Varnost in zagotavljanje zasebnosti bolnišničnih podatkov o pacientih

Nina Marcelan, študent, Fakulteta za varnostne vede, Univerza v Mariboru
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru

Namen in cilj prispevka
Namen prispevka je predstaviti mehanizme varnosti in stopnjo varovanja bolnišničnih podatkov o pacientih. Za varovanje pacientovih podatkov veliko naredijo že sami uslužbenci, ki so zavezani k molku. Za drugi del zaščite pa mora poskrbeti informacijski sistem bolnišnic. Cilj je ugotoviti kolikšna je zaščita bolnišničnih podatkov ter možnost in kaj bi se zgodilo, če bi v javnost prišli vsi bolnišnični podatki. Danes za obisk pri zdravniku uporabljamo kartico zdravstvenega zavarovanja, katera vsebuje veliko podatkov, kateri niso nujno potrebni in ne vplivajo na zdravljenje, za to je temu področju potrebno posvetiti dodatno pozornost.

Metodologija
Za ugotovitev stanja v državi sem uporabila deskriptivno metodo s študijo primerov in primerjalno analizo v kateri sem primerjala izgubo bolnišničnih podatkov o pacientih v Sloveniji ter v tujini. Predstavila bom katere informacijsko-varnostne sisteme uporabljajo za zaščito podatkov slovenske bolnišnice, ter kaj se je zgodilo v primerih izgube zaupnih zdravstvenih podatkov.

Ugotovitve in omejitve
Bolnišnice ter njihovi zaposleni imajo vpogled v veliko naših osebnih podatkov, tudi v tiste kateri niso potrebni za zdravljenje. Tako bolnišnice, kot tudi zakonski predpisi se trudijo zaščititi osebne podatke, vendar še vedno pride v javnost veliko informacij. Zakoni nas že ščitijo pred kršitvami in zlorabami osebnih podatkov, vendar še vedno prihajajo v javnosti. V RS imamo premalo organov nadzora nad zlorabo osebnih podatkov. Kar nekaj podjetij se v Sloveniji ukvarja z izboljšanjem bolnišničnih informacijskih sistemov oziroma ponujajo programe za nadgradnjo le teh. Velikim zdravstvenim ustanovam do take posodobitve finančno prevelik zalogaj, zato ostajajo na starejših programih.

Izvirnost
Prispevek bo proučil načine zaščite in varovanja bolnišničnih podatkov v Sloveniji. Največ oziroma veliko bi morala na tem področju narediti država ali pa vsaj prispevati k izboljšanju varnosti in zaščiti osebnih podatkov.

Ključne besede: varnost, zasebnost, pacienti, bolnišnični podatki

1 UVOD

Varovanje bolnišničnih podatkov se začne pri zaposlenih, ki se morajo držati vsaj osnovnih etičnih standardov. Evropski standardi so v osnovi etični standardi, razviti v pravnem kontekstu, v katerem zdravstveni delavci odločajo o varovanju, rabi in razkrivanju zaupnih osebnih podatkov. Vseh zdravstvenih delavcev ne vežejo iste pravne obveze o zaupnosti, vendar pa vse veže etična dolžnost vzdrževanja zaupnosti.
Zdravstveni delavci morajo spoštovati ključna načela o zaupnosti v zdravstvu. Praksa je pokazala, da so v zdravstvenih institucijah kršitve Zakona o varstvu osebnih podatkov zelo pogoste, saj zdravstveno osebje ključnih občutljivih podatkov pacientov ne varuje primerno. Osebni podatki se nepravilno posredujejo, dostop do njih ni ustrezno varovan ali pa do zdravstvenih podatkov dostopa osebje, ki nima pooblastil.
Danes morajo bolnišnice nuditi hitro delovanje in odzivnost osebja, kar dosežejo s hitrim in varnim dostopom osebja do baze podatkov in zanesljivostjo delovanja informacijskega sistema, hkrati pa morajo zagotavljati točnost in ažurnost podatkov o pacientih, zato je v bolnišnicah pomemben hiter

pretok informacij, čim manjši oziroma ničen izpad računalnikov in stabilna baza podatkov. Bolnišnice morajo biti opremljene z zanesljivo, hitro in učinkovito strojno in programsko opremo. Varnost informacij je pomembna tema vseh podjetij in organizacij. Dandanes se vsi zanašajo na notranje računalniške sisteme in internet. Ne morejo si privoščiti prekinitve poslovanja in upravljanja. Varnostni incident ima lahko širše negativne posledice na zaupanje strank, stike z javnostjo in navsezadnje na dohodke.
Bolnišnični informacijski sistem mora omogočati tudi sledljivost. Sistem mora nuditi vse podatke o obdelavi podatkov, če tudi je bil podatek uporabljen samo vpogled. Ločimo lahko tri nivoje sledljivosti: sledljivost sprememb, sledljivost dostopa do podatkov ter popolna sledljivost z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov. Prvi nivo sledljivosti omogoča naknadno ugotavljanje, kdo je vnesel, ažuriral ali drugače spremenil, izbrisal kateri podatek in kdaj. Drugi nivo omogoča naknadno ugotavljanje, kdo je vnesel, spremenil ali izbrisal kakšen podatek in kdaj, poleg tega pa se beleži tudi kdo in kdaj do določenega podatka zgolj dostopil (vpogled, seznanitev), a podatka ni spremenil. Pri tem je potrebno opredeliti 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.). 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 bi prvotni podatek in v kaj je bil popravljen. Gre torej za popolno zgodovino, v katero se beleži življenjski cikel podatka (Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic, 2008).
Danes nas skorajda vsak, ki želi od nas dobiti povsem neosebno informacijo ali podatek, zaprosi še za osebne podatke. Večina ljudi jih brez premisleka in zadrege tudi pove ali napiše. Premalo se zavedamo komu zaupamo te podatke, ter za kaj jih ta oseba ali organizacija potrebuje in kako jih bo hranila in varovala. V mislih imam tiste, najbolj osnovne, vendar za našo varnost pomembne podatke, kot je datum in letnica rojstva, naslov kjer živimo. Naj vsak premisli, komu in zakaj je posredoval omenjene osebne podatke. Prepričana sem, da jih je veliko, ki se ne spomnijo kolikokrat so to že naredili. Če pomislimo na naše zdravstvene ali bolnišnične podatke, ki so še toliko bolj občutljivi in zaupni. Z njimi upravlja, rokuje veliko zdravstvenega in farmacevtskega osebja. Zbolimo, naj si bo viroza, zaradi katere običajno obiščemo samo osebnega, družinskega zdravnika. Za težave izvesta najmanj dva zdravstvena sodelavca. Za obisk zdravnika potrebujemo kartico zdravstvenega zavarovanja, tudi na njej je zabeleženih kar nekaj podatkov. Običajno nam zdravnik/ca predpiše recept, s katerim moramo v lekarno po zdravilo. Tam tudi farmacevt/ka vidi naše podatke na kartici zdravstvenega zavarovanja. Zatorej se moramo v takih primerih najbolj zanašati in verjeti, da vsi upoštevajo kodeks, kar pomeni molk zdravstvenega in farmacevtskega osebja o pacientovih podatkih.

2 UGOTOVITVE

Za varnost podatkov, kateri so dostopni preko računalnika lahko sami naredimo veliko, tako da ga zaščitimo z geslom, tudi ko samo za kratek čas zapustimo prostor, ne pustimo, da druge osebe na našem računalniku uporabljajo različno strojno opremo in priključke, ne nameščajte nezakonite ali druge nepoznane sumljive programske opreme, zaščitite internetno omrežje z geslom in ne dostopajte do nezavarovanega internetnega omrežja.
Bolnišnice ter njihovi zaposleni imajo vpogled v veliko naših osebnih podatkov, tudi v tiste kateri niso potrebni za zdravljenje. Tako bolnišnice, kot tudi zakonski predpisi se trudijo zaščititi osebne podatke, vendar še vedno pride v javnost veliko informacij. Velikokrat smo že poslušali govorice katere so »skrivnostno« prišle iz ljubljanskega urgentnega bloka, o nevsakdanjih poškodbah znanih Slovencev, prevelikega odmerka droge naših politikov in še bi lahko naštevala.
Zakoni nas že ščitijo pred kršitvami in zlorabami osebnih podatkov, vendar še vedno prihajajo v javnosti. V RS imamo premalo organov nadzora nad zlorabo osebnih podatkov.
Kar nekaj podjetij se v Sloveniji ukvarja z izboljšanjem bolnišničnih informacijskih sistemov oziroma ponujajo programe za nadgradnjo le teh. Velikim zdravstvenim ustanovam do take posodobitve finančno prevelik zalogaj, zato ostajajo na starejših programih. V Kliničnem centru Ljubljana so ob

prenovi Urgentnega bloka prenovili tudi infrastrukturo. Nov informacijski sistem je zasnovan tako, da se lahko v primeru nujnega bolnika povežejo tudi z drugimi bolnišnicami in službami nujne medicinske pomoči.
Informacijski sistem je sistem, ki je urejen in organiziran. Uporabnike oskrbuje z informacijami, na podlagi katerih se lahko odločajo. Osnovne aktivnosti informacijskega sistema so zbiranje, shranjevanje in obdelava in posredovanje informacij končnim uporabnikom.
Tehnologija je vedno bolj napredna, vrhunska. Vendar se pa bodo znova in znova kazali novi problemi, težave predvsem pri zaščiti vseh teh brezžičnih prenosov, predvsem, ker se gre za prenose osebnih podatkov. Veliko je strokovnjakov za zaščito in preprečevanje zlorab teh podatkov, vendar je in bo vedno več tudi takih strokovnjakov, kateri znajo mimo zaščite priti do teh podatkov. Zatorej bodo naši strokovnjaki na področju informacijske tehnologije oziroma varnosti imeli vedno veliko novih izzivov, saj naj bi bili tisti, ki želijo zlorabiti podatke vedno korak pred njimi.
Medicinska oziroma zdravstvena dokumentacija zajema vse pisne podatke (na različnih medijih) o bolnikih, njihovem bolezenskem stanju, družinskih ali drugih razmerah. Izvirniki se hranijo v zavodu in se skrbno varujejo. Potrebno jo je skrbno voditi in vnašati vse pomembne podatke v času njihovega nastanka, dokumentacije se ne spreminja za nazaj. Vsi zaposleni so zavezani, da pri svojem delu upoštevajo etične kodekse s temeljno zahtevo po spoštovanju zasebnosti bolnikov in tajnosti njihovih zdravstvenih podatkov, o katerih so izvedeli pri opravljanju svojega poklica. Kršitev se šteje za hujšo kršitev delovnih obveznosti.
Pomembna je možnost zlorabe posredovanja osebnih in/ali zdravstvenih podatkov v komercialne namene ali zbiranja informacij za potrebe društev bolnikov, čeprav je osnovni namen lahko human. Bolniki so zanimivi za trženje, zato niso redka prizadevanja za pridobitev zlasti njihovih naslovov. Bolnik se mora sam in prostovoljno odločiti, če se bo vključil v kakšno društvo, postal prostovoljec ali se kako drugače izpostavil javnosti (Šparovec, 2009).
Velik korak bodo naredile bolnišnice, če se bodo odločile za modernizacijo temperaturno-terapevtskega lista. Vsi vemo, kako zgleda nekaj papirjev pritrjenih na kovinsko podlago na koncu bolniške postelje. Slovensko podjetje je izumilo elektronski temperaturni-terapevtski list. Ta list bi bil ravno tako prisoten pri vsakemu bolniku, samo vse bi bilo enostavneje.
Uporaba elektronske oblike TTL-a v prvi vrsti odpravlja številne pomanjkljivosti papirnatih medijev. Mogoče je dosledno spremljati tako posamezne zapisovalce kakor spremembe, ki so jih naredili, kar je v tradicionalnem načinu pogosto težko ali celo nemogoče. Zapisani podatki so tudi precej popolnejši. Ker se računalnik nahaja neposredno ob bolnikovi postelji, se namreč podatki evidentirajo sproti. Na ta način se izognemo morebitnemu naknadnemu vnosu, posledično pa dvojnemu delu in, kar je najpomembneje, morebitnim napakam, ki lahko pri tem nastanejo. Hkrati uporabnikom omogočijo, da elektronski zdravstveni zapis pacienta obogatijo s številnimi podatki, ki so zaenkrat ostali zapisani samo na papirju (npr. podatki o razdeljevanju zdravil), ali pa sploh niso bili evidentirani (npr. nekateri postopki in porabljeni material). S tem pa seveda ne pridobijo samo najnujnejših izhodišč za poenostavitev (oziroma sploh vzpostavitev) spremljanja neposrednih stroškov zdravljenja na pacienta, ampak je tako narejen velik korak do trenutka, ko bodo v bolnišničnem informacijskem sistemu celostno zabeleženi vsi s procesom zdravljenja povezani podatki – slednji so namreč bolj kot ne še vedno razpršeni po posameznih vrstah dokumentacije (TTL, laboratorijski in diagnostični izvidi, list zdravstvene nege, elektronski zdravstveni karton pacienta), (povzeto po Novak, 2011).
Že zdaj smo začudeni, da so zdravstveni podatki bolnika v večini primerov še vedno zgolj v papirnati obliki v tako imenovanem zdravstvenem kartonu. Če nič drugega, je oteženo iskanje po njem. Del sistema bo moralo biti torej skladišče e-zdravstvenih kartonov. To bo v centralnem strežniku, v strežniku izvajalca zdravstvenih storitev, verjetno pa na obeh mestih, če želimo, da so podatki v realnem času dosegljivih tudi izven omrežja izbranega zdravnika (v primeru specialističnega zdravljenja), pa še njihovo arhiviranje bo preprosteje. Ljudje smo po naravi radovedni in ne nazadnje so podatki, zapisani v zdravstveni karton, naši osebni podatki. Pričakujemo torej, da bomo do svojih podatkov lahko dostopali od doma, jih po potrebi prebirali in na njihovi osnovi dobili mnenje drugega zdravnika (ali vrača, če hočete). Tak sistem pa bo seveda moral imeti vse potrebne varnostne mehanizme (Kodelja in Banovič, 2007).
Vsi želijo imeti najboljšo tehnologijo, olajšano delo, vendar si ne predstavljam , koliko bi bilo šele potem kršitev, ko bi vsi te podatki potovali po istem informacijskem sistemu. Moje mnenje je da bi prihajalo do večjih zlorab. Ravno zato je potrebno še delati in nadgrajevati informacijsko varnost.

3 SKLEP

Informacijska varnost je bistvo varovanja podatkov vseh podjetij, institucij, organizacij, itd. Pomembno je da podatke, predvsem pa tiste osebne, zaupne zaščitimo kar se da dobro. Med občutljivejše podatke sodijo tudi bolnišnični podatki o pacientih. Bolnikovi osebni podatki so v središču zdravstvenega varstva. Bolnik mora dati soglasje, da deli svoje osebne zdravstvene podatke s strokovnjaki. Po drugi strani pa to soglasje velja skozi celotno zdravstveno oskrbo, podajanje diagnostike in omogoča zapis medicinske zgodovine posameznika in s tem tudi zagotavlja varnost pacientov. Ker gre za občutljive podatke je dolžnost zdravstvenih delavcev, da zagotovijo da so zapisani podatki shranjeni, skupni in dostopni, kakor to določa zakon.
Vsaka bolnišnica in katerakoli zdravstvena ustanova ima predpisane ter javno objavljene pravilnike in predpise katerih se morajo držati in jih upoštevati vsi uslužbenci. Navsezadnje lahko pride pomembna, zaupna informacija v javnost od čistilke bolnišnice ali druge zdravstvene ustanove.
Kodeks etike medicinskih sester in zdravstvenih tehnikov Slovenije v III. načelu opredeljuje, da je medicinska sestra dolžna varovati kot poklicno skrivnost podatke o zdravstvenem stanju, posebej pa zadolžuje zdravstveno institucijo, da vzpostavlja in vzdržuje tak informacijski sistem, ki ščiti varovančevo skrivnost, npr. Z omejitvijo dostopa do dokumentacije. Posebej se to nanaša na računalniški informacijski sistem. Medicinska sestra se moralno ni dolžna držati poklicne molčečnosti, če bi bila zaradi pomanjkanja informacij ogrožena varnost varovanca, družine ali skupnosti. Če se medicinska sestra sooči z nujnostjo razkriti skrivnost, naj bo le ta omejena na tisto število ljudi, ki je nujno potrebna, da se prepreči škodljivo delovanje.
Bolnišnični informacijski sistem je temelj zdravstvene ustanove za upravljanje s pacientovimi podatki. Z bolnišničnim informacijskih sistemom vodijo vsako dogajanja za vsakega posameznika. V program dostopa vso medicinsko osebje, pa naj si bo za naročanje, vodenje čakalnih vrst, vse vrste preiskav, nameščanje pacienta v sobo in posteljo, cenik storitev, urniki, itd.
Varovani prostori morajo biti varovani z organizacijskimi ter fizičnimi in/ali tehničnimi ukrepi, ki nepooblaščenim osebam onemogočajo dostop do podatkov. V skladu s pravilnikom in z direktorjevimi pooblastili mora biti urejen režim vstopanja v prostore, kjer se hranijo občutljivi podatki. Prostore morajo ves čas nadzorovati pooblaščene osebe, t. j. biti prisotne v njih ves čas ko se v njih zadržujejo stranke. Kadar pooblaščene osebe ni v prostoru, morajo biti nosilci podatkov zaklenjeni. Dostop v varovane prostore je mogoč in dopusten le v delovnem času, izven delovnega časa pa le na podlagi dovoljenja, ki ga lahko izda le direktor, če je za delovni postopek to potrebno. Ključe varovanih prostorov posedujejo le direktor in pooblaščene osebe. Ključev ne smemo puščati v ključavnicah vrat varovanih prostorov, varovani prostori ne smejo ostajati nenadzorovani; ob odsotnosti delavcev, ki jih nadzorujejo, morajo biti zaklenjeni. Zaposleni ne smejo nenadzorovano puščati nosilcev osebnih podatkov na mizah ali jih kako drugače izpostavljati nevarnosti vpogleda nepooblaščenim osebam oz. delavcem. Občutljivi osebni podatki se ne smejo hraniti izven varovanih prostorov. Za potrebe obnavljanja računalniškega sistema ob okvarah in ob drugih izjemnih okoliščinah se zagotavlja redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj, če se podatki nahajajo tam. Te kopije se hranijo v zato določenih mestih, ki morajo biti ognjevarna, zavarovana proti poplavam in elektromagnetnim motnjam, v okviru predpisanih klimatskih pogojev ter zaklenjena (povzeto po (Kersnik in Tušek-Bunc, 2007).

VIRI

Kersnik, J. in Tušek – Bunc, K. (2008). Zdravnik kot lastnik in posrednik zdravstvene dokumentacije. Pridobljeno 12.10.2011 na http://www.drmed-mb.org/wp-content/uploads/2010/11/srott_26.pdf

Kodelja, M. in Banovič, Z. (1.9.2007). On-line zdravstveni sistem: Velika pričakovanja. Moj Mikro. Pridobljeno 11.10.2011 na http://www.mojmikro.si/v_srediscu/razkritje/on-line_zdravstveni_sistem_velika_pricakovanja

Novak, R. (2011). Matrixroom. SRC Infonet. Pridobljeno 5.10.2011 na http://www.src.si/library_si/pdf/infosrc/2011-66/infoSRC66.pdf

Smernice za zavarovanje osebnih podatkov v informacijskih sistemih bolnišnic. (15.2.2008). Informacijski pooblaščenec. Pridobljeno 4.10.2011 na https://www.ip-

rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_za_zavarovanje_OP_v_IS_bolnisnic_15022008.pdf
Šparovec, M. (2009). Varstvo osebnih podatkov v Univerzitetnem Kliničnem Centru Ljubljana (Diplomsko delo). Ljubljana: Fakulteta za upravo.