaščenec se zaveda, da je nemogoče stoodstotno preprečiti nepooblaščeno seznanitev in zlorabo osebnih podatkov, vendar pa je potrebno sprejeti vse razumne mere in ukrepe, ki lahko zlorabe preprečijo ali vsaj omogočijo naknadno ugotavljanje odgovornosti. Sledljivost je pomembna tudi s preventivnega vidika, zaradi česar je potrebno zaposlene seznaniti z dejstvom, da se izvaja sledljivost obdelave osebnih podatkov. V nekaterih primerih lahko že to dejstvo odvrne posameznika, da bi se odločil za neupravičen dostop do osebnih podatkov, saj se bo zavedal da bodo njegova dejanja evidentirana.

V prvi vrsti mora sledljivost omogočati hospitalni informacijski sistem. Ker je pojem obdelave osebnih podatkov zelo širok in vključuje praktično kakršno koli ravnanje s podatki, vključno s samim dostopom do njih, mora takšen sistem omogočati sledljivost celotne obdelave OP, torej tudi vpogledov.

Pri tem pa se v praksi porajajo določena vprašanja, saj izvajanje sledljivosti, kljub sodobnim informacijskim tehnologijam, ni enostavno in lahko terja velike resurse.

Ločimo lahko tri nivoje sledljivosti:

1. sledljivost sprememb;
2. sledljivost dostopa do podatkov;
3. popolna sledljivost z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov.

1. Sledljivost sprememb

Prvi nivo sledljivosti omogoča naknadno ugotavljanje, kdo je vnesel, ažuriral ali drugače spremenil, izbrisal kateri podatek in kdaj.

2. Sledljivost dostopa do podatkov

Drugi nivo omogoča naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kakšen podatek in kdaj, poleg tega pa se beleži tudi kdo in kdaj je do določenega podatka zgolj dostopil (vpogled, seznanitev), a podatka ni spremenil. Pri tem je potrebno opredeliti za vpogled oziroma dostop do podatka vsak ukaz podatkovni bazi, ki se odrazi v **pridobitvi podatka** ali **prikazu podatka na izhodni napravi (npr. računalniški zaslon), kot dostop do tega podatka**, ki ga je na tem nivoju potrebno beležiti. Od te točke naprej sledljivost nadaljnje uporabe tako pridobljenih podatkov ni več niti možna niti smiselna, saj je možnih poti enostavno preveč (zaslon je npr. namreč možno fotografirati, posneti, natisniti itd.).

Primer zagotavljanja sledljivosti dostopa do podatkov je uporaba podatkov v policijskih bazah. Vsak dostop posameznega uporabnika se zabeleži, s tem pa je moč izslediti uporabnika, ki je do podatkov določenega posameznika dostopal brez upravičenega namena.

3. Popolna sledljivost z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov.

Pri tretjem nivoju se dejansko beleži vse, kdo in kdaj je dostopal do podatka, ga spreminjal in če ga je spreminjal, kakšen je bil prvotni podatek in v kaj je bil popravljen. Gre torej za popolno zgodovino, v katero se beleži življenjski cikel podatka.

Glede na določbe 1. odstavka 24. člena ZVOP-1-UPB1 je IP mnenja, da tretjega nivoja, torej beleženja podatkov o tem, kakšen je določen podatek bil v času in v kaj se je spremenil, ZVOP-1-UPB1 ne zahteva. Tovrstna zahteva je sicer tehnično tudi izvedljiva, a vsekakor pomeni zahtevno in stroškovno visoko investicijo v opremo za shranjevanje takšnih podatkov brez občutnih koristi z vidika varstva osebnih podatkov. Lahko bi se zgodilo, da bi takšna baza dejansko presegla velikost izvorne, produkcijske baze, kar gotovo ni bil namen zakonodajalca, delovanje produkcijske baze pa bi bilo znatno upočasnjeno.

Pri določanju zahtevane ravni sledljivosti je ključna določba 3. odstavka 24. člena ZVOP-1-UPB1-1, ki določa, da morajo biti postopki in ukrepi za zavarovanje osebnih podatkov ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo. Pri občutljivih osebnih podatkih gre tako za najsubtilnejšo kategorijo osebnih podatkov, ki potrebujejo posebno varstvo in zaščito ter omejitve dopustne obdelave, našteti pa so taksativno in ne primeroma. Pooblaščenec zato vztraja, da mora programska oprema za občutljive osebne podatke omogočati poznejše ugotavljanje kdo, kdaj in do katerih podatkov je dostopal (raven 2). To pomeni, da mora zdravstveni informacijski sistem omogočati naknadno ugotavljanje, kateri uporabnik sistema je ob katerem času na informacijski sistem naslovil zahtevo za pridobitev ali prikaz osebnih podatkov določene osebe. Tovrstna sledljivost je ključnega pomena za naknadno ugotavljanje morebitnih zlorab zaradi nepooblaščene seznanitve (in naknadnega posredovanja oz. obdelave) z osebnimi podatki. Odraz tega je tudi 14. člen ZVOP-1, ki za občutljive osebne podatke določa, da morajo biti pri obdelavi posebej označeni in zavarovani tako, da se nepooblaščenim osebam onemogoči dostop do njih.

Za osebne podatke, ki niso občutljivi, mora upravljavec zagotavljati vsaj raven sledljivosti sprememb, torej kdaj so bili posamezni osebni podatki vneseni v zbirko osebnih podatkov, kdo je to storil in kdaj, vendar se pri tem ne sme tega vzeti kot pravilo v smislu, da sledljivost dostopanja do podatkov ni potrebna. Tudi tu je namreč potrebno upoštevati tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo. Tudi razkritje »običajnega« osebnega podatka ima lahko za posameznika ali upravljavca veliko težo in resne posledice, zato je v določenih primerih potrebno zagotoviti tudi sledljivost vseh dostopov do podatkov, kar pa je potrebno presojati od primera do primera.

V praksi se kljub do sedaj navedenim smernicam porajajo nova vprašanja, predvsem glede dopustnosti uporabe skupinskih dostopnih pravic (timsko delo, skupinska gesla, en prijavljen uporabnik in več dejanskih uporabnikov ipd.)
Zagotovo lahko trdimo, da v takšnem primeru ne moremo omogočiti naknadnega ugotavljanja, kdo je lahko dostopil do določenega podatka in ga potencialno zlorabil, kot je to opisano zgoraj v primerih, ki se pojavijo v praksi, saj se zabeleži kvečjemu ime skupinskega uporabnika (npr. amb1 ali kaj podobnega).

Pri odgovoru na vprašanje, ali je dopustna uporaba skupinskih dostopnih pravic, sta ključni dve stvari:

1. ali je narava dela res takšna, da bi posamična gesla ovirala delovni proces in povzročala druge, potencialno tudi zelo resne posledice (npr. ovirano delo na urgenci zaradi odjavljanja enega in prijavljanja drugega uporabnika);
2. če so skupinske dostopne pravice neizogibne, kako se lahko zagotovi možnost naknadnega ugotavljanja odgovorne osebe, če je prišlo do zlorabe?

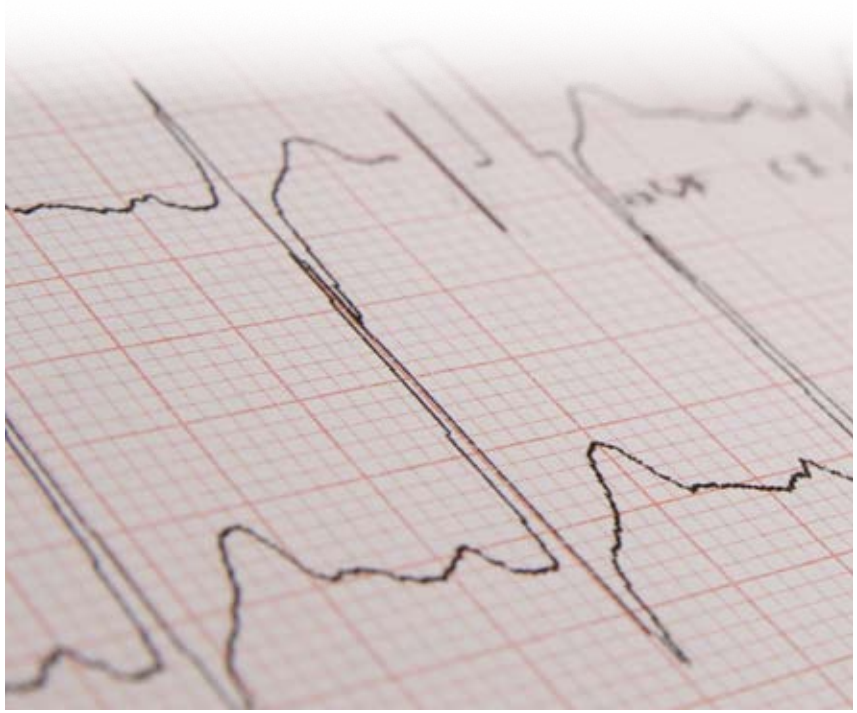
Pooblaščenec meni, da:

1. pri delu urgence in tam, kjer zaradi narave dela ni smiselna uporaba posamičnih dostopnih pravic, se lahko izjemoma uporabijo tudi skupinske dostopne pravice (npr. za urgentni tim). Pooblaščenec pri tem opozarja, da mora biti razlog za uporabo skupinskih dostopnih pravic resnično utemeljen, resnost in tveganje pa morata pretehtati odsotnost zmožnosti natančnega ugotavljanja, kdo je odgovoren za zlorabo osebnega podatka. Zgolj nepraktičnost zaradi večkratnega prijavljanja in odjavljanja v informacijski sistem ali posamezne aplikacije ni zadosten razlog za uporabo dostopnih pravic na ravni skupine (npr. enega uporabniškega imena in gesla za več uporabnikov). Sistem mora kljub temu omogočati naknadno ugotavljanje, kdo so bili člani določenega tima v določenem času, saj je s tem zožen nabor oseb, ki bi lahko zlorabile OP, same uporabniške pravice pa morajo biti natančno dokumentirane. Poleg navedenega je potrebno skupinske dostopne pravice omejiti, in sicer tako, da se s pomočjo skupinskih uporabniških imen in gesel lahko dostopa le do osebnih podatkov pacientov na določenem oddelku in le toliko časa, dokler se pacient nahaja na tem oddelku. Ko je npr. pacient odpuščen, namreč ni utemeljenega razloga, da se lahko do njegovih osebnih podatkov dostopa s skupinskim uporabniškim imenom in geslom in takšen dostop ne sme biti mogoč.

V primerih, ko imajo dostop do osebnih podatkov osebe, ki so na praksi in krožijo po oddelkih, je potrebno tem osebam dodeliti ločene dostopne pravice; v primeru, da praktikant kljub temu uporablja dostopne pravice mentorja, mora namreč mentor prevzeti vso odgovornost za zlorabe osebnih podatkov, ki bi nastale s pomočjo mentorjevih dostopnih pravic.

2. v vseh primerih, kjer odjavljanja enega in prijavljanje drugega uporabnika ne predstavlja nobenih resnejših posledic, temveč je zgolj nekoliko »nadležno« in z vidika uporabnika manj praktično opravilo, Pooblaščenec zahteva, da se uporabijo posamične dostopne pravice (gesla ipd. na ravni uporabnika) in da se uporabnik pred delom prijavi v sistem, po uporabi pa iz njega odjavi. Pooblaščenec zlasti opozarja, da mora sistem omogočati bodisi samodejno zaklepanje po določenem času neaktivnosti uporabnika bodisi ročno zaklepanje delovne postaje s strani uporabnika. Nedopustno je, da je delovna postaja popolnoma dosegljiva, zadnji uporabnik pa še vedno prijavljen v informacijski sistem in morebitne druge aplikacije tudi takrat, ko uporabnika dalj časa ni ob delovni postaji, saj je s tem odprta pot za zelo enostavno zlorabo osebnih podatkov.

Težava pri izvajanju načela sledljivosti lahko nastane tudi takrat, ko so zbirke vodene ročno, ko torej niso informatizirane, kar pa ni predmet obravnave teh smernic. Takšne zbirke je zato primarno potrebno na primeren način hraniti (jih zaklepati v omare, posebne sobe ipd.) in v pravilniku ali drugem ustreznem aktu, ki ga kot obveznega določa 2. odstavek 25. člena zakona, točno določiti osebe, ki imajo pravico dostopa do osebnih podatkov.



Sledljivost pri hkratnem dostopu do seznamov oseb in osebnih podatkov

24. člen terja uveljavitev načela sledljivosti za osebne podatke. V življenjskem ciklu osebnih podatkov do teh dostopajo osebe z različnimi nalogami in pravicami – sprejemni administratorji, medicinsko osebje, fakturisti itd., ki pogosto delajo tudi z različnimi seznami bolnikov, prikazi podatkov o bolnikih po določenih filtrih, uporablja se iskanje po določenih kriterijih in podobno. Pri tem se na izhodnih enotah neizogibno prikazujejo določeni osebni podatki.

Pri tem se pojavijo v praksi naslednja vprašanja:

Vprašanje: Ali je dovolj, da se beležijo vse poizvedbe (npr. SQL stavki oz. njihovi rezultati) za sezname, ali moramo beležiti vsebino seznamov (kateri pacient je bil na katerem seznamu)? Podobno vprašanje se pojavi, ko je obravnava zaključena (z vidika programa zaklenjena) in se izvede samo vpogled. Ali se beleži, kdo je vpogledal ali se beleži tudi vsebina?

Odgovor: Vzemimo za ponazoritev primer, ko pooblaščeni uporabnik išče po kriteriju »Novak« in se mu prikaže seznam 100 pacientov in (nekateri, ne nujno vsi) osebni podatki teh pacientov. Kako lahko naknadno ugotovimo, da se je uporabnik s takšno poizvedbo seznanil z določenimi OP (vzemimo na začetku postavljeni hipotetični scenarij znane osebnosti z AIDS-om). Obstajata dve poti za zagotavljanje sledljivosti:

*a) takšna poizvedba se mora **zabeležiti pri vsakem od pacientov**, katerega osebni podatki so bili prikazani v določenem trenutku na izhodni enoti. Pri posamezniku se mora v tem primeru zabeležiti, kdo in kdaj je s pomočjo poizvedbe prišel do osebnih podatkov posameznika.*

*b) poizvedba mora dati ob ponovitvi enak rezultat, torej se **beleži rezultat poizvedbe v času**. Zabeležiti se mora, **kdo** je izvedel poizvedbo, **kdaj** in **kakšen je bil rezultat poizvedbe v tem času**.*

V obeh primerih je ključno, da se **beleži**, kdo je izvedel določeno poizvedbo, saj se lahko le na ta način določi odgovorno osebo v primeru zlorabe OP.

Če ni možno zagotoviti naknadnega ugotavljanja, do katerih OP je na ta način uporabnik dostopil (do nekaterih ali do vseh), je potrebno predvidevati, da se je uporabnik s poizvedbo seznanil z vsemi OP tega posameznika in temu ustrezno to zabeležiti v dnevniški zapis.

Pooblaščenec je mnenja, da oba načina zadostita zahtevam 24. člena ZVOP-1-UPB1-1, zato je odločitev, kateri način bo v praksi uporabljen, prepuščena posameznemu upravljavcu, ki se mora odločiti na podlagi lastne situacije in okoliščin (informacijski sistem, stroškovni vidiki ipd.)

Vprašanje: Administratorka na svoji delovni postaji odpira obravnave (zunanje napotnice, razlog obiska, izdelava računov za samoplačnike in delne plačnike). Ali se beležijo samo aktivnosti ali tudi vsebina?

Odgovor: Ključni pri odgovoru na to vprašanje so osebni podatki, do katerih ima administratorka dostop. Ker tako ali drugače dostopa do osebnih podatkov, se mora njen dostop do osebnih podatkov posameznika zabeležiti, torej da je uporabnica v določenem trenutku dostopila do podatkov določenega posameznika. Ta podatek se - podobno kot pri odgovoru na prejšnje vprašanje – lahko zabeleži pri posameznem pacientu ali pa kot v času ponovljiv rezultat poizvedbe. Če uporabimo scenarij »pobeglih« podatkov o tem, da ima znana osebnost AIDS, in da je odgovorna oseba za razkritje tega podatka (lahko tudi) administratorka, ki se je s tem podatkom seznanila pri izdelavi računa (ali na drug način), je kot potencialni vir zlorabe njen dostop do tega podatka potrebno zabeležiti. Na tem mestu je vsekakor potrebno opozoriti na ustrezne dostopne pravice zaposlenih v računovodstvu.

Vprašanje: Ali se morajo dnevniške datoteke hraniti na posebnih mestih, ali morajo biti dosegljive takoj, ali lahko zmanjšamo njihovo velikost?

Odgovor: ZVOP-1-UPB1 posebej ne predpisuje mesta ali načina hrambe in tudi izrecno ne določa mesta hrambe dnevniških zapisov, ki se vsekakor lahko hranijo v stisnjeni, komprimirani obliki. Pomembno je, da tovrstni zapisi obstajajo, da so avtentični in da so dosegljivi v razumljivem času (ne nujno takoj oziroma isti dan), saj je za izvedbo inšpekcijskega postopka ključno, da se da naknadno ugotoviti, ali je do zlorabe OP prišlo in kdo je odgovorna oseba za zlorabo.

Vprašanje: Ali je potrebno preprečiti (slediti) ukaze, kot so Ctrl+PrintScreen, oz. Alt+PrintScreen, uporabo prenosnih medijev, na katere se lahko posnamejo podatki (diskete, cd/dvd mediji, usb ključi, prenosni diski…), uporabo e-pošte in interneta, kamer, prenosnih telefonov itd.?

Odgovor: Gre predvsem za vprašanja, ki se nanašajo na sledljivost dostopov do osebnih podatkov. Pri tem je potrebno obravnavati vsako pridobitev podatka oziroma **vsak prikaz podatka na izhodni napravi (npr. računalniški zaslon) kot dostop do tega podatka in s tem vpogled**, ki ga je na tem nivoju potrebno beležiti. Sledljivost ravnanja s tako pridobljenim podatkom od te točke naprej ni več niti možna niti smiselna. Zaslon si namreč lahko hkrati ogleda več ljudi, vsebino zaslona je možno shraniti, posneti, fotografirati, natisniti, zato je prikaz na zaslonu, izvoz podatkov brez takojšnjega vpogleda ali druga pridobitev podatka, kot rezultat določenega ukaza ali poizvedbe, zadnja točka, ko je potrebno zagotavljati sledljivost dostopa do OP, saj je od tega trenutka dalje sledljivost praktično neizvedljiva in jo lahko primerjamo z možnostmi za zagotavljanje sledljivosti zbirk OP, ki se vodijo na papirju.

Pooblaščenec priporoča, da se uporabo interneta in e-pošte vnaprej natančno in transparentno opredeli v ustreznem internem aktu, lahko tudi v Pravilniku o zavarovanju osebnih podatkov. Pri uporabi omenjenih sredstev namreč prihaja do kolizije legitimnih interesov in dolžnosti delodajalca do nadzora nad svojimi delovnimi sredstvi, in na drugi strani temeljne človekove pravice do zasebnosti, ki jo (v določeni meri) uživa posameznik tudi na delovnem mestu. Več o vprašanjih zasebnosti na delovnem mestu, dopustnosti uporabe interneta in e-pošte si lahko preberete v že izdanih mnenjih IP: http://www.ip-rs.si/varstvo-osebnih-podatkov/iskalnik-po-odlocbah-in-mnenjih/. Glede dopustnosti uporabe prenosnih medijev Pooblaščenec priporoča, da se sledi uveljavljenim standardom varnosti v informacijskih sistemih, in sicer, da se to dovoljuje le tistim delavcem, ki zaradi narave dela potrebujejo določene izhodne priključke ali naprave.

Vprašanje: Koliko časa je potrebno hraniti podatke za zagotavljanje sledljivosti (dnevniške datoteke)?

Odgovor: Osebni podatki se lahko shranjujejo le toliko časa, dokler je to potrebno za dosego namena, zaradi katerega so se zbirali ali nadalje obdelovali. Če bi zahtevali hranjenje podatkov o tem, kdo in katere podatke, ali tudi samo kdo in podatke koga je uničil po preteku roka, določenega za hranjenje, bi prišli do absurdne situacije, ko bi morali hraniti tudi podatke o tem, kdo je uničil dnevniške zapise o že uničenih podatkih – in tako v neskončnost. Osebne podatke se lahko uniči, ko preteče zakonski rok za hranjenje osebnih podatkov in v tem roku v zbirko ali konkretni osebni podatek ni nihče vpogledal. V kolikor pa je v tem roku bil zabeležen vpogled v zbirko osebnih podatkov, pa mora nastati nova zbirka vpogledov. Tudi to zbirko vpogledov pa se, kot vsako drugo zbirko osebnih podatkov, lahko uniči šele po preteku zakonskega roka (in tako z vsako novo nastalo zbirko vpogledov naprej). Upravljavec torej lahko po petih letih (razen če zakon ne določa drugačnega roka hranjenja) uniči zbirko vpogledov pod pogojem, da vanjo v tem obdobju ni nihče vpogledal. Poudarjamo pa, da se iz konkretne zbirke osebnih podatkov po preteku zakonskega roka za hranjenje morajo izbrisati vsi tisti osebni podatki, v katere v tem obdobju ni vpogledal nihče. Kar pomeni, da zaradi vpogleda v en osebni podatek v konkretni zbirki ne hranimo celotne zbirke, temveč le tisti del zbirke, v katerega je bilo vpogledano. Obseg zbirke se tako postopoma zmanjšuje.

Vprašanje: Avtomatično pošiljanje podatkov (IVZ, NALEP, e-rojstvo, nova KZZ…)? Kaj bo potrebno slediti, če programi med sabo avtomatično izmenjujejo podatke? Ali je dovolj od proizvajalca dobiti pisno zagotovilo, da njihov program dela samo tisto, čemur je namenjen in nič drugega?

Odgovor: Glede zagotavljanje sledljivosti veljajo ista načela tako za ročno kot za avtomatsko sproženo pošiljanje osebnih podatkov (glej odgovore na prejšnja vprašanja), s tem da ne sledimo, kar si sistemi avtomatsko izmenjujejo, temveč le posege človeka uporabnika v zbirko, ki je sicer lahko tudi avtomatsko pridobila OP. Posebno pozornost pri razvoju sistemov za tovrstno izmenjavo podatkov je potrebno nameniti vprašanjem **zavarovanja občutljivih podatkov med prenosom po telekomunikacijskih omrežjih** in morebitnemu povezovanju zbirk osebnih podatkov. Pri prenosu **občutljivih osebnih podatkov** preko telekomunikacijskih omrežij se namreč glede na določbo 2. odstavka 14. člena ZVOP-1-UPB1 šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in elektronskega podpisa tako, da je zagotovljena njihova nečitljivost oziroma neprepoznavnost med prenosom.

Pooblaščenec posebej opozarja na pomen razlikovanja med notranjo in zunanjo sledljivostjo. Poleg notranje sledljivosti, ki je bila natančneje opredeljena v odgovorih na prejšnja vprašanja, mora upravljavec osebnih podatkov za vsako posredovanje osebnih podatkov (izven svoje institucije) zagotoviti, da je mogoče pozneje ugotoviti, **kateri** osebni podatki so bili posredovani, **komu**, **kdaj** in **na kakšni podlagi**, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja osebnih podatkov. Prejemnik osebnih podatkov pa mora znotraj svoje institucije nato zagotoviti notranjo sledljivost prejetih osebnih podatkov.

Povezovanje zbirk osebnih podatkov iz uradnih evidenc in javnih knjig je posebej urejeno v ZVOP-1-UPB1. Pooblaščenec v zvezi s povezavo zbirk osebnih podatkov opozarja, da mora biti takšno povezovanje določeno v zakonu ter, da v primeru, če katera od zbirk, ki naj bi se jih povezovalo, vsebuje občutljive osebne podatke (19. točka 6. člena ZVOP) ali je za izvedbo povezovanja potrebna uporaba istega povezovalnega znaka (EMŠO, št. zdravstvenega zavarovanja ali davčna številka), **povezovanje ni dovoljeno brez predhodnega dovoljenja Pooblaščenca.** Več o tem na spletni strani Pooblaščenca: http://www.ip-rs.si/varstvo-osebnih-podatkov/register-zbirk/povezava-zbirk-osebnih-podatkov/.

Vprašanje: Kakšne so naše dolžnosti, ko določene osebne podatke v našem imenu in za naš račun v obdelavo zaupamo zunanjemu izvajalcu?

Odgovor: Pooblaščenec opozarja na ustrezno ureditev pogodbene obdelave osebnih podatkov, kot to določa 11. člen ZVOP-1-UPB1. Upravljavec osebnih podatkov (v tem primeru torej bolnišnica, zdravstveni dom ali zasebni izvajalec zdravstvene dejavnosti) lahko posamezna opravila v zvezi z obdelavo osebnih podatkov s pogodbo zaupa pogodbenemu obdelovalcu, ki mora biti registriran za opravljanje takšne dejavnosti in zagotavlja ustrezne postopke in ukrepe iz 24. člena tega zakona. Gre torej za tako imenovano zunanje izvajanje (angl. outsourcing) obdelave OP.

Pogodbeni obdelovalec sme opravljati posamezna opravila v zvezi z obdelavo osebnih podatkov v okviru naročnikovih pooblastil in osebnih podatkov ne sme obdelovati za noben drug namen. Medsebojne pravice in obveznosti se uredijo s **pogodbo**, ki mora biti sklenjena **v pisni obliki** in mora vsebovati tudi **dogovor** o postopkih in ukrepih iz 24. člena tega zakona. **Upravljavec** osebnih podatkov **nadzoruje** izvajanje postopkov in ukrepov iz 24. člena tega zakona.

Pooblaščenec še opozarja, če pride med upravljavcem zbirke osebnih podatkov in pogodbenim obdelovalcem do spora, vam je pogodbeni obdelovalec dolžan na podlagi vaše zahteve osebne podatke, ki jih je pogodbeno obdeloval, nemudoma vrniti. Morebitne kopije teh podatkov mora takoj uničiti ali jih posredovati državnemu organu, ki je v skladu z zakonom pristojen za odkrivanje ali pregon kaznivih dejanj, sodišču ali drugemu državnemu organu, če tako določa zakon. V primeru prenehanja pogodbenega obdelovalca se osebni podatki brez nepotrebnega odlašanja vrnejo upravljavcu osebnih podatkov.

Pri informacijskih rešitvah, ki niso predmet zunanjega izvajanja, ampak so bile kupljene s strani bolnišnice, je vsekakor priporočljivo, da se ob nakupu zahteva popolno in podrobno tehnično dokumentacijo o delovanju sistema in morebitne spremljajoče izjave in zagotovila izvajalca.

Zaključek

Pooblaščenec za konec podaja še priporočilo oziroma poziv k boljši komunikaciji med pravnimi in informacijskimi službami v bolnišnicah. ZVOP-1-UPB1 je namreč zakon, ki je v določenih vidikih izrazito tehnične narave in brez ustreznega sodelovanja in komuniciranja navedenih služb lahko hitro pride do napačnih in nepopolnih interpretacij ali nerazumevanja zakonskih zahtev, ki se nato izrazijo v večjih možnostih za zlorabe osebnih podatkov. Ignorantia iuris nocet, nepoznavanje prava škoduje - v sodobni družbi pa prav tako (ali še bolj) škoduje nepoznavanje tehnologije.