Priporočilni standardi SUVI in dopolnitve za področje varnosti v zdravstveni informatiki

Andrej Orel, Marand d.o.o., Ljubljana, Slovenija
Igor Bernik, Fakulteta za varnostne vede, Univerza v Mariboru, Slovenija

Namen in cilj prispevka
Leta 2008 je bil uveden standard ISO/IEC 27799, ki vsebuje priporočila za upravljanje sistemov informacijske varnosti (SUVI) v zdravstveno varstvenih okoljih. Ta standard predstavlja dopolnitev priporočil ISO/IEC 27002 povezanih z varnostmi kontrolami, ter povzema in dopolnjuje tiste elemente SUVI, ki so specifični za področje zdravstva. V prispevku smo se z analizo obeh standardov (ISO/IEC 27002 in ISO/IEC 27799) dotaknili dopolnitev in izpostavili pomembnost posebnega standarda za varovanje informacij v zdravstvu.

Metodologija
V prispevku so obdelana priporočila za varnostne kontrole in njihovih dopolnitev s pomočjo komparativne analize obeh standardov (ISO/IEC 27002 in ISO/IEC 27799). S pomočjo deskripcije so predstavljene ugotovitve, navedene so značilnosti upravljanja varovanja informacij, ki so posebne v zdravstveno varstvenih okoljih.

Ugotovitve in omejitve
V prispevku ugotovljamo, da sta področji upravljanja z informacijsko varnostjo in zdravstvena informatika preko teh dveh standardov zelo povezani. V prispevku so prikazani samo krovni izsledki analize dopolnitev ISO/IEC 27799.

Izvirnost
Prispevek prikazuje povezavo med standardoma – ISO/IEC 27002 (Kodeks za upravljanje varovanja informacij) in ISO/IEC 27799 (Upravljanje informacijske varnosti v zdravstvu z uporabo standarda). Izvirnost se kaže v tem, da je na omenjenem področju malo napisanega, da je v slovenskem prostoru upravljanje z informacijsko varnostjo v zdravstvu šele v povojih in da za to področje ne obstajajo normativni slovenski prevodi ali uradno izrazoslovje.

Ključne besede: ISO/IEC 27001, ISO/IEC 27799, informacijska varnost, zdravstvena informatika

1 UVOD

ISO/IEC 27001 je standard namenjen sistemom upravljanja varovanja informacij (SUVI), medtem ko v standardu ISO/IEC 27002 najdemo predvsem vodila za izvedbo varnostnih kontrol, ki so primerne za organizacije, ki so se odločile za implementacijo SUVI. ISO/IEC 27002 je široko uporabljan in mednarodno priznani standard, ki vsebuje nabor referenčnih kontrol za potrebe upravljanja varovanja informacij, primernih za večino situacij v različnih branžah. Te kontrole so povzete tudi v prilogi standarda ISO/IEC 27001, ki je najbolj razširjen standard za certificiranje sistemov upravljanja varovanja informacij.

ISO/IEC 27799 je komplementarni standard k že omenjenima ISO/IEC 27001 in ISO/IEC 27002. Ukvarja se z vodili za upravljanje varovanja informacij na področju osebnega zdravja. Že v samem naslovu standarda ISO/IEC 27799 je zapisano: »Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002« (SIST, 2008), kar pomeni, da ta standard ne zamenjuje, ampak zgolj dopolnjuje ISO/IEC 27002 na specifičnem področju zdravstveno varstvenih sistemov.
Nobeden izmed standardov SUVI nima uradnega slovenskega prevoda, zato se pri slovenskem izrazoslovju zanašamo predvsem na dva neuradna prevoda standardov (IZIV, 2006) in izrazoslovje, ki živi in je bolj ali manj sprejeto v stanovskem krogu presojevalcev SUVI v okviru enega izmed

slovenskih certifikacijskih organov. Za mnoge izraze se uporablja več sprejetih izrazov, ki se enakovredno uporabljajo in tako pripomorejo k pestrosti jezika.

2 UPRAVLJANJE VAROVANJA INFORMACIJ V ZDRAVSTVU

Že odkar so se informacijski sistemi vključili v zdravstvo kot njegov nepogrešljiv del, je varnost, povezana z obdelovanimi podatki, veljala za zelo pomembno. To se kaže še posebej v luči dejstva, da so ti podatki zelo občutljivi. V sodobnem času je (tudi politično) sprejeto dejstvo, da bolnik predstavlja osrednjo točko zdravstveno varstvenega sistema, kar pomeni da v mora v zdravstvenih informacijah imeti prednost zasebnost in varnost (COACH, 2011). Edinstvene potrebe po varnosti v zdravstvu je treba raziskati in jih videti v različnih strukturah, ki podpirajo zdravstveno dejavnost. Odločitve, sprejete v posamezni zdravstveno informacijski enoti, temeljijo tudi na informacijah iz drugih subjektov. Med njimi so predvsem izvajalci zdravstvenih storitev, pa tudi zdravstvene zavarovalnice in različne z zdravstvom povezane administrativne institucije.
K subjektom zdravstvenega varstva, kjer v prvi vrsti razumemo izvajalce zdravstvenih storitev, sodijo različni zunanji ali notranji dobavitelji materiala in uslug. Storitve izvajajo zdravniki, medicinske sestre in terapevti. Vse to vodijo ali spremljajo administratorji, poslovni vodje in drugo osebje. Informacije o bolniku krožijo med vsemi omenjenimi, ki te informacije v celoti ali delno obdelujejo in jih posredujejo dalje. Razumevanje vseh dejavnikov napeljuje k misli, da je informacijsko varnost v zdravstvu potrebno voditi celovito, z upoštevanjem specifik, ki jih ima zdravstveni sektor, v primerjavi z ostalimi branžami. Izjave: »Občutljivost informacij o bolniku je izjemna«, ni potrebno prav posebej zagovarjati.
Obstajata dva glavna cilja v zvezi z varnostjo informacij na področju zdravstvenega varstva (Ålhfeldt, 2007):

- doseganje visokega nivoja varnosti, kar omogoča bolnikom vrhunsko zdravljenje z dostopanjem do ustreznih informacij v pravem času in
- doseganje visokega nivoja bolnikove zasebnosti, kar pomeni da nepooblaščene osebe ne morejo do občutljivih informacij.

Za zdravstveni sektor je značilnih nekaj posebnosti v zvezi z varovanjem informacij (Ministrstvo za zdravje RS, 2011):

- elektronski zdravstveni zapisi so posebej občutljivi,
- zdravljenje se izvaja v velikem številu majhnih organizacij,
- izvajalcev zdravstvenega varstva je veliko in se nahajajo na različnih lokacijah,
- informacije o zdravljenju posameznika krožijo med različnimi izvajalci,
- dostop do podatkov je odvisen od vrste izvajalcev,
- zakonodaja v zvezi z varovanjem osebnih podatkov obravnava zdravstvene podatke na različne in pogosto posebne načine.

Zaradi navedenih ciljev varnosti in posebnih značilnosti, je smiselno uvajanje sistema upravljanje varnosti informacij v zdravstvo.

2.1 ISO/IEC 27799 – priporočila za SUVI v zdravstvu

Mednarodni standard ISO/IEC 27799 (ISO, 2008) vsebuje smernice, namenjene ravnanju zdravstvenih organizacij in drugih varuhov osebnih zdravstvenih informacij, kako najbolje čuvati zaupnost, celovitost in dostopnost teh informacij z implementacijo ISO/IEC 27002. ISO/IEC 27799 (op. p.: v celotnem prispevku se sklicujemo ISO/IEC 27799:2008) se posebej ukvarja s potrebami SUVI v zdravstvu. Čeprav je varovanje informacij pomembno na vseh področjih našega življenja; tako za posameznike, podjetja, institucije kakor tudi celotno družbo, so na področju zdravstva še posebne zahteve, ki jih je potrebno spoštovati in s tem zagotavljati zaupnost, celovitost, preverljivost(!) in dostopnost osebnih zdravstvenih informacij:

- Zaupnost je ključna za zagotavljanje zasebnosti vseh v procesu zdravljenja.
- Celovitost je nujna zaradi zagotavljanja bolnikove varnosti, kjer je pomembno to, da je celotni življenjski cikel informacije preverljiv in sledljiv.
- Dostopnost je pomembna za izvajanje uspešnega zdravljenja.

Vse to mora biti zagotovljeno tudi v posebnih razmerah, na primer ob naravnih nesrečah in izpadih različnih procesnih ali podpornih sistemov (ISO, 2008).
Potrebe po učinkovitem upravljanju informacijske varnosti v zdravstvu se z napredovanjem in modernizacijo tehnologij večajo. Brez brezžičnih povezav in uporabe interneta za vse potrebe, si zdravstva ne moremo več predstavljati. V kolikor teh tehnologij ne vpeljujemo pravilno, nam bodo povzročale dodatna tveganja v povezavi z zaupnostjo, celovitostjo in dostopnostjo zdravstvenih informacij. Vse zdravstvene organizacije si morajo, ne glede na svojo velikost in specifično področje v zdravstvu, postaviti ustrezne kontrole (nadzorstva) za zaščito informacij o zdravljenju oseb, ki so jim bile zaupane. To je lahko še posebej problematično v majhnih sredinah, kjer se posamezniki (medicinsko osebje) posvečajo zgolj zdravljenju, varovanje informacij pa se jim zdi morda le drugotnega pomena. Ta ugotovitev seveda ne ustreza zahtevam po varovanju informacij in ni sprejemljiva. Vsaka zdravstveno varstvena institucija mora imetij jasna, enoumna in svojemu delovnemu procesu primerna vodila za izbor in vpeljavo tovrstnih kontrol. Izkušnje v razvitih državah so pokazale, da so vodila za izbor informacijsko varstvenih kontrol, ki so sicer nastajala ločeno od razvoja standarda, podobna. To je bil tudi povod za nastanek posebnega, splošnemu standardu ISO/IEC 27002 komplementarnega standarda za informacijsko varnost v zdravstvu – ISO/IEC 27799.
ISO/IEC 27779 je bil objavljen leta 2008. Razvil ga je tehnični odbor TC125 pri mednarodni standardizacijski organizaciji (ISO). Ta odbor je sicer odgovoren za medicinsko informatiko. Standarde družine ISO 27000 sicer razvija skupni tehnični odbor (JTC1/SC27) dveh standardizacijskih organizacij – ISO in IEC, zato imajo vsi ti standardi tudi oznako obeh organizacij in so identični. Predhodnik standarda ISO/IEC 27799 je imel uradni naziv »Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo ISO/IEC 17799«, kar pa se je kasneje (Rowlands, 2007) spremenilo v ISO/IEC 27002 in tako sta obe, sicer načelno ločeni družini, dobili formalno povezavo.
Čeprav ISO/IEC 27799 temelji na ISO/IEC 27002, je njegova struktura drugačna. Začne se s predgovorom in uvodom, ki nista oštevilčena, sledi jima sedem poglavij, oštevilčenih od 1 do 7 (ISO, 2008). Podobno kot pri ISO/IEC 27002, kjer so prva štiri poglavja uvodna, dejanske kontrole pa so razvrščene šele od petega poglavja dalje, je tudi pri ISO/IEC 27799 začetek posvečen razlagi izhodišč za vpeljavo upravljanja informacijske varnosti v zdravstvu. Poglavja od 1 do 6 standarda ISO/IEC 27799 se ukvarjajo z informativni vidiki informacijske varnosti v zdravstvu, kjer najdemo uvod v informacijsko varnost v zdravstvu, namen standarda, normativne reference, uporabljano izrazoslovje s področja zdravstva in informacijske varnosti, različne definicije, ter obsežno razpravo o praktičnih pristopih k uvajanju informacijske varnosti po »Kodeksu za upravljanje varovanja informacij ISO/IEC 27002« (IZIV, 2006).
Glavnina standarda ISO/IEC 27799 (ISO, 2008) se nahaja v poglavju 7 z naslovom »Vključitev ISO/IEC 27002 v zdravstvo«. V tem poglavju se nahajajo posebni nasveti o enajstih poglavjih varnostnih kontrol oziroma 39 glavnih kontrolnih kategorij (skupin), kot jih najdemo v ISO/IEC 27002. Splošni pristop v ISO/IEC 27002 je zasnovan tako, da spodbuja posamezne organizacije k lastnim interpretacijam tega dokumenta znotraj lastnih pravnih in poslovnih zahtev oziroma potreb. Izkušnje so pokazale (Rudel, 2007), da je v okviru zdravstva potrebno nekatere kontrole še posebej zavarovati. Na podlagi izkušenj iz različnih držav, kjer so upravljanju informacijske varnosti posvetili posebno pozornost že pred samim sprejetjem standarda ISO/IEC 27799 (Rowlands, 2007), so v poglavju 7, v delih kjer je to potrebno, zapisane minimalne zahteve. V posameznih primerih so dodana še normativna vodila za posebno apliciranje varnostnih kontrol iz ISO/IEC 27002 v zdravstveno varstvenih okoljih.
Za celovit opis vsebine standarda ISO/IEC je potrebno omeniti še tri priloge (anekse), ki pa so zgolj informativnega značaja:

- Priloga A obravnava grožnje, ki ogrožajo informacije v zdravstvu.
- V prilogi B so grafično ponazorjena navodila in dokumenti povezani s SUVI v različnih fazah po modelu NSPU (Načrtuj, Stori, Preveri, Ukrepaj – PDCA); v fazi vzpostavitve SUVI, v fazi vpeljave in delovanja SUVI, v fazi nadzora in pregledovanja SUVI, ter v fazi vzdrževanja in izboljševanja SUVI.
- Priloga C obravnava potencialne koristi in zahtevane lastnosti podpornih orodij za posamezne procese SUVI.

Sledi jim še bibliografija s povezanimi standardi s področja informacijske varnosti v zdravstvu.

2.2. Primerjava varnostnih kontrol ISO/IEC 27002 in ISO/IEC 27799

Kot rečeno, se varnostne kontrole, zajete v poglavju 7 standarda ISO/IEC 27799, neposredno nanašajo (mapirajo) na poglavja 5 do 15 standarda ISO/IEC 27002 oziroma jih dopolnjujejo. Kako se podpoglavja točke 7 (»Vključitev ISO/IEC 27002 v zdravstvo«) iz ISO/IEC 27799 navezujejo na omenjena poglavja Kodeksa za upravljanje varovanja informacij, je prikazano Tabeli 1. Uporabljeni so neuradni, a splošno sprejeti slovenski nazivi (IZIV, 2006).

Tabela 1: Skupine varnostnih kontrol – ISO/IEC 27002 in ISO/IEC 27799

Točka in poglavje ISO/IEC 27002	Točka in poglavje ISO/IEC 27299
-	7.1 Splošno
5 Varnostna politika	7.2 Informacijska varnostna politika
6 Organizacija varovanja informacij	7.3 Organizacija informacijske varnosti
7 Upravljanje sredstev	7.4 Upravljanje sredstev
8 Varovanje človeških virov	7.5 Varnost človeških virov
9 Fizična zaščita in zaščita okolja	7.6 Fizična zaščita in zaščita okolja
10 Upravljanje s komunikacijami in produkcijo	7.7 Upravljanje s komunikacijami in produkcijo
11 Nadzor dostopa	7.8 Nadzor dostopa
12 Nakup razvoj in vzdrževanje informacijskih sistemov	7.9 Nakup razvoj in vzdrževanje informacijskih sistemov
13 Upravljanje incidentov pri varovanju informacij	7.10 Upravljanje incidentov pri varovanju informacij
14 Upravljanje neprekinjenega poslovanja	7.11 Vidiki informacijske varnosti pri upravljanju neprekinjenega poslovanja
15 Združljivost	7.12 Združljivost

Iz Tabele 1 je razvidno, da so varnostne kontrole v obeh standardih na prvem nivoju dokaj enakomerno porazdeljene. Izjema sta 7.1 in 7.11 (v tabeli osenčeni), kjer imamo samo načelni opis, dejanskih opisov ali dopolnitev kontrol pa ni. Ko pa gremo globlje in si za referenčno razporeditev vzamemo ISO/IEC 27002, je podobnosti manj.

Tabela 2: Število varnostnih kontrol - ISO/IEC 27002 in ISO/IEC 27799

	ISO/IEC 27002	ISO/IEC 27799
Št. poglavij s kontrolami (in brez)	11	10 (12)
Št. skupin kontrol	39	41
Število vseh kontrol	133	136

Formalna primerjava obeh standardov nas pripelje do nekaterih ugotovitev. Večina poglavij, ki se nanašajo na varnostne kontrole, ima v obeh standardih skoraj enake nazive. Kontrole so nekoliko drugače razporejene po skupinah, zato sta v ISO/IEC 27799 dve skupini več, hkrati pa ima ta standard tudi tri dodatne kontrole, v vsakem od poglavij po eno.
Tako se seveda postavi vprašanje, kdaj v zdravstvu uporabiti priporočila ISO/IEC 27002, kdaj pa ISO/IEC 27799. Odgovor je dvoplasten. Po eni strani – nobenega razloga ni, da ne bi uporabljali ISO/IEC 27799, če je to le možno. Po drugi strani, pa se zlasti v praksi izkaže (to trditev bom omejil na slovenski prostor!), pripravljavci podlag za SUVI v zdravstvenih organizacijah tega standarda sploh ne poznajo in tudi ne vedo, kakšne potencialne koristi jim prinaša.

3 SKLEP

V današnjem svetu zdravstvene informatike je polno pasti, ki jih postavljajo vsi trije zadani cilji (zaupnosti, dostopnosti in celovitosti informacij) pred vpletene v zdravstveno varstvo. Ti cilji so si med seboj dokaj kontradiktorni in zahtevajo različno ukrepanje za njihovo doseganje. Zdravstvene

informacije so večinoma še bolj občutljive od ostalih, saj se najpogosteje dotikajo oseb, ki imajo različne probleme in jim ni vseeno, kaj se dogaja z njihovim zdravjem in dobrim počutjem. Zdravje in zdravstvena informacija pa sta, čeprav se večinoma tega ne zavedamo, dva neločljivo povezana pojma. Zdravstvo je v bistvu edino področje, ki ima svoj posebni dopolnilni standard za zagotavljanje informacijske varnosti. Dopolnilni standard upravljanja z informacijsko varnostjo je sicer na voljo tudi za področje telekomunikacij (ISO 27011), vendar pa je šele v fazi pred-standarda (The ISO 27000 Directory, 2011a).), hkrati pa se ne dotika le enega tipa informacij, pri ISO/IEC 27799 govorimo o osebnih zdravstvenih informacijah, temveč celovitega SUVI v telekomunikacijski industriji.
Velika prednost standarda ISO/IEC 27799 je, da je nastajal v okviru delovnih skupin, ki se ukvarjajo posebej z zdravstveno informatiko (Rowlands, 2007), tako v okviru ISO (TC215), kakor tudi CEN (TC251). V teh okoljih predstavlja upravljanje informacijske varnosti le enega izmed vidikov zdravstvene informatike. Na drugi strani imamo znotraj organizacije ISO delovno skupino (oziroma več njih), ki se ukvarja z upravljam informacijske varnosti na splošno in za vse potrebe. V njihovem okolju je nastala družina standardov ISO/IEC 27000 (The ISO 27000 Directory, 2011b). Razveseljujoče je, da je med obema delovnima okoljema nastala sinergična povezava, katere posledica je standard ISO/IEC 27799 - Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002.

VIRI

Åhlfeldt, RM., Söderström, E. (2007). *Information Security Problems and Needs in a Distributed Healthcare Domain – A Case Study*. Pridobljeno 1.12.2011 na ftp://163.25.117.117/gyliao/PaperCollection/20091030/10.1.1.99.8862[1].pdf

Carlson, T. (2008). *Information Security Management: Understanding ISO 17799*. Pridobljeno 8.11.2011 na http://www.netbotz.com/library/ISO_17799.pdf

COACH. (2011) Canada's Health Informatics Association Guidelines for the Protection of Health Information. Pridobljeno 22.10.2011 na https://ams.coachorg.com/inventory/PurchaseDetails.aspx?Id=13d04bfb-3f71-4cbd-a69a-26a961236fe2

IZIV. (2006a). *Prevod standarda BS ISO/IEC 27001:2005: Informacijska tehnologija – Varnostne tehnike – Sistemi za upravljanje varovanja informacij – Zahteve.* Slovenija: Inštitut za informacijsko varnost (IZIV).

IZIV. (2006b). *Prevod standarda BS ISO/IEC 17799:2005: Informacijska tehnologija – Varnostne tehnike – Kodeks za upravljanje varovanja informacij*. Slovenija: Inštitut za informacijsko varnost (IZIV).

ISO 27002. (2005). *ISO/IEC 27002: Information Technology – Security Techniques – Code of Practice for Information Security Management (1st ed.)*. Švica: International Organization for Standardization (ISO).

ISO 27799. (2008). *ISO/IEC 27799: Health informatics — Information security management in health using ISO/IEC 27002 (1st ed.)*. Švica: International Organization for Standardization (ISO).

Ministrstvo za zdravje RS. (2011). *Sistem za upravljanje z informacijsko varnostjo – SUVI / Spletno mesto eZdrav.si*. Pridobljeno 1.12.2011 na http://www.ezdrav.si/?page_id=158

Rowlands, D. (2007). *Report on ISO TC 215 Health Informatics standards development meetings 2007*. Pridobljeno 17.11.2011 na http://www.e-health.standards.org.au/LinkClick.aspx?fileticket=8Rj6_oXnIwg%3D&tabid=145&mid=770

Rudel, D., Kozar, M., Pušnik, S. (2007). Common approach to healthcare information security management in Slovenia using ISO 27799. Bryden, J.S., de Lusingan, S., Blobel, B. (ur.), *Medical informatics in enlarged Europe. Proceedings of the European federation for medical informatics. Special topic conference STC 2007* (str. 114-119). Berlin: Akademische Verlagsgesellschaft.

SIST. (2008). *SIST EN ISO 27799:2008 Zdravstvena informatika – Upravljanje informacijske varnosti v zdravstvu z uporabo standarda ISO/IEC 27002.* Slovenija: Slovenski inštitut za standardizacijo (SIST).

The ISO 27000 Directory, (2011a). *Introduction To ISO 27011 (ISO27011)*. Pridobljeno 15.12.2011 na http://www.27000.org/iso-27011.htm

The ISO 27000 Directory, (2011b). *An Introduction to ISO 27001, ISO 27002....ISO 27008.* Pridobljeno 15.12.2011 na http://www.27000.org/index.htm