UPRAVLJANJE PODACIMA I INFORMACIJAMA U ZDRAVSTVENIM INFORMACIJSKIM SUSTAVIMA REPUBLIKE HRVATSKE - SIGURNOST, ZAŠTITA I ODGOVORNOST

MARIJA BOBAN
Sveučilište u Splitu, Pravni fakultet, Split, Hrvatska
E-pošta: marija.boban@pravst.hr

Sažetak Svaki pružatelj usluga u elektroničkom poslovanju u Republici Hrvatskj i Europskoj uniji, pa tako i pružatelji zdravstvenih usluga, koji koriste računalnu mrežu, obrađuju i pohranjuju razne informacije, svakodnevno su izloženi opasnosti otkrivanja podataka i informacija te samim time. Također, sukladno Općoj uredbi o zaštiti podataka i Zakonu o podacima i informacijama u zdravstvu Republike Hrvatske, moraju implementirati tehničke i organizacijske mjere zašite informacijskih sustava kako bi povećali razinu zaštite podataka. Autorica u radu stavlja naglasak na metodologiju sigurnosti i zaštite podataka te odgovornost u upravljanju rizicima u zdravstvenim informacijskim sustavima primjenom međunarodnih standarda, osobito standarda ISO 27799:2016, gdje se obrada podataka temelji na zakonitim načelima prikupljanja, korištenja i obrade zdravstvenih podataka i informacija sukladno važećem zakonskom okviru u području zaštite osobnih podataka i informacija u zdravstvu kojima se osigurava visoka razina zaštite uz jasno utvrđivanje odgovornosti nadležnih osoba i tijela u upravljanju podacima i informacijama u zdravstvu.

Ključne riječi: informacijski sustavi, obrada osobnih podatka, sigurnost, zaštita, zdravstvo

University of Maribor Press
DOI https://doi.org/10.18690/978-961-286-478-1.12
ISBN 978-961-286-478-1

Data and Information Management in Health Information Systems of the Republic of Croatia - Security, Protection, and Liability

Marija Boban
University of Split, Faculty of Law, Split, Croatia
E-mail: marija.boban@pravst.hr

Abstract Every provider of electronic services in the Republic of Croatia as well as in the European union, including healthcare services providers, is exposed to the risk of data and information disclosure on a daily basis. In accordance with the General Data Protection Regulation and the Law on Data and Information in Health of the Republic of Croatia, they must implement technical and organizational measures to increase the level of data protection. The author in this paper emphasizes the methodology of security and data protection and liability in risk management in health information systems by applying international standards, ISO 27799: 2016 in particular in accordance with the applicable legal framework in the field of protection of personal data and information in health care, which ensures a high level of protection, with a clear identification of the liability of supervisory entities in the management of data and information in health care.

Keywords: information, systems, health care, personal data processing, protection, security

https://doi.org/10.18690/978-961-286-478-1.12 DOI
978-961-286-478-1 ISBN
University of Maribor Press

UPRAVLJANJE PODATKOV IN INFORMACIJ V ZDRAVSTVENIH INFORMACIJSKIH SISTEMIH REPUBLIKE HRVAŠKE - VARNOST, ZAŠČITA IN ODGOVORNOST

MARIJA BOBAN
Univerza v Splitu, Pravna fakulteta, Split, Hrvaška
E-pošta: marija.boban@pravst.hr

Povzetek Vsak ponudnik elektronskih storitev, vključno s ponudniki zdravstvenih storitev, ki uporablja računalniško omrežje, obdeluje in shranjuje različne informacije, predvsem osebne podatke, je izpostavljen nevarnostim odkrivanja podatkov in informacij na dnevni osnovi, zato morajo v skladu z splošno Uredbo o varstvu podatkov in zakonom o podatkih in informacijah na področju zdravja Republike Hrvaške izvajati tehnične in organizacijske ukrepe za zaščito informacijskih sistemov, da bi povečali raven varstva teh podatkov. Avtorica se osredotoča na metodologijo za varnost in varstvo podatkov ter odgovornost za obvladovanje tveganj v zdravstvenih informacijskih sistemih z uporabo mednarodnih standardov, zlasti standardov ISO 27799:2016, kjer obdelava podatkov temelji na pravnih načelih za zbiranje, uporabo in obdelavo zdravstvenih podatkov in informacij v skladu s sedaj veljavnim pravnim okvirom na področju varstva osebnih podatkov in informacij o zdravju, ki zagotavlja visoko raven zaščite, z jasno opredelitvijo odgovornosti nadzornih organov pri upravljanju podatkov in informacij v zdravstvu.

Ključne besede:
informacijski sistemi,
obdelava osebnih podatkov,
varnost,
zaščita,
zdravje

Univerzitetna založba Univerze v Mariboru

DOI https://doi.org/10.18690/978-961-286-478-1.12
ISBN 978-961-286-478-1

1 Uvod

Zdravstvene informacijske sustave u Republici Hrvatskoj možemo definirati kao stručne zdravstvene postupke i procese koji su podržani informatičko – komunikacijskim uslugama. Obuhvaća informacijske sustave u zdravstvenim ustanovama, uključujući razmjenu elektroničkim zdravstvenim zapisom, i distribuciju zdravstvenih informacija (Boban, 2019: 41-72). Omogućuje kvalitetnije i učinkovitije pružanje zdravstvene skrbi te bolju komunikaciju svih sudionika u zdravstvu na dobrobit pacijenata. Međutim, rukovanje osobnim podacima nosi sa sobom određene rizike i izazove. Zloupotreba osobnih podataka o zdravstvenom stanju može prouzročiti štetu, ne samo osobi kao pojedincu, već i članovima njegove obitelji (Končar, 2011).

Zdravstvo obiluje informacijama koje nastaju kao rezultat direktnog rada s bolesnikom, ali i kao rezultat stručnih sastanaka, konzultacija zdravstvenih djelatnika i pisanih materijala poput raznih izvješća. Ipak, direktni rad s bolesnikom je najbogatiji izvor informacija u zdravstvu. Zdravstveni djelatnici prikupljaju podatke, pohranjuju ih u medicinske zapise te koriste postojeće ili dodaju nove podatke (Kičić, 2014: 65-68). S obzirom da se zdravstvena zaštita provodi dislocirano, jedan dio tih podataka putuje na drugu lokaciju, primjerice u drugu zdravstvenu ustanovu iz koje često dolazi povratna informacija.

U informatiziranom zdravstvu informacije putuju mrežom, a takav način komunikacije zahtijeva zaštitu samog sustava, a što podrazumijeva zaštitu podataka koji se prenose i zaštitu komunikacijskih kanala. Zaštita podataka u komunikaciji ima tri dimenzije i to: dostupnost, povjerljivost i integritet, te tri načina regulacije: sigurnosni, pravni i etički. Dostupnost podataka podrazumijeva pravo i mogućnost da se pročita podatak zabilježen u medicinskom zapisu. Povjerljivost znači pravo da se štiti pravo bolesnika na privatnost. Integritet uključuje pravo unosa novih podataka u medicinski zapis bolesnika odnosno eventualne promjene u zapisu. Sigurnosna regulacija zaštite podataka uključuje fizičku zaštitu, uporabu lozinke te osiguravanje podataka (primjerice asimetrično kriptiranje). Pravna zaštita podataka zahtijeva zakone koji reguliraju prava i obveze onih koji pristupaju s podacima, dok etički aspekt zaštite podataka regulira ono što zakon izostavlja. Na tom tragu u veljači 2019. donesen je Zakon o podacima i informacijama u zdravstvu (Narodne novine 14/19 – dalje ZPIZ) koji uz Opću uredbu o zaštiti podataka (EU) 2016/679 dodatno

regulira upravljanje podacima i informacijama u zdravstvu i samim time zaštitu podataka pacijenata diže na višu razinu.

2 Sigurnost i zaštita podataka i informacija u zdravstvenim informacijskim sustavima

2.1 Sigurnosni izazovi u zdravstvu

Nagla ekspanzija trenda neovlaštene obrade velikih količina osobnih podataka poprimila je zabrinjavajuće razmjere na globalnoj razini. U današnjem suvremenom društvu organizacije sve više ovise o informacijsko – komunikacijskoj tehnologiji. Jedno od ključnih pitanja informatizacije zdravstva je sigurnost i to pitanje gdje se čuvaju osobni podaci, kome su sve i na koji način dostupni. Temeljni cilj zaštite informacijskih sustava u zdravstvu je zaštititi povjerljivost, dostupnost i integritet informacija o pacijentu. U zaštiti informacija potrebno je voditi računa o svim elementima sustava, odnosno o pacijentima, zaposlenicima, javnosti, poštivanju zakona i drugih propisa. Svi sudionici sustava moraju biti zadovoljeni u kontekstu zaštite integriteta, te zaštite i dostupnosti informacija (Čizmić, Boban & Zlatović, 2016: 550).

2.2 Upravljanje rizicima i zaštita podataka u zdravstvenim informacijskim sustavima

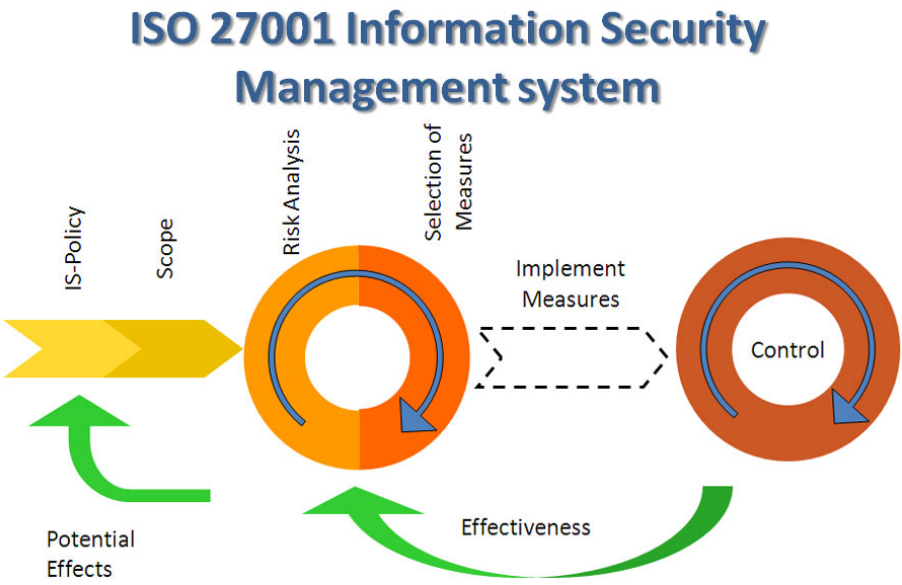
Prilikom zaštite podataka potrebno je voditi računa o riziku sigurnosti osobnih podataka. Taj rizik proizlazi iz ranjivosti sustava i posljedica koje može prouzročiti. U zdravstvenim ustanovama najčešće postoji rizik od nedostupnosti podataka, neovlaštenog pristupa podacima i neovlaštenog mijenjanja podataka. Kako bi se ti rizici sveli na prihvatljivu razinu, potrebno je upravljati rizicima.

Tri su osnovna mehanizma za upravljanje rizicima:

- BSC (Balanced Scorecard) – strateška razina;
- COBIT 4.1 + IT Risk (COBIT 5.0) – taktička razina;

– ISO 27799: 2016 — Health informatics — Information security management in health using ISO/IEC 27002 (second edition) – operativna razina – konkretne aktivnosti (Božić, 2013: 220).

Informacijska sigurnost definirana je najšire u međunarodnom standardu ISO/IEC 27001:2013 punim nazivom [ISO/IEC 27001:2013] - Information technology — Security techniques — Information security management systems — Requirements koji specificira zahtjeve za uspostavljanje, provedbu, održavanje i kontinuirano poboljšavanje sustava upravljanja informacijskom sigurnošću u kontekstu organizacije uspostavljajući sustav upravljanja informacijskom sigurnošću (engl. *Information Security Management System*) - dalje ISMS. Uključuje i zahtjeve za procjenu i postupanje s rizicima informacijske sigurnosti prilagođenim potrebama organizacije. Zahtjevi iz ISO / IEC 27001: 2013 su općeniti i trebaju se primjenjivati na sve organizacije, bez obzira na vrstu, veličinu ili prirodu (Kenyon, 2019: 15-20).



Slika 1: ISO 27001 Information Security Management System
(preuzeto sa https://avkashk.wordpress.com/information-security-management-systemiso-27001/) (16.01.2020)

Kao i kod svih procesa upravljanja, ISMS (Humphreys, 2016: 101) mora dugoročno ostati učinkovit i efikasan, prilagođavajući se promjenama u unutarnjoj organizaciji i vanjskom okruženju. ISO / IEC 27001: 2013 je, dakle, uključio „Plan-Do-Check-Act" (PDCA) ili Demingov pristup:

- Faza PLAN ('planiranja") odnosi se na osmišljavanje ISMS-a, procjenu rizika od informacijske sigurnosti i odabir odgovarajuće kontrole.
- Faza DO ('implementacije')uključuje provedbu i upravljanje kontrolama.
- Cilj faze CHECK (provjere) je pregledati i procijeniti uspješnost (učinkovitost i djelotvornost) ISMS-a.
- U fazi ACT („uvođenje") izmjene se uvode po potrebi kako bi se ISMS vratio do vrhunskih performansi.[1]

Prijetnje sigurnosti osobnih podataka u zdravstvenim ustanovama su specifične. One obuhvaćaju: namjerne i slučajne ljudske radnje unutar i izvan organizacije kao što su krađe podataka unutar organizacije i izvan nje, neovlašteni pristup podacima kao što je primjerice ostanak u programu nakon prestanka rada pa se drugi zaposlenik koristi programom pod tuđom lozinkom, nehotično slanje podataka na krive adrese, problemi sustava poput tehničkih greški, greški u funkcioniranju sustava, hardverske i softverske greške, zatim drugi problemi kao što su greške u održavanju, greške zaposlenika i sl. (Gallotti, 2019: 23). Stoga se upravljanje sigurnošću podataka u zdravstvu ne svodi se samo na sigurnost korisničkih imena i lozinki, već je potrebno voditi računa i o razvijanju svijesti o informacijskoj sigurnosti, provedbi edukacija o informacijskoj sigurnosti, kontroli pristupa podacima, provedbi disciplinskog postupka za kršenje sigurnosti, inzistirati na odgovornosti i ukidanju prava pristupa podacima (Tan, 2005: 91).

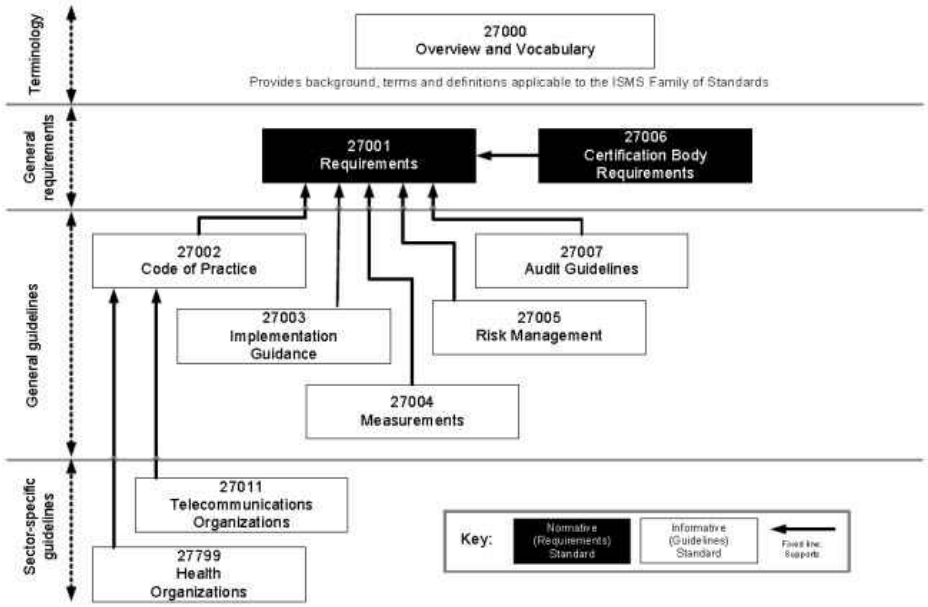
Osim osobnih podataka pacijenata potrebno je osigurati sustav zaštite podataka o pacijentima koji su prikupljeni za potrebe nekih istraživanja (statističkih ili kliničkih), podatke koji služe za donošenje odluka u klinici, te informacije o zdravstvenim djelatnicima, ostalom osoblju i volonterima. Kao glavne preporuke za čuvanje sigurnosti baze podataka su stalna nadogradnja programskih paketa, odvajanje baze na sigurne segmente mreže, korištenje enkripcije pri transferu i skladištenju podataka

[1] Definicija ISMS-a prema https://avkashk.wordpress.com/information-security-management-systemiso-27001/ (16.01.2020).

te korištenje autorizacije autentifikacije i uloga za pristup bazama. Također, preporučljivo je redovito mijenjati lozinke za pristup bazama podataka, primjerice svaka tri mjeseca s time da se ne mogu ponavljati one lozinke koje je korisnik koristio ranije (Adams, Purtova & Leenes, 2016).

2.3 Međunarodni standard ISO 27799:2016 i upravljanje podacima i informacijama u zdravstvenim informacijskim sustavima

ISO 27799: 2016 daje smjernice za organizacijske standarde informacijske sigurnosti i prakse upravljanja informacijskom sigurnošću, uključujući odabir, primjenu i upravljanje kontrolama uzimajući u obzir okruženje rizika informacijske sigurnosti organizacije (kako je i prikazano na Slici 2.) (Tamò-Larrieux, 2018).



Slika 2. Pregled standarda 27000 – od općenitih prema specifičnih prema sektorima
(preuzeto sa http://zdenkoadelsberger.blogspot.com/2009/05/osvrt-na-tekst-zasto-iso-27001-mozda.html) (17.01.2020)

U njemu su definirane smjernice za podršku tumačenja i primjene u zdravstvenoj informatici ISO/IEC 27002 i pridružuju se tom međunarodnom standardu. Temeljen je na smjernicama za provedbu kontrola opisanih u ISO/IEC 27002 i dopunjava ih po potrebi kako bi se mogle učinkovito koristiti za upravljanje sigurnošću zdravlja. Primjenom ISO 27799: 2016 zdravstvene organizacije i ostale institucije koje obrađuju podatke i informacije u zdravstvu moći će osigurati minimalnu potrebnu razinu sigurnosti koja je primjerena okolnostima njihove organizacije i koja će održavati povjerljivost, integritet i dostupnost osobnih zdravstvenih podataka u njihovoj skrbi. Primjenjuje se na podatke i informacije u zdravstvu, bez obzira na oblik informacije (riječi i brojevi, zvučni snimci, crteži, videozapisi i medicinske slike), bez obzira na sredstva koja se koriste za njihovo pohranjivanje (ispis ili ručnu obradu na papiru ili spremanje u elektroničkom obliku), i koja god sredstva koja se koriste za prijenos (ručno, faksom, računalnim mrežama ili poštom), jer su podaci uvijek na odgovarajući način zaštićeni (Weiss & Solomon, 2015: 89).

Međunarodni standardi ISO 27799: 2016 i ISO/IEC 27002 zajedno definiraju što je potrebno kako bi se postigao sustav zaštite u pogledu sigurnosti informacija u zdravstvu, ali ne definiraju kako se ti zahtjevi trebaju ispuniti. To znači, u najvećoj mogućoj mjeri, ISO 27799: 2016 je neutralan u odnosu na tehnologiju i orijentiran je procedurama i zahtjevima zaštite podataka i informacija u zdravstvu.[2]

3 Pravni okvir zaštite podataka i informacija u zdravstvu

Od veljače 2019. na snazi je Zakon o podacima i informacijama u zdravstvu čime se definiraju prava, obveze i odgovornosti pravnih i fizičkih osoba zdravstvenog sustava Republike Hrvatske u području upravljanja podacima i informacijama u zdravstvu, pojmovi i temeljna načela prikupljanja, korištenja i obrade zdravstvenih podataka i informacija, nadležna tijela, kvaliteta i obrada zdravstvenih podataka, njihova zaštita te inspekcijski i stručni nadzor, radi sveobuhvatnog i djelotvornog korištenja zdravstvenih podataka i informacija u zdravstvenoj zaštiti radi unaprjeđenja i očuvanja zdravlja stanovništva u Republici Hrvatskoj (ZPIZ, čl. 1).

[2] Prema podacima na službenoj stranici ISO.org https://www.iso.org/standard/62777.html (15.01.2020).

Važno je naglasiti kako u okviru zaštite osobnih podataka posebno mjesto zauzima zaštita medicinskih osobnih podataka. Podaci o zdravstvenom stanju su vrlo značajni i spadaju u specifične podatke te su potrebne stroge norme koje će regulirati pristup tim podacima. Kako bi se omogućilo što kvalitetnije liječenje, liječniku moraju biti dostupni mnogi pacijentovi osobni podaci osjetljivog karaktera te je nužno potpuno povjerenje pacijenata u tajnost i zaštićenost tih podataka. Zaštita osobnih podataka koji se odnose na pacijentovo zdravstveno stanje provodi se sa svrhom zaštite prava na privatnost osobnog i obiteljskog života, koja je jedno od osobnih prava koje se štiti hrvatskim pravnim poretkom. Čuvanje pacijentove privatnosti sadrži u sebi pravo na povjerljivost i privatnost informacija o zdravstvenom stanju, medicinskom statusu, obiteljskim prilikama, tijeku liječenja i prognozi ishoda liječenja (SEISMED Consortium, Data Security for Health Care, 1996: 63).

Život i zdravlje ljudi važne su ustavnopravne kategorije. Iako je zaštita privatnosti u liječničkoj profesiji značajna još od 4. stoljeća prije Krista (kada je postavljena Hipokratova zakletva, a o čemu će biti više opisano u nastavku teksta), to danas postaje sve teže budući da je u postupak liječenja uključen sve veći broj stručnjaka. Vrlo često podaci o zdravstvenom stanju moraju biti dostupni i izvan liječničkih ordinacija kao što su primjerice osiguravajuća društva (Institute of Medicine, 2001: 40). Informatizacija u zdravstvu uvelike olakšava liječenje, ali donosi nove rizike i daleko veću odgovornost.

3.1 Zaštita osobnih podataka pacijenata u pravnom okviru Republike Hrvatske

Svrha zaštite osobnih podataka je zaštita privatnog života i ostalih ljudskih prava i temeljnih sloboda u prikupljanju, obradi i korištenju osobnih podataka.[3] Zaštita osobnih podataka u Republici Hrvatskoj je ustavna kategorija koja je osigurana svakoj fizičkoj osobi bez obzira na državljanstvo i prebivalište, neovisno o rasi, boje kože, spolu, jeziku, vjeri, političkom ili drugom uvjerenju, nacionalnom ili socijalnom podrijetlu, imovini, rođenju, naobrazbi, društvenom položaju ili osobinama. Ustav Republike Hrvatske (Narodne novine 56/90, 135/97, 08/98, 113/00, 124/00,

[3] Osim definicije osobnih podataka, zakonodavac je još od 2003.g. jasno definirao i pojmove što je obrada podataka, zbirka osobnih podataka, voditelj zbirke osobnih podataka, korisnik i privola ispitanika. Vidi Zakon o zaštiti osobnih podataka, pročišćeni tekst, NN 103/03, 118/06, 41/08, 130/11, 106/12 – prestao važiti 25.05.2018.

28/01, 41/01, 55/01, 76/10, 85/10, 05/14) u članku 37 jasno navodi: „Svakom se jamči sigurnost i tajnost osobnih podataka. Bez privole ispitanika osobni se podaci mogu prikupljati, obrađivati i koristiti samo uz uvjete određene zakonom. Zakonom se određuje zaštita podataka te nadzor nad djelovanjem informatičkih sustava u državi. Zabranjena je uporaba osobnih podataka suprotna utvrđenoj svrsi njihova prikupljanja." Ustav RH, čl. 37.

Temeljem ustavne odredbe o zaštiti osobnih podataka 2003.g. donesen je Zakon o zaštiti osobnih podataka (Narodne novine 103/03, 118/06, 41/08, 130/11, 106/12) kao temeljni akt kojim se uređivalo prikupljanje, obradu, korištenje i zaštitu osobnih podataka te nadzor nad njihovom obradom.[4] Navedeni Zakon o zaštiti osobnih podataka prestao je važiti 25. svibnja 2018.g. a zamijenila ga je Uredba 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (dalje u tekstu - *Opća uredba o zaštiti podataka* - GDPR). Opća uredba o zaštiti podataka nastala je kao posljedica neujednačene prakse zaštite osobnih podataka u zemljama Europske unije. Osnovna ideja je sprječavanje narušavanja povjerljivosti i integriteta osobnih podataka kao i sprječavanje neovlaštene dostupnosti te osiguravanje nesmetane dostupnosti osobnih podataka onima koji imaju ovlaštenja. Općom uredbom o zaštiti podataka[5] želi se doprinijeti uspostavi područja slobode, sigurnosti i pravde prvenstveno kako bi se osigurala postojana i visoka razina zaštite pojedinaca te uklonile prepreke protoku osobnih podataka unutar Unije, razina zaštite prava i sloboda pojedinaca u vezi s obradom takvih podataka trebala bi biti jednaka u svim državama članicama. U čitavoj Uniji trebalo bi osigurati postojanu i homogenu primjenu pravila za zaštitu temeljnih prava i sloboda pojedinaca u vezi s obradom osobnih podataka. U pogledu obrade osobnih podataka za usklađivanje s pravnom obvezom, za izvršavanje zadaće od javnog interesa ili pri obavljanju službene ovlasti dodijeljene voditelju obrade državama članicama trebalo bi dopustiti da zadrže ili uvedu nacionalne odredbe kako bi se dodatno odredila primjena pravila iz ove Uredbe. Zajedno s općim i

[4] Zakon o zaštiti osobnih podataka, pročišćeni tekst, NN 103/03, 118/06, 41/08, 130/11, 106/12 – stavljen van snage 25. svibnja 2018.

[5] Službeni list Europske unije, UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ. Dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR (20.01.2020).

horizontalnim zakonodavstvom o zaštiti podataka kojim se provodi Direktiva 95/46/EZ, države članice imaju nekoliko posebnih zakona za pojedine sektore u onim područjima u kojima su potrebne konkretnije odredbe. Ovom Uredbom također se državama članicama pruža prostor za djelovanje kako bi bolje odredile njezina pravila uključujući obradu posebnih kategorija osobnih podataka („osjetljivi podaci"). U tom smislu ovom se Uredbom ne isključuje pravo države članice kojim se utvrđuju okolnosti posebnih situacija obrade, što uključuje preciznije određivanje uvjeta pod kojima je obrada osobnih podataka zakonita (Preambula, točka 10).[6]

Ispunjavanje zahtjeva Opće uredbe o zaštiti podataka zahtijeva angažiranost cijele organizacije te je potrebno poduzeti nekoliko ključnih koraka. Ključni koraci ka usklađenosti su: definiranje projekta, analiza postojećeg stanja, donošenje strategije, implementacija strategije i aktivno provođenje strategije. Postoji obveza imenovanja službenika za zaštitu osobnih podataka, nakon čega je potrebno izraditi popis osobnih podataka koji se prikupljaju i obrađuju te popis tokova osobnih podataka koji se razmjenjuju. Nadalje, potrebno je utvrditi pravni temelj (zakone, privole) za obradu i razmjenu tih podataka, implementirati mjere za zaštitu podataka, uvesti postupak za slučajeve „curenja" osobnih podataka (incidente) te svakako educirati djelatnike i uspostaviti kulturu zaštite podataka (Čizmić & Boban, 2018: 79-110).

3.2 Zakonski okvir o upravljanju podacima i informacijama u zdravstvu – zaštita i odgovornost

Zakon o podacima i informacijama u zdravstvu u prvom redu osigurava se provedba Uredbe (EZ) br. 1338/2008 Europskog parlamenta i Vijeća od 16. prosinca 2008. o statističkim podacima Zajednice o javnom zdravlju i zdravlju i sigurnosti na radnom mjestu (SL L 354, 31. 12. 2008., u daljnjem tekstu: Uredba (EZ) br. 1338/2008). U pogledu zašite podataka i informacija u zdravstvu u Republici Hrvatskoj ovaj zakon definira i temeljne pojmove koji imaju sljedeće značenje kako slijedi:

> 1. zdravstveni podatak je podatak o pojedincu, o njegovu fizičkom ili mentalnom zdravlju, uključujući pružene mu zdravstvene usluge u zdravstvenom sustavu Republike Hrvatske;

[6] Sukladno tekstu Preambule Uredbe. Vidi GDPR, Preambula, t. 10.

2. zdravstvena informacija nastaje obradom zdravstvenih podataka sa svrhom njezine daljnje uporabe u zdravstvenom sustavu ili za potrebe sustava povezanih sa zdravstvenim sustavom;
3. izvorni zdravstveni podatak je vjerodostojan zapis o određenoj zdravstveno relevantnoj činjenici, mjerenju odnosno zaključku, koji se bilježi na mjestu nastanka podatka ili na način za koji ovlaštena osoba može jamčiti njegovu izvornost, cjelovitost i vjerodostojnost u trenutku bilježenja;
4. izvori zdravstvenih podataka za potrebe evidencija u području zdravstva su pojedinci o kojima se prikupljaju zdravstveni podaci, pravne i fizičke osobe zdravstvenog sustava koje sudjeluju u stvaranju zdravstvenih podataka za upravljačke, poslovne, stručne, znanstvene, istraživačke, statističke, administrativne, nadzorne, sigurnosne, informativne i druge potrebe;
5. obrada zdravstvenih podataka je svaki postupak ili skup postupaka koji se obavljaju na podacima ili na skupovima podataka iz izvora zdravstvenih podataka i drugih izvora, bilo automatiziranim bilo neautomatiziranim sredstvima, kao što su prikupljanje, bilježenje, organizacija, strukturiranje, pohrana, prilagodba ili izmjena, pronalaženje, obavljanje uvida, uporaba, razmjena, otkrivanje prijenosom, širenjem ili stavljanjem na raspolaganje na drugi način, usklađivanje ili kombiniranje, ograničavanje, brisanje ili uništavanje;
6. voditelj obrade je fizička ili pravna osoba, tijelo javne vlasti ili drugo tijelo koje samo ili zajedno s drugima određuje svrhe i sredstva obrade osobnih podataka; kada su svrhe i sredstva takve obrade utvrđeni pravom Europske unije ili pravom države članice, voditelj obrade ili posebni kriteriji za njegovo imenovanje mogu se predvidjeti pravom države članice;
7. izvršitelj obrade je fizička ili pravna osoba, tijelo javne vlasti ili drugo tijelo koje obrađuje osobne podatke u ime voditelja obrade;
8. medicinska dokumentacija je skup medicinskih zapisa i dokumenata nastalih u procesu pružanja zdravstvene zaštite kod ovlaštenih pružatelja zdravstvene zaštite koji sadrže podatke o zdravstvenom stanju i tijeku liječenja pacijenata;
9. zdravstvena dokumentacija je izvorna ili reproducirana dokumentacija, neovisno o obliku zapisa i stvaratelju zapisa podataka,

obuhvaća medicinsku dokumentaciju (liječničku, sestrinsku i drugu dokumentaciju) i svu ostalu dokumentaciju koja nastaje ili je preuzeta u zdravstvenoj djelatnosti (administrativnu, financijsku i drugu nemedicinsku dokumentaciju);
10. evidencija u području zdravstva je strukturirani i standardizirani skup podataka ciljno prikupljan sustavnim bilježenjem i održavan kroz radne procese pružatelja zdravstvene zaštite i drugih pravnih i fizičkih osoba u zdravstvu zaduženih za određenu evidenciju;
11. javnozdravstveni registar je organizirani sustav prikupljanja, analize i distribucije podataka i informacija o populacijskim skupinama određenim prema njihovu zdravstvenom stanju, bolesti i korištenju zdravstvene zaštite i o pružateljima zdravstvenih usluga, koji je uspostavljen za unaprijed određene kliničke, javnozdravstvene, upravljačke i/ili znanstvene potrebe i vodi se u Nacionalnom javnozdravstvenom informacijskom sustavu;
12. zdravstveni registar je evidencija u području zdravstva koja nastaje prikupljanjem, analizom i distribucijom podataka i informacija o populacijskim skupinama s određenim zdravstvenim stanjem, izloženošću ili pruženom zdravstvenom uslugom, podataka i informacija o pružateljima zdravstvenih usluga, koji je uspostavljen za unaprijed definirane kliničke, javnozdravstvene, upravljačke i/ili znanstvene potrebe i vodi se u zdravstvenim ustanovama;
13. Centralni zdravstveni informacijski sustav Republike Hrvatske (u daljnjem tekstu: CEZIH) je središnji sustav pohrane zdravstvenih podataka i informacija za njihovu standardiziranu obradu na primarnoj, sekundarnoj i tercijarnoj razini zdravstvene zaštite i dio je zdravstvene informacijske infrastrukture Republike Hrvatske;
14. Nacionalni javnozdravstveni informacijski sustav (u daljnjem tekstu: NAJS) je sustav pohrane zdravstvenih podataka i informacija za njihovu obradu i arhiviranje (zdravstvene evidencije i registri) radi ostvarenja javnozdravstvenih potreba i dio je zdravstvene informacijske infrastrukture Republike Hrvatske;
15. zdravstvena informacijska infrastruktura Republike Hrvatske je sustav usklađenih procesa i usluga upravljanja zdravstvenim podacima, informacijama, registrima i drugim evidencijama u zdravstvu Republike Hrvatske, dio je državne informacijske infrastrukture i čine ju CEZIH,

NAJS i drugi zdravstveni nacionalni i institucionalni informacijski sustavi (ZPIZ, čl. 3.).

Novim Zakonom o podacima i informacijama u zdravstvu (NN 14/19, koji je na snazi od 15.02.2019.), utvrđuju se prava, obveze i odgovornosti pravnih i fizičkih osoba zdravstvenog sustava u području upravljanja podacima i informacijama u zdravstvu, korištenje i obrada zdravstvenih podataka i informacija u zdravstvenoj zaštiti (Munns & Basu, 2017: 102).

3.2.1 Temeljna načela prikupljanja, korištenja i obrade zdravstvenih podataka i informacija

Prikupljanje, korištenje i obrada zdravstvenih podataka i informacija mora se provoditi po načelima zakonitosti prikupljanja i obrade zdravstvenih podataka i informacija, izvornosti i neposrednosti, vjerodostojnosti, istinitosti i pouzdanosti zdravstvenih podataka i informacija, standardizacije obrade i interoperabilnosti zdravstvenih podataka, sljedivosti i ažurnosti zdravstvenih podataka, dostupnosti i zaštite zdravstvenih podataka i informacija te učinkovitosti, smanjenja količine i ograničenja pohrane zdravstvenih i drugih osobnih podataka (ZPIZ, čl. 4.).

Kao osnova za prikupljanje i obradu svakog zdravstvenog podatka i informacije mora postojati zakonita svrha te cilj prikupljanja povezan s neposrednim ili posrednim pozitivnim učinkom na zdravlje stanovništva. Daljnja obrada zdravstvenih podataka dozvoljena je u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe radi proučavanja i praćenja stanja zdravlja stanovništva ili u druge svrhe utvrđene posebnim zakonom. (ZPIZ, čl. 5.) U zdravstvenom sustavu Republike Hrvatske obvezno je korištenje izvornih zdravstvenih podataka, osim ako je ovim Zakonom drugačije uređeno a izvorni podaci prikupljaju se što bliže izvoru i vremenu njihova nastanka. (ZPIZ, čl. 6.)

Temeljna načela prikupljanja, korištenja i obrade zdravstvenih podataka i informacija su kako slijedi:

Načelo vjerodostojnosti, istinitosti i pouzdanosti zdravstvenog podatka ostvaruje se na način da je zdravstveni podatak preuzet iz službenih zapisa ovlaštene pravne ili fizičke osobe u za to predviđenom obliku i rezultat je formalno definiranog i propisanog postupka. Zdravstvena informacija je vjerodostojna, istinita i pouzdana samo ako proizlazi iz vjerodostojnih zdravstvenih podataka i za nju se nedvojbeno može utvrditi temelj, nadležnost, svrha, izvor, namjena, korištena metodologija i autor (ZPIZ, čl. 7.).

Standardizacija obrade zdravstvenih podataka ostvaruje se na način da je standardiziran svaki postupak vezan uz nastanak, prikupljanje, bilježenje, preuzimanje, korištenje, prosljeđivanje, pohranu i arhiviranje zdravstvenih podataka u njihovu ukupnom ciklusu na razini zdravstvenog sustava. Pravne i fizičke osobe i/ili sustavi u zdravstvu moraju ostvarivati zajedničke standarde kao jedinstven sustav neovisno o razini integracije. Međusobno djelovanje osoba i sustava u odnosu na prikupljanje i obradu zdravstvenih podataka i informacija mora biti pravno, organizacijski, procesno, semantički i tehnički usklađeno i standardizirano, uz primjenu jedinstvenih metodoloških principa i statističkih te drugih standarda. Interoperabilnost zdravstvenih podataka ostvaruje se njihovom razmjenom elektroničkim putem, korištenjem unaprijed dogovorenih strukturiranih poruka kao standardnog načina razmjene zdravstvenih podataka, osim u iznimnim slučajevima kada elektronička razmjena podataka iz opravdanih razloga nije moguća (ZPIZ, čl. 8.).

Sljedivost nastanka, promjene i uporabe zdravstvenih podatka i informacija (vrijeme, mjesto, izvršitelj, temelj, razlog, način, korišteni standardi te okolnosti utvrđivanja sadržaja) ostvaruje se uspostavom standardnih postupaka prikupljanja i obrade zdravstvenih podataka i informacija. Ažurnost zdravstvenih podataka i informacija ostvaruje se na način da svi voditelji obrade i korisnici zdravstvenih podataka precizno utvrde vrijeme nastanka zdravstvenog podatka i njegovu točnost u odnosu na trenutak obrade (ZPIZ, čl. 9.).

Načelo dostupnosti i zaštite zdravstvenih podataka i informacija ostvaruje se na način da su zdravstveni podaci i informacije dostupni svim ovlaštenim pravnim i fizičkim osobama, korisnicima zdravstvenog sustava, kojima je to pravo priznato ovim Zakonom te zakonima koji reguliraju prava i obveze u zdravstvenom sustavu te prava pacijenata. Voditelji obrade i izvršitelji obrade zdravstvenih podataka

moraju osigurati zaštitu osobnih podataka u svim postupcima koji uključuju uvid i obradu osobnih podataka, u skladu s propisima koji uređuju zaštitu osobnih podataka (ZPIZ, čl. 10.).

Načelo učinkovitosti i smanjenja količine zdravstvenih i drugih osobnih podataka postiže se prikupljanjem i obradom samo onih zdravstvenih i drugih osobnih podataka koji su potrebni, relevantni i ograničeni na ono što je nužno u odnosu na svrhe u koje se obrađuju. (2) Administrativne poslove vezane uz postupke prikupljanja, pristupa i obrade podataka iz stavka 1. ovoga članka potrebno je svesti na najmanju mjeru, radi nesmetanog obavljanja poslova pružanja neposredne zdravstvene zaštite (ZPIZ, čl. 11.).

Načelo ograničenja pohrane zdravstvenih i drugih osobnih podataka ostvaruje se na način da zdravstveni i drugi osobni podaci moraju biti čuvani u obliku koji omogućava identifikaciju ispitanika samo onoliko dugo koliko je potrebno u svrhe radi kojih se ti podaci obrađuju. Podaci se mogu pohraniti na dulja razdoblja ako će se obrađivati isključivo u svrhe arhiviranja u javnom interesu, u svrhe znanstvenog ili povijesnog istraživanja ili u statističke svrhe, što podliježe provedbi propisanih tehničkih i organizacijskih mjera radi zaštite prava i sloboda ispitanika (ZPIZ, čl. 12.).

3.2.2 Nadležna tijela i odgovornost za zaštitu podataka i informacija u zdravstvu

Zdravstveni informacijski sustavi (*dalje ZIH)* Republike Hrvatske od posebnog nacionalnog interesa su oni dijelovi zdravstvene informacijske infrastrukture Republike Hrvatske nužni za nesmetano pružanje zdravstvene zaštite te zapisi i dokumenti nastali djelovanjem pružatelja zdravstvene zaštite Republike Hrvatske:

> – za koje je utvrđen stupanj tajnosti ili;
> – koji sadrže podatke vezane uz zdravstvene i druge osobne podatke građana u zdravstvenim registrima i informacijskim sustavima kojima se osigurava nesmetano obavljanje zdravstvene djelatnosti te druge povjerljive podatke čijom objavom bi se počinila šteta ugledu Republike Hrvatske ili njezinih građana, za koje nije utvrđen stupanj tajnosti (ZPIZ, čl. 13.).

Zdravstveni i drugi osobni podaci moraju biti obrađivani na način kojim se osigurava odgovarajuća sigurnost i povjerljivost podataka, uključujući zaštitu od neovlaštene ili nezakonite obrade te od slučajnog gubitka, uništenja ili oštećenja primjenom odgovarajućih organizacijskih, tehničkih i sigurnosnih mjera (Murphy, 2015). Obrada zdravstvenih podataka provodi se elektroničkim putem u zdravstvenoj informacijskoj infrastrukturi Republike Hrvatske, koja je obvezna koristiti zajedničku tehnološku osnovicu i komponente razvijene za potrebe državne informacijske infrastrukture. Način obrade podataka u CEZIH-u, NAJS-u i drugim zdravstvenim nacionalnim i institucionalnim informacijskim sustavima, način čuvanja i zaštite zdravstvenih podataka i izrade zdravstvenih pokazatelja, standardizirane obrasce za prikupljanje i obradu zdravstvenih podataka, sadržaj, popis i opis zdravstvenih registara i evidencija u području zdravstva koje služe za zdravstvena statistička istraživanja iz područja zdravstvene zaštite, javnog zdravstva, zdravstvenih djelatnosti, pružatelja i korisnika zdravstvenih usluga, zdravstvene infrastrukture, pruženih usluga, utvrđenih bolesti, stanja i ozljeda, krvi, krvnih pripravaka, lijekova i medicinskih proizvoda, zdravstvenog osiguranja i financiranja zdravstvene zaštite pravilnikom propisuje ministar nadležan za zdravstvo (ZPIZ, čl. 19.).

Člancima 20. – 23. ZPIZ uređuje se vođenje zdravstvene dokumentacije i evidencija u području zdravstva, medicinske dokumentacije i središnjeg elektroničkog zdravstvenog zapisa (e-Kartona) te odgovornost za potpunost i vjerodostojnost zdravstvenih podataka i to:

- Zdravstvena dokumentacija vodi se u zdravstvenoj djelatnosti u elektroničkom obliku. Vode je pružatelji zdravstvene zaštite i druge pravne i fizičke osobe u zdravstvenoj djelatnosti (ZPIZ, čl. 20.).
- Medicinska dokumentacija je dio zdravstvene dokumentacije koji se vodi na svim razinama zdravstvene zaštite u elektroničkom Ova medicinska dokumentacija pacijenata nastala u procesima pružanja zdravstvene zaštite pohranjuje se u zdravstvenoj informacijskoj infrastrukturi Republike Hrvatske i razmjenjuje se servisima zdravstvene informacijske infrastrukture. Opseg i sadržaj te način vođenja medicinske dokumentacije pravilnikom propisuje ministar nadležan za zdravstvo (ZPIZ, čl. 21.).

- e-Karton - središnji elektronički zdravstveni zapis je dio medicinske dokumentacije pacijenta koji objedinjava zdravstvene i druge osobne podatke o pacijentu, prikupljene i pohranjene u CEZIH-u. e-Kartonu imaju pristup samo ovlašteni zdravstveni radnici koji sudjeluju u liječenju, zdravstvenoj njezi i skrbi za pacijenta te one ovlaštene osobe kojima je pacijent dao izričitu privolu. Uvid u podatke u e-Kartonu ima i sam pacijent putem sustava e-Građani. Opseg i sadržaj podataka te način vođenja e-Kartona pravilnikom propisuje ministar nadležan za zdravstvo (ZPIZ, čl. 22.).

3.2.3 Odgovornost za potpunost i izvornost zdravstvenih podataka

Radi osiguravanja jedinstvenog sustava statističkih istraživanja, pri vođenju evidencija u području zdravstva primjenjuju se jedinstveni metodološki principi i statistički standardi (Institute of Medicine, 2001). Potpunost podataka u medicinskoj dokumentaciji i evidencijama u području zdravstva nadzire i kontrolira organizacijski nadređena osoba odgovorna za dokumentaciju i/ili evidencije pružatelja zdravstvene zaštite i drugih pravnih i fizičkih osoba u zdravstvu. Za potpunost i vjerodostojnost izvornog zdravstvenog podatka upisanog u medicinskoj dokumentaciji odgovoran je nadležni zdravstveni radnik i drugi radnik koji je taj podatak upisao te ispitanik (pacijent ili druga osoba koja je dala osobne podatke) (ZPIZ, čl. 23.).

Zakon o podacima informacijama u zdravstvu prema tom tumačenju obvezno primjenjuju i odgovorni su za njihovu primjenu:

- Ministarstvo zdravstva,
- Hrvatski zavod za javno zdravstvo,
- Hrvatski zavod za zdravstveno osiguranje, zdravstveni zavodi i agencije
- pružatelji zdravstvene zaštite na primarnoj, sekundarnoj i tercijarnoj razini zdravstvene djelatnosti.
- komore u zdravstvu i
- trgovačka društva za zdravstveno osiguranje.

Obveza je bolnica, poliklinika, domova zdravlja, drugih zdravstvenih ustanova, pružatelja zdravstvenih osiguranja, pridržavati se svih zahtjeva i obveza utvrđenih Općom uredbom o zaštiti podataka (GDPR) te nacionalnim propisima zaštite podataka te zakonu o informacijskoj sigurnosti (Mantas, Hasman & Gallos, 2019). Osobni podaci o zdravlju pojedinaca pod povećalom su struke, javnosti i nadzornih tijela, a kazne za otkrivanje i curenje takovih informacija predviđeni su novčani iznosi pri kršenju GDPR-a ali i Zakona o podacima i informacijama u zdravstvu. Povrede zdravstvenih informacija mogu imati ozbiljne posljedice i za pružatelje zdravstvene usluge i za njihove pacijente, a informacije o pacijentu uključuju različite osobne podatke koje se mogu koristiti za krađu identiteta (Boban, 2016: 152-159). Svaki pružatelj usluga u elektroničkom poslovanju, pa tako i pružatelji zdravstvenih usluga, koji koriste računalnu mrežu, obrađuju i pohranjuju razne informacije, svakodnevno su izloženi opasnosti otkrivanja podataka i informacija te samim time moraju, sukladno Općoj uredbi o zaštiti podataka (Boban, 2018: 26-40), implementirati tehničke i organizacijske mjere zaštite informacijskih sustava kako bi povećali razinu zašite podataka (Leenes, et al., 2017: 117).

4 Zaključak

Sukladno definiciji Zakona o podacima i informacijama u zdravstvu. e-zdravstvo čine sustavni stručni i poslovni zdravstveni postupci, procesi i usluge podržane informacijskim i komunikacijskim tehnologijama, a obuhvaća informacijske sustave u zdravstvenim ustanovama, uključujući razmjenu elektroničkim zdravstvenim zapisom, distribuciju zdravstvenih informacija, medicinska istraživanja i internetske servise za korisnike sustava zdravstva. U zdravstvenim ustanovama koje pružaju zdravstvenu zaštitu 24 sata dnevno mora biti osigurana i dostupnost informacijskih i komunikacijskih sustava 24 sata dnevno. Isto vrijedi i za sustav odgovornosti i zašite zdravstvenih informacijskih sustava. Na tom tragu donošenje cjelokupnog zakonskog okvira zaštite podataka a poglavito zaštite podataka i informacija u zdravstvu u Republici Hrvatskoj predstavljalo je nužnost u današnjem digitalnom društvu. Također, kao ključan korak predstavlja i upravljanje sigurnošću zdravstvenim informacijskim sustavima primjenom međunarodnih standarda, osobito standarda ISO 27799:2016 koji je i prikazan u radu. Svakako, na kraju valja istaknuti i poslovanje sukladno temeljnim načelima prikupljanja, korištenja i obrade zdravstvenih podataka i informacija čime se osigurava visoka razina zaštite uz jasno

utvrđivanje odgovornosti nadležnih osoba i tijela u upravljanju podacima i informacijama u zdravstvu.

Zakonodaja, sudska praksa

Information Security World, https://avkashk.wordpress.com/information-security-management-systemiso-27001/ (16.01.2020).

Institute of Medicine, Division of Health Care Services, Committee on the Role of Institutional Review Boards in Health Services Research Data Privacy Protection, Protecting Data Privacy in Health Services Research, National Academies Press, 2001.

ISO.org https://www.iso.org/standard/62777.html.

UREDBA (EU) 2016/679 EUROPSKOG PARLAMENTA I VIJEĆA od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ. Dostupno na https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&qid=1462363761441&from=HR (20.01.2020).

Ustav Republike Hrvatske Narodne novine br. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

Zakon o podacima i informacijama u zdravstvu, Narodne novine br. 14/19.

Zakon o zaštiti osobnih podataka, pročišćeni tekst, Narodne novine br. 103/03, 118/06, 41/08, 130/11, 106/12 – prestao važiti 25.05.2018.

Literatura

Adams, S., Purtova, N. & Leenes, R. (eds.) (2016). *Under Observation: The Interplay Between eHealth and Surveillance* (Springer).

Adelsberger, Z. (2009). *Osvrt na tekst „Zašto ISO 27001 (možda) nije dovoljan?*, dostupno na http://zdenkoadelsberger.blogspot.com/2009/05/osvrt-na-tekst-zasto-iso-27001-mozda.html (20.02.2020).

Boban, M. (2016), ePrivacy and new European Data Protection Regime, U: *International Scientific Conference ESD 2016*, *Managerial Issues in Modern Business*, Warsaw, Poland, str. 152-159.

Boban, M. (2019). E-zdravlje: zaštita osobnih podataka u novim uvjetima, U: *Zbornik radova, 1. Kongres KOKOZ-a i 3. Hrvatski kongres medicinskog prava s međunarodnim sudjelovanjem, Rabac, Hrvatska*, str. 41-72.

Boban, M. (2018). Zaštita osobnih podataka i nova EU uredba o zaštiti podataka, *Bilten Hrvatskog društva za medicinsku informatiku*, 24(1), str. 26-40.

Božić, V. (2013) Upravljanje informacijskom sigurnošću u zdravstvu, *Medix: specijalizirani medicinski dvomjesečnik,* 19(107/108).

Čizmić, J. & Boban, M. (2018). Primjena GDPR-a u hrvatskom pravu s posebnim osvrtom na pravna sredstva za zaštitu osobnih podataka, U: *Zbornik radova „Aktualnosti građanskog procesnog prava – nacionalna i usporedna pravno teorijska i praktična dostignuća*, Sveučilište u Splitu, Pravni fakultet, str. 79-110.

Čizmić, J., Boban, M. & Zlatović, D. (2016). *Nove tehnologije, intelektualno vlasništvo i informacijska sigurnost* (Split: Sveučilište u Splitu Pravni fakultet).

Gallotti, C. (2019). *Information security: risk assessment, management systems, the ISO/IEC 27001 standard* (Lulu.com).

Humphreys, E. (2016). *Implementing the ISO/IEC 27001:2013 ISMS Standard* (Artech House).

Kenyon, B. (2019). *ISO 27001 controls – A guide to implementing and auditing* (IT Governance Ltd).

Kičić, M. (2014). E-zdravlje – savjetodavna uloga medicinskih sestara, *Acta medica Croatica*, 68(1), str. 65-68.

Končar, M. (2011). Europska iskustva projekata e-zdravstva, *Medix: specijalizirani medicinski dvomjesečnik*, 17(94/95).

Leenes, R., van Brakel, R., Gutwirth, S. & De Hert, P. (eds.) (2017). *Data Protection and Privacy*: *(In)visibilities and Infrastructures*, (Springer), str. 117.

Mantas, J., Hasman, A. & Gallos, P. (eds.) (2019). *Health Informatics Vision: From Data via Information to Knowledg*e (IOS Press).

Munns, C. & Basu, S. (2017). *Privacy and Healthcare Data: 'Choice of Control' to 'Choice' and 'Control'* (Taylor & Francis).

Murphy, S.P. (2015). *Healthcare Information Security and Privacy* (McGraw Hill Professional).

SEISMED Consortium (1996). *Data Security for Health Care* (IOS Press).

Tamò-Larrieux, A. (2018) *Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Thing*s (Springer).

Tan, J. (2005). *E-Health Care Information Systems: An Introduction for Students and Professionals* (John Wiley & Sons).

Weiss, M. & Solomon, M. G. (2015). *Auditing IT Infrastructures for Compliance* (Jones & Bartlett Publishers).