

ZAŠTITA LIČNIH INFORMACIJA U MEDICINSKIM INFORMACIONIM SISTEMIMA

*mr. ing. Pavle Kostić
Visaris d.o.o., Beograd, SCG*

Sažetak: Elektronska medicinska dokumentacija (elektronski kartoni) sadrži osetljive lične informacije koje mogu biti lako zloupotrebene. Sa druge strane, širok pristup elektronskom kartonu pacijenta od strane medicinskih i drugih profesionalaca koji treba da pruže medicinsku uslugu pacijentu je preduslov za uspešno lečenje. Tako, sa jedne strane postoji potreba ograničenja pristupa podacima iz elektronskog kartona pacijenta, dok sa druge postoji interes pacijenta da što više stručnjaka (iz, po pravilu, različitih organizacija) ima uvid u njegov elektronski karton u cilju što boljeg sagledavanja medicinskog statusa i time što kvalitetnijeg i efikasnijeg donošenje dijagnostičkih i terapijskih odluka. Multiorganizaciona transparentnost, legalni i etički aspekti i odgovornost, nameću složene izazove ne samo u pogledu tehnološke arhitekture medicinskih informacionih sistema. Pri tome, tehnološka arhitektura mora biti usklađena sa etičkim i pravnim standardima koji često nisu u saglasnosti sa tehničko-tehnološkim mogućnostima. Generički mehanizmi zaštite treba da omoguće definisanje standarda i politike korišćenja ličnih medicinskih informacija koji će biti tehnološki skalabilni. Time se postiže maksimalno iskorišćenje tehnološkog razvoja uz smanjenu opasnost od pojave „rupa“ u sistemu zaštite koje mogu dovesti do zloupotreba.

1. Uvod

Mnoge zdravstvene organizacije, od državnog nivoa do nivoa primarne zdravstvene zaštite, razvijaju i uvode razne oblike informacionih sistema i sistema elektronske medicinske dokumentacije (elektronski kartoni pacijenta eng. *Electronic Patient Record - EPR*). Sastavni deo nabavke ili sopstvenog razvoja tih sistema je i proces obezbeđivanja zaštite informacija kao i proces definisanja načina da se smanje rizici i preduprede negativne posledice koje mogu nastati usled neadekvatne zaštite informacija.

Privatnost podataka se odnosi na želju pojedinca da kontroliše publikovanje (javno iznošenje) ličnih zdravstvenih i drugih informacija. Poverljivost se odnosi na informacije - u ovom kontekstu, na mogućnost pojedinca da kontroliše način na koji pružalac zdravstvene usluge (organizacija ili pojedinac) koristi lične informacije kao i dalje širenje tih informacija (izdavanje drugim pojedincima ili organizacijama). Zaštita omogućava osiguranje privatnosti i poverljivosti kroz izbor strategija, procedura i mehanizama zaštite.

Informatička bezbednost se definiše kao „...skup tehničkih i administrativnih procedura ustanovljenih sa ciljem da se podaci zaštite od neovlašćenog ili nenamenskog uvida i otuđenja, izmene ili uništenja kao i radi zaštite funkcionalnosti samog informacionog sistema“ [1]. Posebni ciljevi u naporu da se obezbedi sigurnost odnosno pruži zaštita informacijama, su:

- Očuvanje integriteta podataka
- Jednostavnost pristupa podacima od strane legitimnih korisnika
- Osiguranje privatnosti ličnih podataka kao i njihovog prikladnog korišćenja

Ovi ciljevi se u medicinskoj informatici posebno fokusiraju na specifične aspekte [2]:

- **Dostupnost** koja obezbeđuje tačnu i ažurnu informaciju svakome kome je potrebna i na mestu na kojem je potrebna.
- **Uračunljivost** pomaže da su korisnici odgovorni za njihov pristup i korišćenje informacija po principu potreba i prava da određenu informaciju znaju.
- **Definicija perimetra** omogućava da sistem kontroliše granice poverljivog pristupa, i fizički i logički.
- **Pristup baziran na ulogama** omogućava pristup korisnika samo onim informacijama koje su važne za njihov posao čime se ograničava i sprečava iskušenje da neko neovlašćeno pristupi informacijama koje su van granica njegovih legitimnih potreba.
- **Sveobuhvatnost i kontrola** obezbeđuju da vlasnik elektronske medicinske dokumentacije (organizacija, lekar, med. i paramedicinsko osoblje uključeno u proces prižanja zdravstvene usluge), IT osoblje i pacijenti mogu da razumeju i imaju efektivnu kontrolu nad prikladnim aspektima poverljivosti i pristupa informacijama.

Zaštita podataka i jednostavan, lak, pristup su često suprotstavljeni zahtevi: pojednostavljenje pristupa može ugroziti sigurnost podataka, ako softverska aplikacija nije pažljivo i adekvatno projektovana i implementirana, dok previše rogovatni mehanizmi zaštite najčešće narušavaju ergonomiju aplikacije sa stanovišta korisnika. Veliki deo laika ali i informatičkih profesionalaca, nažalost, ne respektuje kompleksnost zaštite informacija čak i kada razume njen značaj.

2. Metodologija

Uobičajena metodologija za razvoj zaštite ličnih informacija u medicinskim informacionim sistemima se sastoji od šest osnovnih koraka:

1. Identifikacija informatičkih resursa koji zahtevaju zaštitu
2. Deskripcija arhitekture informacionog sistema koji se implementira
3. Identifikacija opasnosti po informacije u sklopu planirane arhitekture
4. Rangiranje opasnosti po značaju i potencijalnoj šteti
5. Dizajniranje rešenja koja treba da smanje rizike i posledice
6. Specifikacija implementacionih preporuka

Izbor optimalne strategije zaštite predstavlja kompromis između nivoa i obima zaštite i potencijalnih rizika i cene posledica u slučaju hazarda. Stoga se često u ovom procesu koriste metodologije analize sistema, procesa, kontrole rizika kao itd.

3. Informacioni resursi

Pre same primene mera obezbeđenja informacija, potrebno je identifikovati same informacije koje je potrebno štititi. Previše široka zaštita koja čuva i informacije koje nisu kritične (njihova (zlo)upotreba ili nekontrolisana izmena ne izazivaju štetne posledice) iziskuje nepotrebne resurse, komplikuje implementaciju i često degradira ukupne

performanse sistema. Stoga je važno naći optimalan odnos između kritičnog skupa informacija i raspoloživih resursa.

Medicinski informacioni sistemi koji sadrže lične informacije (ne samo kliničke, već i socijalne, demografske i druge) moraju primenjivati posebne mere opreza i zaštite kako bi se sprečile potencijalne zloupotrebe koje mogu ugroziti zakonska i ljudska prava (privatnost) pojedinca. Ovde je veoma važno razumeti da se lične informacije ne odnose samo na slučajeve direktne veze jednog skupa podataka za određenu osobu (podaci o osobi), već i na slučajeve kada se ukrštanjem ili analizom podataka ti podaci ili informacije mogu dovesti u vezu sa razumno malim brojem osoba. Dovodjenje u vezu je često znatno složeniji aspekt potencijalnog rizika od zloupotrebe informacija nego sama zaštita podataka.

4. Arhitektura sistema

Informacioni sistem, ili aplikacija, uvek se pojavljuje u kontekstu šireg sistema odnosno njegove arhitekture. Razmena informacija, njihova diseminacija i korišćenje u eksternim sistemima ima značajnu ulogu u povećanju efikasnosti svih poslovnih procesa. U kontekstu potrebe za što širom integracijom informacionih sistema i aplikacija, sve većim zahtevima za slobodnom razmenom informacija i povezivanje sa drugim izvorima podataka, raste i rizik od zloupotrebe ili oštećenja informacija.

Arhitektura informacionog sistema predstavlja plan ostvarenja vizije buduće funkcionalnosti sistem kroz sprovođenje potrebnih nabavki (što uključuje i sopstveni razvoj) i implementacije komponenti i elemenata sistema. Proces nabavke se sprovodi kroz standardnu proceduru investicionog odlučivanja koja treba da obezbedi potrebnu tehnologiju (tehniku - hardver, softver i komunikacije - ali i ljude koji su sposobni da ta sredstva na najefikasniji način primene).

Neadekvatna sredstva i/ili nestručna upotreba predstavljaju najveći faktor rizika za funkcionalnost sistema i bezbednost podataka. Najčešće havarije nastaju kao posledica potpunog odsustva svesti o postojanju nestručnog pristupa ili improvizovanih rešenja. Stoga je profesionalno dizajniranje arhitekture i njeno striktno poštovanje u osnovi planiranja i sprovođenja mehanizama zaštite.

5. Identifikacija rizika

Rizik je mogućnost da dođe do materijalne ili nematerijalne štete usled neplanirane izmene ili gubitka informacija. Odnosi se na situaciju ljudske greške ili namerne akcije, kao i na okolnosti tehničkih ili prirodnih faktora koji mogu izazvati štetu.

Prvi korak u kontroli rizika je razumevanje šta je to rizično (potencijalno opasno) po poslovni proces, poslovne ciljeve ili resurse organizacije. Nakon toga, sprovodi se sveobuhvatna evaluacija ili istraživanje rizika što dovodi do identifikacije rizika. Nakon početne identifikacije, vrši se izrada planova za umanjeње rizika koji mogu imati najštetnije posledice (određivanje prioriteta). Ovakav kontinualni proces identifikacije rizika i razvoja planova za njihovo otklanjanje se definiše kao kontrola (upravljanje) rizika.

Najčešće, zdravstvene organizacije ne sagledavaju sve potencijalne rizike i ne formulišu colovitu i sveobuhvatnu strategiju kontrole rizika. Važno je razumeti da samo sveobuhvatan pristup, čak i sa elementarnim mehanizmima zaštite, znači mnogo više od parcijalnog rešavanja problema (čak i sa najskupljim mehanizmima).

Jedna od metodologija evaluacije rizika (OCTAVE - Operationally Critical Threat, Asset, and Vulnerability Evaluation) omogućava istraživanje organizacionih i tehnoloških aspekata radi sinteze sveobuhvatne slike potreba informatičke bezbednosti. Osnovne faze OCTAVE metodologije obuhvataju [3]:

- Izgradnja profila opasnosti za resurse – Ovde se evaluiraju organizaciona svojstva sistema. Istražuju se osnovni informatički zahtevi po stručnim segmentima organizacije, opasnosti po ključne informacione resurse koji su vezani za te domene, bezbednosne mere koje su potrebne, trenutno primenjene mere kao i organizacione slabosti i ranjivosti u organizacionom smislu (organizaciona ranjivost).
- Pronalaženje slabosti u infrastrukturi – Ovde se evaluira informatička infrastruktura. Ključne komponente infrastrukture (serveri, radne stanice, mreža, eksterne komunikacije, operativni sistemi, baze podataka itd.) se istražuju radi pronalaženja slabosti i „rupa“ (tehnološka ranjivost) koje mogu dovesti do neplaniranih aktivnosti na nivou informacionog sistema.
- Razvoj sigurnosne strategije i plana – U ovoj fazi se analiziraju svi uočeni rizici. Informacije sakupljene u organizacionoj i tehnološkoj evaluaciji (faze 1 i 2) se analiziraju sa aspekta identifikacije rizika i da bi se procenio značaj svakog rizika na ukupne interese organizacije. Paralelno se razvija strategija zaštite i planovi za izbegavanje pojedinih opasnosti saglasno prioritetu pojedinih rizika.

6. Mehanizmi zaštite

Mehanizmi zaštite su organizacione i tehnološke mere koje se preduzimaju radi smanjenja rizika i otklanjanja uzroka rizika. Vrlo često se, nepravilno, smatra da su tehnološki mehanizmi zaštite sami po sebi dovoljni odbrambeni mehanizam. Većina šteta koje nastaju kao posledica zloupotrebe informacija (ne gubitka ili oštećenja) su posledica ljudskog faktora, ili iz razloga neprofesionalne primene tehnoloških mehanizama zaštite ili zbog organizacionih propusta.

Organizacioni mehanizmi zaštite podrazumevaju planiranje pravila i procedura koje se odnose kako na IT osoblje u svakodnevnom administriranju sistema tako i na korisničku politiku tj. pravila i prava u korišćenju informacija.

Tehnološki mehanizmi treba da obezbede pouzdanu i kontrolisanu funkciju svih komponenti sistema i time sistema u celini. Primeri tehnoloških mehanizama zaštite (tehnologija zaštite) su: antivirusni programi (aplikacija), RAID kontroler (uređaj), Firewall (servis), Smart-kartica (medijum), PKI (standard), SSL (mrežni protokol) itd.

U sklopu funkcionalnosti sistema se onda obezbeđuju i potrebni mehanizmi za primenu i sprovođenje organizacionih mehanizama zaštite. Naglasimo da to znači da se sprovođenje organizacione zaštite informacija bazira na planskoj ugradnji potrebnih funkcionalnosti sistema, odnosno da bez pravilnog dizajna arhitekture, planiranja i sprovođenje

implementacije (koja garantuje dosledno ispunjenje svih dizajniranih funkcionalnosti) nema pouzdane zaštite.

Generičke funkcionalnosti se mogu realizovati, manje ili više efikasno, različitim tehnološkim mehanizmima odnosno rešenjima. Generičke funkcionalnosti su veoma stabilne, odnosno ne menjaju se radikalno sa promenom tehnologije. To omogućava da strategija zaštite bazirana na generičkim mehanizmima ne zahteva stalne izmene i revizije procedura (organizacionih mehanizama) usled napretka tehnologije, već tehnološki napredak samo stabilno podiže nivo i efikasnost zaštite. Ovo je veoma važno jer u praksi najveći problem i energiju zahteva uvođenje procedura, odnosno privikavanje korisnika na dosledno sprovođenje politike upotrebe sistema i raspolaganja informacijama. Tehniku i tehnologiju je lakše menjati nego ljudske navike.

Većina savremenih ICT infrastrukturnih komponenti (OS, DBMS, mrežni uređaji itd.) obezbeđuju generičke zaštitne funkcionalnosti. Zato je pre izbora konkretnih komponenti neophodno stručno proceniti stvarni nivo sigurnosnih mehanizama koje generička funkcionalnost uređaja podrazumeva. Sama generička funkcionalnost ne podrazumeva i stvarnu efektivnu zaštitu koju konkretna komponenta omogućava. Laički i neprofesionalni pristup stvara iluziju zaštite dok se u stvarnosti pojavljuju visok faktor rizika od "upada" upravo kroz "sigurnu" komponentu.

7. Zaključak

Bezbednost i zaštita informacija u medicinskim informacionim sistemima je veoma važan aspekt koji treba posebno planirati i razmatrati u implementaciji bilo kog sistema ili aplikacije. Opisana metodologija razvoja prikladne politike zaštite informacija je opšta u načelu ali je veoma pogodna za primenu u aktuelnim projektima koji se sprovode u našim zdravstvenim ustanovama. Poseban akcenat je stavljen na razumevanje balansa između potreba, mogućnosti i potencijalnih rizika. U uslovima ograničenih sredstava, što je svakako slučaj u našim zdravstvenim organizacijama, pravilno planiranje bezbednosne politike informacionog sistema pre ulaska u nabavku opreme i aplikativnih rešenja je od suštinskog značaja ne samo sa aspekta racionalizacije troškova nabavke samih resursa, već i sa aspekta smanjenja rizika od problema i šteta koje će se pojaviti u budućnosti.

Literatura

- [1] Lawrence O. Gostin et al., "*Privacy and Security of Personal Information in a New Health Care System*," Journal of the American Medical Association, 270(20), Nov. 24, 1993, p 2487.
- [2] Medical Informatics, Edward H. Shortliffe and Laslie E. Perreault, Springer, NY USA, 2001, p 174
- [3] Managing Information Security Risks: The OCTAVE Approach, Christopher Alberts and Audrey Dorofee, Addison Wesley Professional, 2002, p 152