Bilt. Hrvat. druš. med. inform. 2025:31(1-2)
STRUČNI ČLANAK

Digitalna transformacija i izazovi informacijske sigurnosti u bolničkom poslovanju

Dražen Milković[1]
[1]Klinički bolnički centar Zagreb, Zagreb, Hrvatska
E-pošta: drazen.milkovic@kbc-zagreb.hr

https://doi.org/10.69827/bhdmi-39976

Sažetak: Povećanje potreba za različitim specijalističkim medicinskim uslugama, kao i rastuće složenosti medicinskog poslovanja, zahtijeva rješenja koja mogu uštedjeti vrijeme kao npr. definiranje, automatizacija i integracija poslovnih procesa te primjena novih inovativnih rješenja. Intenzivna primjena brojnih informacijskih tehnologija, sve veća umreženost i mobilnost, izlažu bolničko poslovanje rizicima koji proizlaze iz digitalnog okruženja, istovremeno postavljajući nove zahtjeve u pogledu sigurnosti i kontinuiteta poslovanja. Povećava se i digitalni otisak svakog pojedinca, čineći ga ranjivijim na informacijske sigurnosne prijetnje, kojih često nismo dovoljno svjesni. Agilno unaprjeđenje poslovnih procesa u medicinskoj djelatnosti, uz podršku naprednih informacijsko-tehnoloških rješenja, postaje nužnost u današnjem vremenu digitalne transformacije poslovanja. Za potrebe pružanja zdravstvene skrbi bolesnicima stvaraju se, prikupljaju i obrađuju velike količine medicinskih podataka koje je potrebno na odgovarajući način zaštiti od neovlaštene upotrebe. Cilj ovog rada je prikazati kako tehnološki napredak utječe na promjene u bolničkom poslovanju te indirektno na pružanje zdravstvene skrbi bolesnicima. Intenzivno korištenje digitalnih tehnologija je neizbježno povezano i s rizicima koji dolaze iz digitalnog okruženja u kojemu je sve međusobno povezano. U digitalnom okruženju promjene su sve brže i vidljivije, od naprednih digitalnih alata koji su nam dostupni, preko mogućnosti koje pružaju, do izazova digitalne sigurnosti koje sa sobom donose. Zbog svega navedenog, uprave u zdravstvenim ustanovama imaju nove izazove na koje je potrebno odgovoriti kroz odgovorno upravljanje, kako bi organizacije na siguran način postigle svoje ciljeve u kontekstu digitalne transformacije i informacijske sigurnosti.

Ključne riječi: digitalna transformacija; informacijska sigurnost; kibernetička sigurnost; korporativno upravljanje; poslovni procesi; umjetna inteligencija.

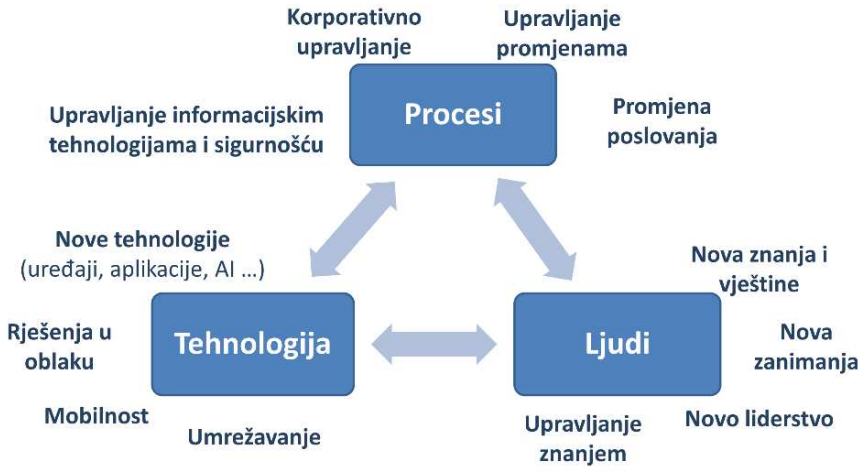
Digitalna transformacija, upravljanje promjenama i upravljanje u organizaciji

Digitalizaciju možemo definirati kao proces pretvaranja analognih odnosno fizičkih oblika poput dokumenata, slike, zvuka, video zapisa ili sl. u digitalni oblik, koji se pohranjuje u elektronički sustav radi daljnje obrade, dijeljenja i čuvanja. Digitalizacija se može promatrati kao put kretanja prema digitalnom poslovanju i digitalnoj transformaciji. Trendovi pokazuju da sve ono što se može automatizirati, digitalizirati ili virtualizirati, to će se i dogoditi (1).[24]

Digitalna transformacija je neprekidni proces u kojemu se mijenja poslovanje organizacija, postiže veća kvaliteta, sigurnost, povezanost i komunikacija uz intenzivnu primjenu digitalnih tehnologija (2).[25]

Digitalna transformacija nije pitanje izbora, već je neizbježna i neophodna. Neizostavni je pojam u razgovorima s donositeljima ključnih odluka u korporacijama i organizacijama. Prema nekim autorima promjene na poslovnoj sceni jasno ukazuju da poslovnim subjektima koji ne provedu digitalnu transformaciju poslovanja prijeti ubrzano izumiranje (engl. *„Digital or die"*) (2).[26]

Digitalna transformacija je sveobuhvatan proces koji istovremeno utječe na promjene vezano uz poslovne procese, ljude i tehnologije, kako je prikazano na slici 1. U najširem smislu, procesi obuhvaćaju, između ostalog, operativno poslovanje organizacije, korporativno upravljanje odnosno upravljanje na najvišoj razini, upravljanje promjenama unutar organizacije, te upravljanje informacijskim tehnologijama i sigurnošću.



Slika 1. Prikaz sveobuhvatnosti utjecaja digitalne transformacije (izvor: izrada autora)

Rad u digitalnom okruženju zahtijeva nove vještine i znanja zaposlenika. Stvaraju se nova zanimanja, te istovremeno smanjuje potreba za nekim tradicionalnim vještinama i zanimanjima. Digitalizacijom i primjenom umjetne inteligencije (UI) relativno se lako nadomještaju uglavnom ponavljajući poslovi, brzo se prikupljaju podaci, mogu se prepoznavati problemi te nuditi ili pak predviđati rješenja. Obrazovanje i razvoj novih digitalnih kompetitivnih vještina bi trebalo biti usmjereno na razvijanje sposobnosti obavljanja nerutinskih poslova, kritičko razmišljanje,

[24] Gerd Leonhard: „How The Future works?" [pristupljeno: 02.12.2025.]. Dostupno na: https://www.futuristgerd.com/howthefutureworks/ ?gclid=EAIaIQobChMIj-TRteWG6AIVWfBRCh241QxFEAAYASAAEgL6pfD_BwE
[25] Spremić M. Digitalna transformacija poslovanja. Sveučilište u Zagrebu, Ekonomski fakultet Zagreb, 2017., str. 38.
[26] Spremić M. Digitalna transformacija poslovanja. Sveučilište u Zagrebu, Ekonomski fakultet Zagreb, 2017., str. 18.

sposobnosti interpretacije i primjene informacija, etičnost, sposobnost stalnog učenja i sl. Vođenje u digitalnom dobu također traži i nove vještine.

U tehnološkom smislu promjene su možda i najvidljivije. Od umrežavanja, mobilnih tehnologija, društvenih mreža, računalstva u oblaku (engl. *Cloud Computing*), obrade velikih količina podataka (engl. *Big Data*), korištenja senzora i interneta stvari (engl. *IoT - Internet of Things*), lanca blokova (engl. *Blockchain*), 3D ispisa, nosivih tehnologija (engl. *Wearables*), dronova, virtualne stvarnosti, pa sve do robotizacije i UI-a. Danas tehnologija oblikuje gotovo svaki aspekt našeg života, od posla i zdravlja do načina na koji provodimo slobodno vrijeme.

Još 1977. godine bilo je moguće nacrtati logičku shemu interneta, tadašnjeg ARPANET-a kao prve računalne mreže Agencije za napredne istraživačke projekte – ARPA (engl. *Advanced Research Projects Agency*), pod ingerencijom američkog Ministarstva obrane, što danas zbog kompleksnosti jednostavno više nije slučaj (3).[27] Podsjetimo se također na to da je internet uveden u Republici Hrvatskoj 1992. godine puštanjem u rad Hrvatske akademske i istraživačke računalno komunikacijske mreže - CARNet (engl. *Croatian Academic and Research Network*). U današnje vrijeme visoke mrežne povezanosti aplikacije i podaci više nisu nužno ograničeni samo na lokalno korištenje u bolnicama. Prisutni su trendovi prema kojima se podaci pohranjuju i koriste u računalnom oblaku, s ciljem da budu dostupni u bilo koje vrijeme i s bilo kojeg mjesta. Primjerice, sve je češća uporaba nosivih uređaja koji prikupljaju podatke o zdravstvenom stanju pacijenata izvan zdravstvenih ustanova, uz korištenje mobilnih aplikacija i pohranu podataka u računalnom oblaku. Tim podacima mogu pristupati i liječnici radi kontinuiranog praćenja pacijenata i pravovremenog reagiranja. Mobilnost, odnosno rad izvan organizacije, također predstavlja snažan izazov sigurnom pristupu mrežnim resursima kao i zaštiti podataka koji napuštaju mrežnu granicu organizacije. Gotovo sva medicinska oprema i uređaji su danas digitalizirani i u svom redovitom radu se spajaju na računalnu mrežu bolnice.

Upravljanje organizacijom na najvišoj razini ili korporativno upravljanje u digitalnom okruženju postavlja pred menadžment nove izazove, posebno pred najviši menadžment organizacije. Premda se pojam korporativnog upravljanja uobičajeno povezuje s velikim trgovačkim društvima tj. poduzećima, univerzalno je primjenjiv. Bolnice kao javne ustanove nisu profitne organizacije, ali imaju sličnu upravljačku i organizacijsku strukturu trgovačkim društvima i raspolažu značajnim sredstvima u svom poslovanju, pa se analogija ogleda u implementaciji najbolje prakse u upravljanju iz korporativnog sektora. Na globalnoj razini OECD (engl. *Organisation for Economic Co-Operation And Development*) daje najveći doprinos razvoju dobre prakse korporativnog upravljanja. U Smjernicama OECD-a za multinacionalna poduzeća o odgovornom poslovnom ponašanju (2023.) se navodi kako se preporuke za multinacionalna poduzeća u državnom vlasništvu odnose se i na poduzeća u privatnom vlasništvu, ali je javni nadzor često povećan kada je država krajnji vlasnik. Također se navodi da su smjernice OECD-a za korporativno upravljanje u poduzećima u državnom vlasništvu koristan vodič namijenjen upravo takvim poduzećima, a sadržavaju preporuke koje mogu znatno poboljšati upravljanje (4).[28] Smjernice su tako primjenjive neovisno o vlasničkoj strukturi poduzeća.

[27] Wikipedia - Advanced Research Projects Agency Network (ARPANET). Dostupno na: https://en.wikipedia.org/wiki/ARPANET. Pristupljeno: 10.12.2025.
[28] Nacionalna kontaktna točka – NKT (2023.), *Smjernice OECD-a za multinacionalna poduzeća o odgovornom poslovnom ponašanju*, str. 21 [pristupljeno: 12.12.2025.]. Dostupno na: https://investcroatia.gov.hr/wp-content/uploads/2023/11/NKT_Smjernice_odgovorno-poslovno-pona%C5%A1anje.pdf.

Nisu namijenjene isključivo velikim poduzećima, već se primjenjuju i na mala i srednja poduzeća, uz uvažavanje razine kapaciteta za njihovu provedbu (4).[29]

Također, u skladu sa Zakonom o sustavu unutarnjih kontrola u javnom sektoru (2015.), korporativno upravljanje predstavlja sustav upravljanja, kontrola i nadzora uspostavljen u institucijama, osobito u trgovačkim društvima. Obuhvaća strukturu i postupke koji se provode radi rukovođenja, usmjeravanja i praćenja aktivnosti te informiranja s ciljem ostvarenja poslovnih ciljeva (5).[30] U tom smislu bolničke institucije, kao proračunski korisnici javnog sektora, provode korporativno upravljanje kroz funkciju ravnatelja i ravnateljstvo, zatim stručno vijeće, upravno vijeće, sustav unutarnjih kontrola, nadzorne mehanizme, transparentno izvještavanje te primjenu etičkih standarda. Na taj se način osigurava da bolnice posluju u interesu pacijenata i javnog zdravlja, zaposlenika i šire zajednice, uz istodobno poštivanje fiskalne odgovornosti i zakonskih obveza.

Sukladno Zakonu o kibernetičkoj sigurnosti – ZKS (2024.), Nacionalni centar za kibernetičku sigurnost (NCSC-HR - engl. *National Centar Cybersecurity Centar*) kao nadležno tijelo za zdravstvo, koji djeluje u okviru Sigurnosno obavještajne agencije (SOA), proveo je nacionalnu procjenu kibernetičkih sigurnosnih rizika i kategorizaciju subjekta. Odlukom NCSC-a, KBC Zagreb je kategoriziran kao ključan subjekt u sektoru zdravstva, sa utvrđenom visokom razinom kibernetičkih rizika i obvezom provođenja napredne razine mjera kibernetičke sigurnosti. Bolnice su kao pravne osobe, pružatelji zdravstvene zaštite u sektoru Zdravstva, koji je ujedno jedan od sektora visoke kritičnosti (6).[31]

Zakon o kibernetičkoj sigurnosti propisuje kako su za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima odgovorni članovi upravljačkih tijela ključnih i važnih subjekata, odnosno čelnici tijela državne uprave, drugih državnih tijela i izvršnih tijela jedinica lokalne i područne (regionalne) samouprave. Dakle odgovornost pripada najvišem menadžmentu ključnih i važnih subjekata, odnosno organizacija, što se u slučaju bolnica odnosi na ravnateljstvo, odnosno ulogu ravnatelja. Zakon također nalaže osobama odgovornim za upravljanje mjerama kibernetičke sigurnosti sljedeće obveze:

- provoditi mjere upravljanja kibernetičkim sigurnosnim rizicima,
- odobravati mjere upravljanja kibernetičkim sigurnosnim rizicima,
- kontinuirano se osposobljavati te omogućiti zaposlenicima organizacije pohađanje odgovarajućih edukacija u području upravljanja kibernetičkim sigurnosnim rizicima (6).[32]

Sukladno Uredbi o kibernetičkoj sigurnosti – UKS, odgovorna osoba za provedbu mjera može imenovati dediciranu osobu koja je za razinu cijelog subjekta operativno odgovorna za kibernetičku sigurnost (7).[33] Međutim, krovna odgovornost za provedbu mjera kibernetičke sigurnosti definirana Zakonom o kibernetičkoj sigurnosti je neprenosiva, te se ne može delegirati.

[29] Nacionalna kontaktna točka – NKT (2023.), *Smjernice OECD-a za multinacionalna poduzeća o odgovornom poslovnom ponašanju* [pristupljeno: 12.12.2025.]. Dostupno na: https://rbcroatia.gov.hr/smjernice-oecd-a-za-multinacionalna-poduzeca-o-odgovornog-poslovnom-ponasanju/
[30] Narodne novine, (2015.), *Zakon o sustavu unutarnjih kontrola u javnom sektoru*, NN br. 78/2015. Zagreb, članak 4. [pristupljeno: 10.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_07_78_1492.html
[31] Narodne novine, (2024.), *Zakon o kibernetičkoj sigurnosti,* NN br. 14/2024., Zagreb, PRILOG I., str. 35. [pristupljeno: 05.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html
[32] Narodne novine, (2024.), *Zakon o kibernetičkoj sigurnosti,* NN br. 14/2024., op.cit., članak 29.
[33] Narodne novine, (2024.), *Uredba o kibernetičkoj sigurnosti*, NN 135/2024, PRILOG II., Mjere upravljanja kibernetičkim sigurnosnim rizicima, točka 1.6. [pristupljeno: 14.12.2025.]. https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_135_2217.html,

U svom razmatranju tko bi i što trebao učiniti kako bi se pomoglo u ublažavanju kibernetičkih prijetnji u zdravstvu, Belani i Fišter zaključuju kako je kibernetička sigurnost u zdravstvu zajednička odgovornost pri čemu se u očekivanim ulogama ključnih dionika pojavljuju vlada, zakonodavac, menadžeri u zdravstvu, IT stručnjaci i zdravstveni djelatnici. Svijest i prihvaćanje vlastite odgovornosti, dosljedno praćenje najboljih praksi, kao i razumijevanje postupaka drugih dionika usmjerenih prema zajedničkom cilju sigurnog sustava, od ključne su važnosti (8).[34]

Odgovornim korporativnim upravljanjem raspoloživim resursima u ostvarenju strateških ciljeva organizacije, najviši menadžment treba uvažavati cjelokupni potencijal i prednosti digitalne tehnologije u provedbi zacrtane strategije. Istodobno je nužno odgovorno upravljati rizicima povezanim s digitalnim okruženjem kako bi poslovanje bilo sigurno, neprekinuto i usmjereno na ostvarenje ciljeva organizacije.

Odgovornim korporativnim upravljanjem raspoloživim resursima u ostvarenju strateških ciljeva organizacije, najviši menadžment treba uvažavati cjelokupni potencijal i prednosti digitalne tehnologije u provedbi zacrtane strategije. Istodobno je nužno odgovorno upravljati rizicima povezanim s digitalnim okruženjem kako bi poslovanje bilo sigurno, neprekinuto i usmjereno na ostvarenje ciljeva organizacije.

Digitalna transformacija poslovanja i utjecaj na promjene u bolnicama

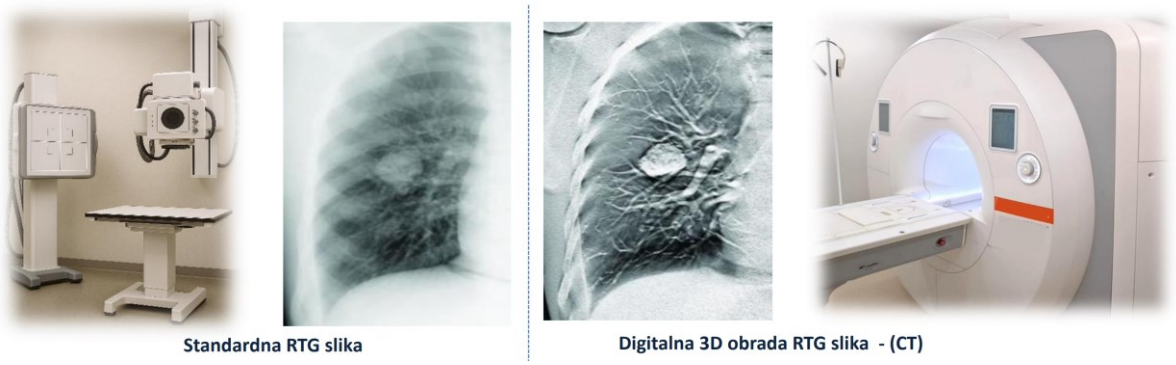
Razvoj i digitalizacija medicinske opreme je omogućio iznimno veliki pomak u gotovo svim medicinskim specijalnostima, primjerice u radiološkoj dijagnostici, nuklearnoj medicini, radio terapiji, laboratorijskoj djelatnosti, bolničkom ljekarništvu, robotiziranoj kirurgiji i sl.

Radiologija je tako iz analognog tj. fizičkog prikaza rendgenskih slika prešla u potpuno digitalno trodimenzionalno računalno okruženje. Kvaliteta prikaza i dijagnostička vrijednost slikovnog materijala je značajno unaprijeđena kako je prikazano na slici 2. Umjesto jedne radiološke slike, uz primjenu kompjuterizirane tomografije (engl. *computed tomography* - CT) proizvodi se trodimenzionalni slikovni model u boji, koji sadrži i po nekoliko tisuća slika za pojedinu dijagnostičku obradu, što značajno povećava potrebe za digitalnim kapacitetima u obradi i sigurnoj pohrani medicinskih podataka. Primjena UI-a u analizi radiološkog slikovnog materijala dodatno ubrzava dijagnostički postupak i pisanje nalaza.

U medicinsko-laboratorijskom poslovanju prikupljeni krvni uzorci se u velikim količinama automatizirano obrađuju u suvremenim laboratorijskim uređajima, a rezultat je nalaz u digitalnom obliku s analizom rezultata i već označenim parametrima koji odstupaju od referentnih vrijednosti. Uređaji su povezani u središnji laboratorijski sustav bolnice – LIS, koji je nadalje povezan s BIS-om i CEZIH-om, što je ključno za automatizirano slanje laboratorijskih nalaza na središnji informacijski zdravstveni sustav i primarnu zdravstvenu zaštitu. U tom smislu, iznimno velika količina ljudskog rada je zamijenjena preciznim strojnim procesima, a u segmentima laboratorijskog poslovanja gdje je to

[34] *Who should do what to help mitigate cyber threats in health care: narrative review of practical approaches and actionable recommendations*, International Journal of Health Governance (2025.), Vol. 30 No. 3, 2025, pp. 282-292, str. 288 [pristupljeno: 17.12.2025.]. Dostupno na: https://doi.org/10.1108/IJHG-03-2025-0030

primjenjivo, također je rad na mikroskopu zamijenjen automatiziranim uređajima za obradu bioloških uzoraka.



Slika 2. Prikaz tehnološkog napretka u radiološkoj dijagnostici (izvor: izrada autora uz korištenje generativne umjetne inteligencije - Microsoft Copilot - u prikazu grafičke komponente RTG uređaja s vertikalnim stativom)

Slično je i s patološkim i citološkim laboratorijskim poslovanjem koje je također visoko automatizirano, te je uz primjenu digitalnih skenera patoloških stakalaca patologu omogućeno provođenje pregleda patoloških stakalaca i pisanja nalaza u cijelosti digitalno, odnosno radom na računalu.

Digitalna transformacija je omogućila postupni prelazak iz analognog u digitalni svijet ili pojednostavljeno rečeno prelazak sa gledanja u mikroskop na gledanje na ekranu računala, kako je prikazano na slici 3. Radi se zapravo o iznimno značajnoj tehnološkoj promjeni koja je dugotrajna i bitno olakšava laboratorijsko poslovanje uslijed povećanog opsega posla.

Slika 3. Prikaz digitalne transformacije laboratorijskog poslovanja (izvor: izrada autora)

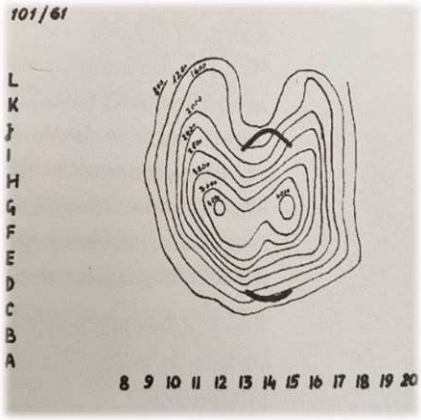
Razvoj nuklearne medicine se temelji na multidisciplinarnim dostignućima više znanstvenih disciplina poput fizike, elektrotehnike, informatike, kemije i biologije. Razvojem brojača za mjerenje radioaktivnosti ili scintilacijskog brojača, 1952. godine se pojavljuje prvi uređaj za scintigrafiju kojega je konstruirao Benedict Cassen kao prvi mehanički uređaj za scintigrafiju kojim se biodistribucija radioaktivnog spoja u organizmu mogla prikazivati vizualno i dvodimenzionalno.

Dijagnostički slikovni materijal tj. scintigram štitnjače je tako u samim počecima rađen ručno na temelju izmjerenih podataka s ručnim scintilacijskim brojačem. Primjer takvog ručnog scintigrama

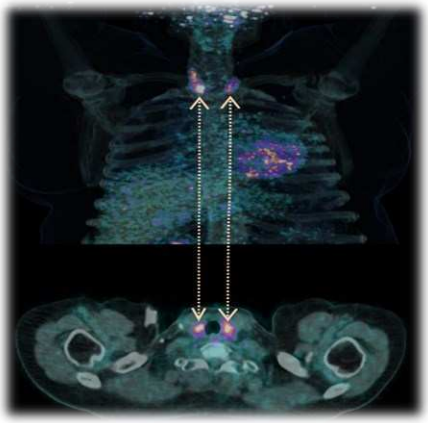
prikazanog na slici 4., nastao je u Zagrebu 1962. godine i ujedno je bio prvi izvještaj o scintigrafiji u nas (9).[35]

U sedamdesetim godinama prošloga stoljeća nuklearno medicinska oprema se priključuje i na digitalna računala (9).[36] Daljnji tehnološki napredak je omogućio konstruiranje sofisticirane brojačke opreme, kojom se biodistribucija radioobilježivača u tijelu mogla znatno kvalitetnije slikovno prikazati, a što je posljedično zajedno s razvojem radiofarmaka, dalo veliki zamah daljnjem razvoju nuklearne medicine (9).[37] Tako je današnja slikovna dijagnostika u nuklearnoj medicini bazirana na fuzioniranju funkcijskog i morfološkog (anatomskog) oslikavanja, odnosno pozitronske emisijske tomografije i kompjutorizirane tomografije (PET/CT), pri čemu nastaje trodimenzionalna slika koja daje veću dijagnostičku vrijednost kako je vidljivo na slici 4.

Pored tehnološkog aspekta, utjecaj digitalne transformacije u nuklearnoj medicini na procese i ljude je vidljiv kroz organizacijske promjene. Tako je početak organizirane kliničke nuklearne medicine u Zagrebu utemeljen Odlukom Medicinskog fakulteta o osnivanju Radioizotopnog odjela na Rebru, koji je 1959. godine započeo s radom (9).[38] Protekom vremena Odjel je prerastao u Klinički zavod za nuklearnu medicinu i zaštitu od zračenja, koji djeluje kao jedna od tridesetak klinika i kliničkih zavoda u okviru KBC Zagreb.



Manualni scintigram štitnjače
(1962. g., KBC Zagreb)



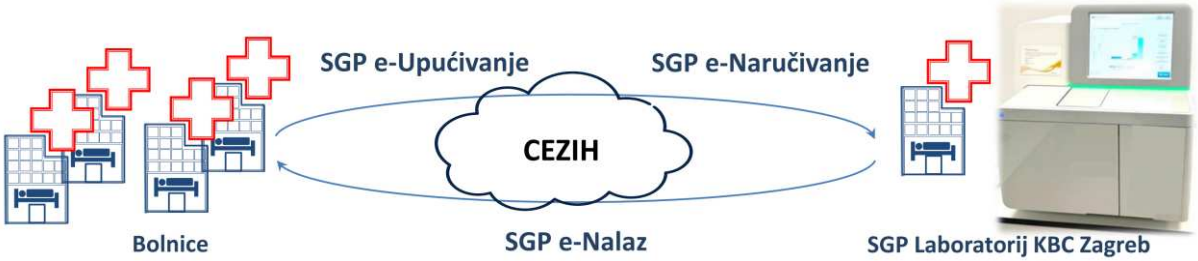
PET/CT - fuzionirani slikovni materijal štitnjače

Slika 4. Prikaz napretka digitalizacije u nuklearnoj medicini

Liječenje u onkologiji je primarno bilo vođeno lokacijom tumora, međutim tehnološkim napretkom u molekularnoj biologiji pristup se mijenja u liječenje vođeno molekularnim karakteristikama tumora (10).[39] Napredna dijagnostika je sve dostupnija, poput primjene metode naprednog sekvenciranja druge generacije (engl. *Next Generation Sequencing - NGS*) kojom se omogućuje masovno sekvenciranje velikih količina genetskog materijala (DNK - deoksiribonukleinska kiselina; RNK - ribonukleinska kiselina) što zapravo tijek liječenja bolesnika usmjerava ka personaliziranom pristupu prilagođenom molekularnim specifičnostima pojedinog bolesnika s ciljem očekivanih poboljšanja u ishodima liječenja. Poticani tehnološkim napretkom

[35] Huić, D., Lovrec, P., (2019), *60 Godina – Klinički zavod za nuklearnu medicinu i zaštitu od zračenja*, Medcinska naklada, Zagreb, str. 15
[36] Huić, D., Lovrec, P., (2019), op.cit., str. 8
[37] Huić, D., Lovrec, P., (2019), op.cit., str. 77
[38] Huić, D., Lovrec, P., (2019.), op.cit., str. 9
[39] Subbiah, V., Kurzrock, R., (2018), *Challenging Standard-of-Care Paradigms in the Precision Oncology Era,* Trends in Cancer, Volume 4, Issue 2, Pages 101-109 [pristupljeno 28.11.2025.]. Dostupno na: https://doi.org/10.1016/j.trecan.2017.12.004

mijenjaju se procesi i organizacijska struktura u bolnicama. U tom smislu tijekom 2024. godine je u KBC Zagreb osnovan te započeo s radom i novi Zavod za personaliziranu medicinu. Zavod je opremljen najsuvremenijim laboratorijskim uređajima za provođenje sveobuhvatnog genomskog profiliranja. Za potrebe naručivanja bolesnika na postupak sveobuhvatne genomske profilacije (SGP) također je po prvi puta u zdravstvenom sustavu RH preko središnjeg informacijskog sustava CEZIH uvedena funkcionalnost e-Naručivanje/e-Nalaz između bolničkih centara kroz funkcionalnost *SGP e-Upućivanje/Naručivanje – SGP e-nalaz*, kako je prikazano na slici 5.



Slika 5. Prikaz digitalizacije procesa SGP e-Naručivanja/e-Nalaza između bolnica (izvor: izrada autora)

Do uvođenja SGP-naručivanja, funkcionalnost e-naručivanje/e-nalaz prema bolničkim ustanovama je bila moguća samo iz primarne zdravstvene zaštite. Vrijednost provedene automatizacije procesa naručivanja je višestruka na način da se ista funkcionalnost može u budućnosti koristiti i za naručivanje niza drugih postupka i medicinskih usluga koje se odvijaju između bolničkih centara, a koji se sada odvijaju bez digitalne poveznice tj. ručno.

U bolničkom ljekarništvu digitalnom transformacijom je omogućen prijelaz s volumetrijske na gravimetrijsku metodu u procesu izrade antineoplastičnih lijekova. Integracijom računala i vaga u izolatorima i uvođenjem bar kodiranja pripravaka u cijelosti je digitaliziran proces Središnje priprave antineoplastičnih lijekova (SPAL). Na primjeru KBC Zagreb sustav SPAL je uveden krajem 2018. godine te početkom 2019. godine provedena integracija s bolničkim informacijskim sustavom - BIS i laboratorijskim informacijskim sputavam - LIS. Daljnja primjena robotiziranih uređaja u pripremi jedinične terapije mijenja način pripreme i izdavanja lijekova bolesnicima, a implementacijom rješenja za cjelovito praćenje puta lijeka se optimizira distribucija i utrošak lijekova na razini bolničkih ljekarni u zdravstvenom sustavu. Navedeni primjeri pokazuju kako se pravilnom implementacijom i cjelovitom integracijom aplikativnih rješenja i digitalnih uređaja očekivano nastoji postići niz pozitivnih efekata poput:

- racionalnije primjene lijekova i optimizacije troškova
- veće sigurnosti bolesnika
- veće sigurnosti zdravstvenih profesionalaca
- sljedivosti svih procesa rada
- sljedivosti svih lijekova
- racionalnijeg korištenja resursa zdravstvenih profesionalca
- pomaka fokusa više na bolesnika, što bi očekivano trebalo rezultirati boljim korisničkim iskustvom i kvalitetom zdravstvene skrbi za bolesnike.

Robotizacija je danas sastavni dio medicinskih procesa, osobito u kirurgiji. Klasični invazivni operativni zahvati sve se češće izvode laparoskopski uz pomoć robotske tehnologije, čime se postiže veća preciznost, smanjuje boravak bolesnika u bolnici, te skraćuje vrijeme oporavka. Uz pomoć UI-a, roboti će postajati sve više samostalni u obavljanu pojedinih operativnih koraka, međutim potpuna odgovornost je kao i u drugim medicinskim segmentima isključivo na zdravstvenom osoblju, dok tehnologija ima pomoćnu ulogu.

Navedeni primjeri digitalne transformacije jasno ukazuju kako se bolničko poslovanje značajno mijenja i unaprjeđuje razvojem novih digitalnih rješenja. Od primjene novih tehnoloških rješenja, oblikovanja procesa i promjena vezanih uz ljudski faktor. Uz dinamične tehnološke trendove može se očekivati dodatno ubrzanje i unaprjeđenje mogućnosti u pružanju zdravstvene skrbi bolesnicima.

Složenost poslovno-tehnološke okoline bolnica, standardizacija i integracija

U praksi se vrlo često susreću informacijska rješenja građena tijekom vremena kao skup izoliranih otoka. Da je takva praksa prisutna i u zdravstvu potvrđuje se i u Nacionalnoj strategiji razvoja zdravstva 2012.–2020. Vlade RH, gdje se navodi kako je unatoč napretku informatizacije zdravstva u proteklih 10 godina i dalje prisutan glavni problem, što se informacijski sustav u velikoj mjeri gradio kao skup izoliranih otoka (11).[40] Također se u Nacionalnom planu razvoja zdravstva za razdoblje od 2021. do 2027. godine navodi kako informacijski sustavi još uvijek nisu u potpunosti cjeloviti i integrirani kako bi omogućili integrirano pružanje zdravstvene zaštite koja bolesnike stavlja u središte pozornosti, a zdravstvenom sustavu na taj način nedostaje je fleksibilnosti da apsorbira sve potrebne promjene i moguća poboljšanja (12).[41]

Imajući u vidu izazove povijesnog razvoja informacijskog zdravstvenog sustava od dostupnih tehnologija i opreme, preko raspoloživih ljudskih i materijalnih resursa, pa sve do zakonskog i regulatornog okvira, sustav je dosegnuo razinu na kojoj je, prema navedenim strateškim dokumentima, nužno usmjeriti fokus na intenzivniju integraciju svih njegovih komponenti. Time bi se povećala sposobnost zdravstvenog sustava u prihvaćanju novih promjena i pružanju integrirane zdravstvene zaštite. Važno je istaknuti kako u visoko umreženoj digitalnoj okolini izgradnja sustava s digitalnim otočnim rješenjima nije prihvatljiva iz različitih aspekata, kao i da se takva praksa danas uvelike mijenja. Međutim, ako prihvatimo realnost postojanja otočnog pristupa, onda se moramo zapitati koliko smo zapravo digitalno sigurni.

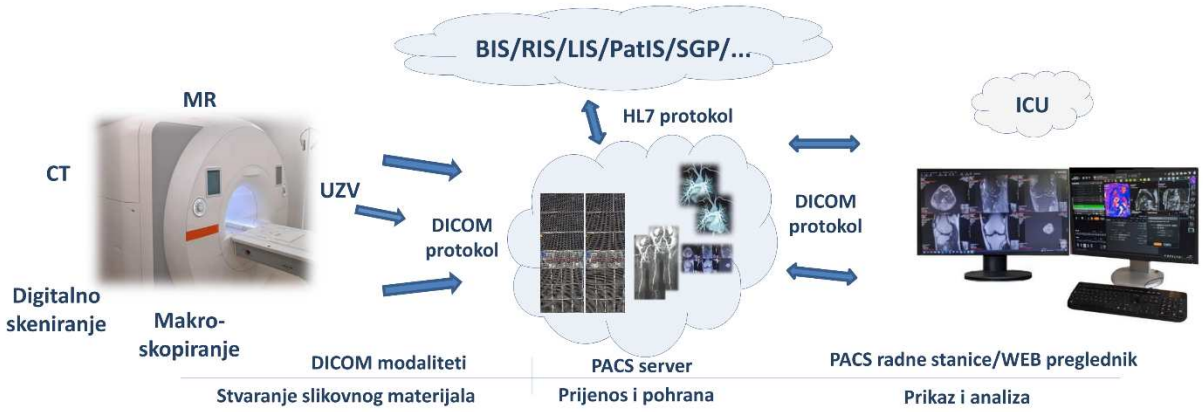
Pri izgradnji informacijskih sustava za podršku bolničkom poslovanju ključna je standardizacija poslovno tehnološke platforme uz visoki stupanj integracije. U razmatranju korištenja otvorenih i zatvorenih standarda svakako treba napomenuti kako zatvoreni standardi, tj. standardi pojedinih proizvođača, vrlo često predstavljaju izazov u integraciji s drugim sustavima i uređajima ali i u pitanjima informacijske sigurnosti. U zdravstvu su opće prihvaćeni otvoreni standardi poput protokola HL7- FHIR i DICOM. Protokol HL7 - FHIR (engl. *Health Level Seven International - Fast Healthcare*

[40] Vlada RH, Ministarstvo zdravlja RH, (2012.), *Nacionalna strategija razvoja zdravstva 2012.– 2020.*, str. 62 [pristupljeno: 25.11.2025.]. Dostupno na: https://zdravlje.gov.hr/UserDocsImages/dokumenti/Programi,%20projekti%20i%20strategije/Skracena%20Nacionalna%20strategija%20razvoja%20zdravstva%20-%20HRV%20-%20za%20web.pdf,

[41] Vlada RH, Ministarstvo zdravstva RH, (2021.), *Nacionalni plan razvoja zdravstva za razdoblje od 2021. do 2027. godine,* str. 3. [pristupljeno: 02.12.2025.]. Dostupno na: https://zdravlje.gov.hr/UserDocsImages/2022%200bjave/Nacionalni%20plan%20razvoja%20zdravstva%202021.-2027..pdf

Interoperability Resources) je međunarodni standard za interoperabilnost u zdravstvu koji se primjenjuje u povezivanju i razmjeni podatka o bolesnicima i drugih medicinskih podataka između bolničkog informacijskog sustava te drugih informacijskih sustava, aplikacija i uređaja (13).[42] Protokol DICOM (engl. *Digital Imaging and Communications in Medicine*) je međunarodni standard za pohranu, prijenos i prikaz medicinskih slika i pripadajućih podataka (14).[43]

Uz primjenu otvorenih protokola bolnički se sustavi mogu graditi na standardiziran način te povezivati kao digitalni specijalistički podsustavi u jedinstvenu poslovno-tehnološku platformu bolničke ustanove s prikazom osnovne strukture na slici 6. Na taj je način moguće povezati, primjerice, više desetaka ili stotina radioloških dijagnostičkih uređaja (MR, CT, PET/CT, UZV i sl.) u jedan radiološki informacijski sustav s konsolidiranim mjestom za pohranu slikovnog materijala – PACS (engl. *Picture Archiving and Communication System*).



Slika 6. Prikaz standardizacije i integracije poslovno-tehnološke platforme bolnice (izvor: izrada autora)

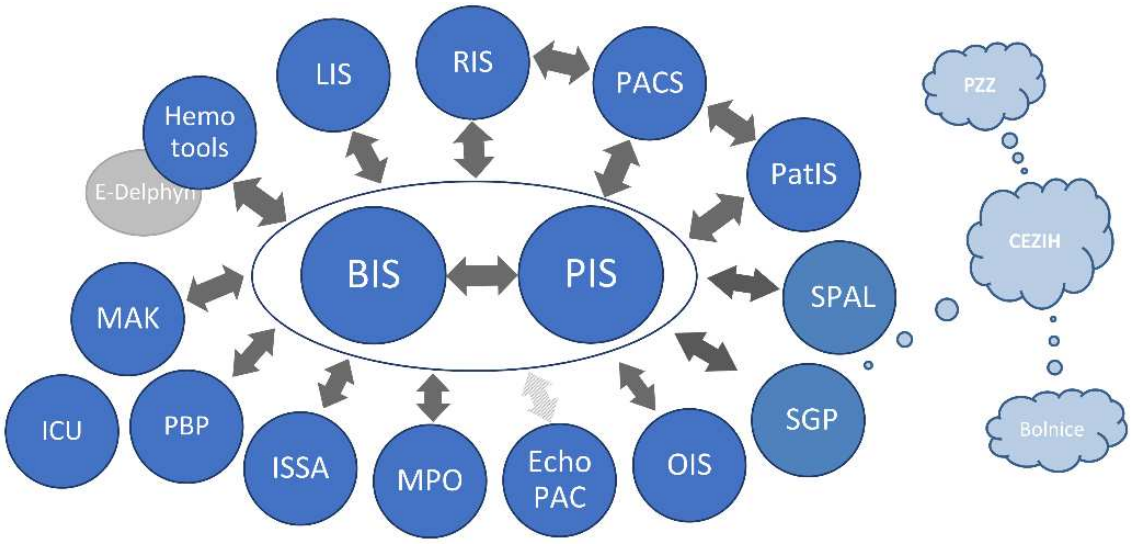
Slično tome, umrežavanjem niza laboratorijsko-dijagnostičke opreme grade se Laboratorijski informacijski sustav (LIS), Patološki informacijski sustav (PatIS), Onkološki informacijski sustav (OIS), Sustav za nadzor bolesnika na intenzivnoj njezi (engl. *Intensive Care Unit - ICU*) i drugo. Sustavi se zatim mogu povezati s bolničkim informacijskim sustavom (BIS) koji se nadalje povezuje s CEZIH-om, te nastavno s drugim bolničkim centrima i primarnom zdravstvenom zaštitom.

Ono što se prepoznaje kao izazov je razvoj novog standarda koji bi podržavao interakciju između medicinskih uređaja tj. omogućio povezivanje uređaja i autonomno donošenje odluka o tretmanu bolesnika, podržano UI-em. Inicijativa se razmatra u sklopu proizvodnje i primjene opreme i sustava na intenzivnoj njezi, kao pomoć medicinskom osoblju čija aktivnost traje 24 sata. Za održavanje vitalnih funkcija bolesnika značajni podaci se prikupljaju iz različitih izvora i uređaja, uključujući i podatke iz laboratorijskih informacijskih sustava. Za automatizaciju procesa intenzivne njege i pomoć medicinskom osoblju potreban je siguran i pouzdan protokol te na njemu baziran sustav interakcije između uređaja, koji bi trebao biti omogućen napretkom u digitalnoj transformaciji medicinske opreme i kliničkih bolničkih procesa.

[42] Health Level Seven International (HL7) [internet] [pristupljeno: 25.11.2025.]. Dostupno na: https://www.hl7.org/index.cfm,
[43] DICOM® Secretariat [internet] [pristupljeno: 25.11.2025.]. Dostupno na: https://www.dicomstandard.org/contact

Na primjeru KBC-a Zagreb kao najveće, te po broju i raznolikosti zdravstvenih usluga koje pruža jedinstvene zdravstvene ustanova u RH, može se prikazati vrlo složena poslovna okolina. U okviru ustanove djeluje 101 referentni centar Ministarstva zdravstva, 30 klinika i kliničkih zavoda te ima oko 6.000 zaposlenika. Organizacija raspolaže složenom IT infrastrukturom, brojnim sustavima i uređajima, brojnim korisnicima informacijskih sustava te pripadajućim digitalnim identitetima. Središnji logički dio čine Bolnički informacijski sustav (BIS) i Poslovni informacijski sustav (PIS) s kojima se povezuju brojni drugi informacijski sustavi, mrežni uređaji i oprema kako je konceptualno prikazano na slici 7. Podaci pokazuju da složenost poslovno-tehnološke tj. digitalne okoline KBC-a Zagreb iz godine u godinu raste.

U kontekstu digitalizacije i povezanosti procesa u okviru zdravstvenog informacijskog sustava u cjelini, ključna je sustavna primjena računalno potpomognutog unošenje liječničkih naloga (engl. *Computerized Physician Order Entry – CPOE*). Sustav CPOE omogućuje liječnicima unos elektroničkih naloga primjerice za lijekove, laboratorijske, radiološke i druge postupke, što ubrzava protok informacija, smanjuje pogreške, omogućuje sljedivost i bolju kvalitetu u pružanju zdravstvene skrbi pacijentima.



Slika 7. Prikaz složenosti poslovno-tehnološke okoline bolnice (izvor: izrada autora)

U suvremenim zdravstvenim informacijskim sustavima CPOE se primjenjuje cjelovito u procesima primarne zdravstvene zaštite, ljekarnama i bolničkim ustanovama. Elektronički nalozi poput e-Recepta, e-Uputnica i e-Nalaza su opće poznati primjeri kako u praksi primjena elektroničkih naloga olakšava rad liječnicima i pacijentima, čineći u određenim segmentima zdravstvenu skrb jednostavnijom i dostupnijom.

Primjena elektroničkih naloga predstavlja ključnu komponentu digitalne transformacije kliničkih procesa. Danas je to zapravo standard u bolnicama ključan za sigurnost pacijenata i učinkovitost rada. CPOE je tako integralni dio bolničkog informacijskog sustava (BIS) kao središnjeg mjesta za upravljanje svim relevantnim podacima o pacijentu u okviru bolničkih ustanova. BIS obuhvaća cjelokupni skup administrativnih, kliničkih i terapijskih podataka, uključujući identifikacijske podatke, alergije, dijagnoze, ordiniranu i provedenu terapiju, čime se osigurava jedinstveni i konzistentni izvor podataka o kliničkoj slici pacijenta. CPOE-funkcionalnosti BIS-a omogućuju liječnicima elektroničko ordiniranje terapije, laboratorijskih i drugih dijagnostičkih pretraga odnosno radnih naloga izravno unutar BIS-a, bez potrebe za papirnatom dokumentacijom ili višestrukim unosom podataka. U

integraciji BIS-a s laboratorijskim informacijskim sustavom (LIS), omogućuje se dvosmjerna razmjena podataka. BIS prosljeđuje naloge za laboratorijske pretrage, dok su rezultati pretraga dostupni u BIS-u za prikaz u kliničkom kontekstu pacijenta. Osim laboratorijskog sustava, BIS se povezuje i sa svim drugim relevantnim specijalističkim sustavima unutar bolničke ustanove, uključujući poslovni informacijski sustav, ljekarnički informacijski sustav, radiološki sustav, onkološki sustav, patološki sustav, sustav za pripremu antineoplastičnih lijekova, sustav za pripremu jedinične terapije i dr. U konačnici je povezan s CEZIH-om te s elektroničkim kartonom pacijenta u nacionalnom zdravstvenom sustavu. Pri implementaciji specijalističkih informacijskih sustava u bolničkoj ustanovi, integracija s BIS-om i elektroničko slanje i zaprimanje radnih naloga je nužno. Na taj način se osigurava razmjena svih potrebnih podataka o pacijentu i kliničkih operativnih informacija čime se uklanjaju ručni prijepisi i smanjuje rizik od pogrešaka.

Izazovi u implementaciji funkcionalnosti CPOE uključuju prije svega standardizaciju, budući da različite bolnice koriste različite informacijske sustave, što otežava njihovu jedinstvenu primjenu. Nadalje, tu je i obuka osoblja, pri čemu se liječnici i medicinske sestre trebaju prilagoditi novom načinu rada. Značajan izazov predstavljaju i investicije, s obzirom na dostignutu razinu zrelosti tehnološke okoline u bolnicama, implementacija i integracija novih funkcionalnosti zahtijevaju odgovarajuća financijska sredstva i tehničku potporu

Opisani integrirani informacijski ekosustav potvrđuje ulogu BIS-a kao središnje platforme za provedbu CPOE-a te doprinosi povećanju sigurnosti pacijenata, učinkovitosti kliničkih procesa i kvaliteti zdravstvene skrbi kroz standardizirano, digitalno i interoperabilno upravljanje kliničkim nalozima.

Također, uz brojna tehnološka rješenja, složenosti bolničke poslovno-tehnološke okoline doprinosi i digitalni otisak svakog zaposlenika kao korisnika informacijskog sustava. Digitalni otisak obuhvaća sve tragove koje osoba ostavlja tijekom korištenja digitalnih tehnologija i interneta, bilo svjesno ili nesvjesno. Takvi skupovi podataka mogu se koristiti za identifikaciju, profiliranje ili praćenje aktivnosti pojedinca na mreži.

Povećanje složenosti digitalne poslovne okoline bolničkih ustanova istodobno povećava površinu napada u kibernetičkom prostoru, čime organizacije postaju izloženija kibernetičkim prijetnjama i rizicima.

Podaci i informacijski sustavi bolnice kao ključna imovina

U suvremenim zdravstvenim sustavima podaci se sustavno prikupljaju, obrađuju i analiziraju na različitim razinama. To obuhvaća primjerice podatke o bolesnicima, kliničke informacije povezane s poviješću bolesti, laboratorijske nalaze, dijagnostičke snimke, klinička ispitivanja, kao i operativne podatke vezane uz bolničke procese, troškove i resurse.

Podaci u zdravstvu ključni su za kvalitetnu skrb i sigurnost bolesnika. Integracijom velikih skupova podataka (engl. *Big data*) omogućuje se razvoj prediktivne analitike, personalizirane medicine te naprednije upravljanje javnim zdravljem. Pored samih tehnoloških bolničkih sustava, podaci također predstavljaju ključnu imovinu u bolničkom poslovanju te ih je potrebno na odgovarajući način i štititi.

Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation - GDPR*) nalaže obradu podataka isključivo s opravdanom svrhom koja mora biti izrijekom navedena i opravdana te određena

u vrijeme prikupljanja osobnih podataka. Osobni podaci bi pri tome trebali biti primjereni, bitni i ograničeni na ono što je zapravo nužno za svrhe u koje se obrađuju (15).[44] Sukob s uredbom nastaje kada se podaci prikupljaju, obrađuju ili im se pristupa neovlašteno, bez pravne osnove ili izvan jasno definirane svrhe. GDPR posebno naglašava načela zakonitosti, poštenosti i transparentnosti, ograničenje svrhe, minimizaciju podataka, točnost, ograničenje pohrane te integritet i povjerljivost.

Bolničke ustanove kao voditelji obrade podataka su obvezne osigurati da se osobni podaci obrađuju na način koji štiti prava i slobode pojedinaca, uz primjenu odgovarajućih tehničkih i organizacijskih mjera. Na taj način GDPR ne predstavlja samo regulatornu obvezu, već i okvir za izgradnju povjerenja između organizacija i korisnika.

Informacijska sigurnost postiže se implementacijom odgovarajućeg, odnosno prikladnog skupa kontrola, što uključuje politike, pravila, procese, procedure, organizacijsku strukturu te softverske i hardverske funkcije. Uspostavljanjem Sustava upravljanja informacijskom sigurnošću (engl. *Information Security Management System – ISMS*) omogućuje se zaštita ciljeva organizacije, kontinuiteta poslovanja, imovine poput opreme, podataka i sl., zaposlenika i bolesnika, kao i postizanje regulatorne i zakonske usklađenosti u odnosu na rizike iz digitalnog okruženja.

Sustav informacijske sigurnosti u pravilu se izgrađuje sukladno odgovarajućim standardima, ponajprije sukladno standardu ISO/IEC 27001, koji predstavlja globalno priznati okvir za upravljanje informacijskom sigurnošću (16). Standard ISO/IEC 27001/2022 je zadnja je verzija standarda izdana 2022. godine. Prvi dio standarda sadrži 11 poglavlja sa Zahtjevima norme (engl. *Requirements*). Prva četiri poglavlja su uvodna dok su ostalih sedam poglavlja standarda obvezni Zahtjevi u primjeni za organizacije koje se žele uskladiti i certificirati prema standardu ISO 27001. Drugi dio norme je Prilog A, koji sadrži 93 kontrole. Ako organizacije provode i certifikaciju implementiranog sustava ISMS sukladno standardu ISO 27001, to može biti dodatno korisno, međutim nije nužno i obvezno. Predmetno ovisi o regulatornim zahtjeva ili ciljevima organizacije.

Primjena standarda ISO 27001 osigurava:

- definiranje i provođenje sigurnosnih politika i procedura,
- strukturirani pristup identifikaciji i upravljanju rizicima,
- kontinuirano praćenje i poboljšavanje sigurnosnih mjera,
- dokaz usklađenosti prema zakonskim i regulatornim zahtjevima, povjerenje partnera, bolesnika i korisnika.

Na taj način sustav upravljanja informacijskom sigurnošću, uz ispunjenje zakonskih i regulatornih zahtjeva, postaje i strateška prednost organizacije.

U kontekstu razmatranja poslovne okoline organizacije, interesnih skupina (dionika), zahtjev norme ISO 27001 u poglavlju 4. Kontekst organizacije (engl. *Contest of organisation*) definira kako organizacije u uspostavljanju sustava ISMS moraju razumjeti vlastiti kontekst organizacije (16). To se odnosi na traženje i davanje odgovora na pitanja koja je to kritična imovina organizacije koju štitimo (informacije tj. podaci, serveri, aplikacije, digitalna oprema, medicinski sustavi i sl.) tj. gdje to postoji potreba u organizaciji za štićenjem povjerljivosti, integriteta i dostupnosti. Također treba utvrditi tko su dionici u organizaciji, interni ili eksterni, koji su njihovi legitimni zahtjevi vezano uz informacijsku

[44] Europski parlament i Vijeće Europske unije, 2016/679, *Opća uredba o zaštiti podataka, članak 39.* [pristupljeno: 03.12.2025.]. Dostupno na: https://eur-lex.europa.eu/legal-content/HR/TXT/HTML/?uri=CELEX:32016R0679&from=HR,

sigurnost i kako ih postići u sklopu izgradnje sustava ISMS (16).[45] Nadalje u poglavlju 5. Vođenje (engl. *Leadership*) se definira zahtjev za posvećenošću najvišeg menadžmenta u uspostavi i održavanju ISMS-a koji se ogleda kroz uspostavljanje politike i ciljeva informacijske sigurnosti, osiguranje potrebnih resursa organizacije, jasno komuniciranje i davanje podrške u uspostavljanju sustava ISMS i njegovom kontinuiranom unaprjeđenju (16).[46]

Pri uvođenju sustava ISMS sukladno zahtjevima standarda ISO 27001, organizacije moraju definirati svoje zahtjeve vezane za informacijsku sigurnost, pri čemu su tri glavna izvora IS zahtjeva:

- kontrole prema standardu ISO 27001: izbor kontrola se temelji na provedenoj, za pojedinu organizaciju specifičnoj IS-analizi rizika, koja je specifična jer uzima u obzir poslovnu strategiju i ciljeve organizacije. Cilj primjene odabranih kontrola je smanjenje rizika na prihvatljivu razinu te ispunjavanje zakonskih i regulatornih zahtjeva, kao i ugovornih obveza koje organizacija ima. Organizacije općenito trebaju provoditi procjenu rizika i njegovog utjecaja na poslovanje u cjelini, strategiju i ciljeve poslovanja. To može biti podržano i kroz procjenu rizika specifično vezano uz informacijsku sigurnost, kao jedne od komponenti ocjene rizika u organizaciji. Očekivani rezultat je određivanje kontrola neophodnih za umanjenje rizika informacijske sigurnosti kako bi rezidualni ili preostali rizik dostigao kriterije prihvatljivosti rizika za organizaciju. Pri tretiranju rizika i postizanju prihvatljive razine sigurnosti treba pažljivo odabrati i implementirati odgovarajuće kontrole.
- pravni, statutarni, regulatorni i ugovorni zahtjevi koje organizacija i njezine zainteresirane strane poput ugovornih partnera, dobavljača roba i pružatelja usluga, moraju zadovoljiti u odnosu na okolinu organizacije.
- principi, ciljevi i poslovni zahtjevi organizacije vezani uz cjeloživotni ciklus informacija koje je organizacija razvila kako bi podržala svoje operativno djelovanje.

Rezultati provedene procjene rizika trebaju biti osnova za usmjeravanje i određivanje prikladnih aktivnosti u okviru organizacije. Služe za prioritizaciju u upravljanju informacijskim sigurnosnim rizicima i implementiranju kontrola neophodnih za zaštitu od utvrđenih rizika. U određivanju primjene pojedinih kontrola organizacije trebaju razmotriti resurse i investicije potrebne za implementaciju i održavanje pojedine kontrole u odnosu na dobivenu poslovnu vrijednost, odnosno potencijalni utjecaj i štetu koja može nastati za poslovanje nastupanjem sigurnosnog incidenta u slučaju da kontrola nije primijenjena. Na taj način se može odrediti koje kontrole i kojim prioritetom treba primjetni kako bi se organizacija zaštitila od prepoznatih rizika.

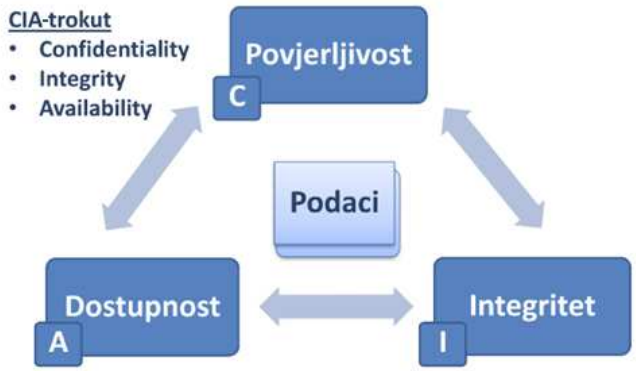
Prikladan i učinkovit sustav ISMS pruža menadžmentu organizacije i zainteresiranim stranama sigurnost da su njihove informacije i s njima povezana imovina razumno sigurne i zaštićene od prijetnji i rizika, čime organizacije ostvaruju svoje poslovne ciljeve na siguran način.

---

[45] International Organization for Standardization – ISO, (2022), ISO/IEC 27001:2022 , *Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, 4 Context of the organization, page 1 [pristupljeno: 03.12.2025.]. Dostupno na: https://www.iso.org/standard/27001

[46] International Organization for Standardization – ISO, (2022), ISO/IEC 27001:2022, op.cit., 5 Leadership, page 2. [pristupljeno: 03.12.2025.]. Dostupno na: https://www.iso.org/standard/27001

Kada je riječ o zaštiti podataka ona se primarno ogleda kroz komponente povjerljivosti, integriteta i dostupnosti, što se u terminologiji informacijske sigurnosti naziva i CIA-trokut (engl. *Confidentiality, Integrity, Availability - CIA*)[47], kako je prikazano na slici 8 (17).



Slika 8. Prikaz pristupa zaštite podatka kroz CIA-trokut (izvor: izrada autora)

Povjerljivost znači da su podaci dostupni samo ovlaštenim osobama. Cilj je zaštititi povjerljive podatke od neovlaštenog pristupa podacima. Pristup u tom smislu može značiti na primjer ovlaštenje za čitanje, uređivanje tj. mijenjanje ili brisanje. Integritet podataka znači da podaci nisu neovlašteno mijenjani. Mjere usmjerene na povećanje integriteta informacija stoga također ciljaju na pitanje autorizacije pristupa u vezi sa zaštitom od vanjskih i unutarnjih napada. Potrebno je osigurati ispravnost podataka i sustava, potpunost odnosno cjelovitost podatka i sljedivost promjena. Dostupnost podataka znači da podaci, uključujući potrebne informatičke sustave, moraju biti dostupni svakoj ovlaštenoj osobi u bilo koje vrijeme i upotrebljivi tj. funkcionalni u potrebnoj mjeri. Ako podaci nisu dostupni uslijed kvara sustava ili sl. to može dovesti do poremećaja u održavanju procesa ili pak poremećaja s dalekosežnim posljedicama za organizaciju. Odgovor na pitanje održavanja kontinuiteta poslovanja daju aktivnosti povezane s izradom plana kontinuiteta poslovanja (engl. *Business Continuity Plan - BCP*) i plana oporavka nakon prekida poslovanja uslijed nastupanja katastrofalnih posljedica (engl. *Disaster Recovery Plan – BRP*).

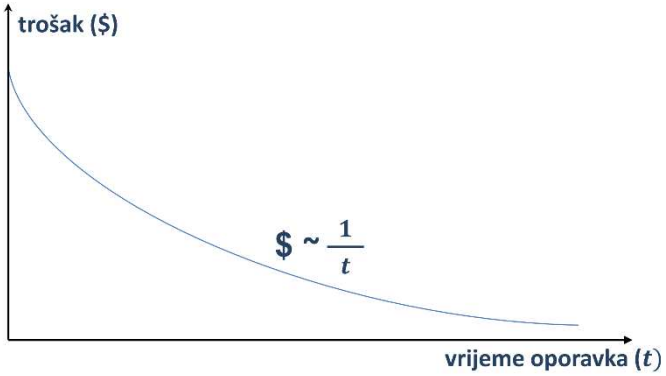
Sustav upravljanja informacijskom sigurnošću čuva povjerljivost, cjelovitost i dostupnost informacija (podataka) primjenom procesa upravljanja rizicima, te zainteresiranim stranama za upravljanje informacijskom sigurnošću pruža sigurnost da se rizicima informacijske sigurnosti u organizaciji odgovarajuće i upravlja (16).[48]

Informacijski sustavi ključni su za poslovanje bolnice, pa kontinuitet rada bolnice ovisi o njihovoj ispravnosti, pouzdanosti i dostupnosti, kao i o dostupnosti medicinskih podataka koje oni pohranjuju i obrađuju. U okviru Sustava upravljanja informacijskom sigurnošću, pored analize rizika, bolnice trebaju identificirati koji su to sustavi, oprema i uređaji ključni za njihovo poslovanje, koliko su izloženi rizicima i koje mjere trebaju poduzeti za umanjenje rizika. Ključni sustavi su oni bez kojih se određeni poslovni procesi bolnice ne mogu nastaviti odvijati ako je sustav nedostupan uslijed nekog incidenta, kvara, kibernetičkog napada ili sl. U tu svrhu provodi se analiza utjecaja na poslovanje (engl. *Business Impact Analysis - BIA*) koja treba dati odgovore na neka ključna pitanja. Jedno od pitanja je koliko dugo poslovni proces može održivo raditi bez informatičke podrške odnosno kritičnog informacijskog

[47] Fortinet, Inc, *What Is the CIA Triad?* [pristupljeno: 03.12.2025.] Dostupno na: https://www.fortinet.com/resources/cyberglossary/cia-triad,
[48] International Organization for Standardization – ISO, ISO/IEC 27001:2022, op. cit., Introduction, page V.

sustava, tj. nakon koliko vremena od incidenta sustav mora biti opravljen (engl. *Recovery Time Objective - RTO*). Drugo ključno pitanje je u koju vremensku točku prije nastupanja incidenta smijemo vratiti poslovanje (engl. *Recovery Point Objective - RPO*) tj. koliko podataka smijemo izgubiti prilikom povratka u redovno poslovanje. Ako je očekivano vrijeme oporavka poslovanja kraće i dozvoljeni gubitak podataka manji, tada su mjere koje treba poduzeti za osiguranje oporavka složenije i skuplje. Vrijeme opravka sustava odnosno kritičnog procesa i trošak za njegovo postizanje su u obrnuto proporcionalnom odnosu kako je prikazano na slici 9.

Predmetno je važno razumjeti s aspekta očuvanja kontinuiteta poslovanja i opravka, posebno kod incidenata s velikim utjecajem na organizaciju i njezino redovno poslovanje. Za te potrebe, organizacije izrađuju posebne planove kontinuiteta poslovanja (engl. *Busienss Continuity Plan – BCP*) i planove oporavka od katastrofe (engl. *Busienss Continuity Plan – BCP*). Na taj način su pitanja kontinuiteta poslovanja lišena mogućeg pristupa slobodne procjene i prepuštanja slučaju, već su svjesna i upravljana odluka organizacije o svojim poslovnim ciljevima, potrebama i prihvatljivim troškovima.



Slika 9. Prikaz uzajamne povezanosti vremena oporavka i troška za postizanje oporavka sustava (izvor: izrada autora)

Kada je riječ o zaštiti pristupa informacijskim mrežnim sustavima i podacima, nužna je primjena slojevitih mjera odnosno kontrola koje osiguravaju odgovarajuću razinu sigurnosti. Međutim, u praksi se nerijetko događa da primjena takvih mjera smanjuje korisničko iskustvo rada na sustavu, povećava zahtjeve prema sistemskom administrativnom osoblju ili pak utječe na operativnu učinkovitost. Primjena sigurnosnih zaštitnih mjera nije pitanje samo voljnosti u primjeni već postaje i zakonska obveza.

Tako se primjerice Pravilnikom o načinu obrade zdravstvenih i drugih osobnih podataka u zdravstvenim nacionalnim i institucionalnim informacijskim sustavima u zdravstvu, konkretno nalaže obvezna primjena snažnih zaporki visoke razine sigurnosti, od najmanje 16 znakova (kombinacija velikih i malih slova, brojki i interpunkcijskih znakova) (18).[49]

Obveza organizacija u stvaranju zapisa o svakoj prijavi i aktivnosti na kritičnom mrežnom i informacijskom sustavu radi osiguravanja forenzičkog traga, propisana je u mjerama Uredbe o kibernetičkoj sigurnosti (7).[50]

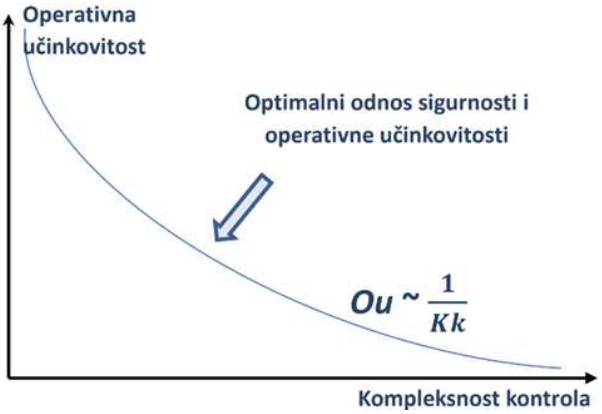
[49] Narodne novine, (2024.), *Pravilnik o načinu obrade zdravstvenih i drugih osobnih podataka u zdravstvenim nacionalnim i institucionalnim informacijskim sustavima u zdravstvu*, NN 150/2024, članak 8. [pristupljeno: 01.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/ clanci/sluzbeni/full/2024_12_150_2465.html,

[50] Narodne novine, (2024.), *Uredba o kibernetičkoj sigurnosti*, NN 135/2024, *mjera: 5. Osnovne prakse kibernetičke* higijene [pristupljeno: 01.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_135_2217.html,

Za prijavu na mrežne resurse redovito se, uz korištenje lozinke, primjenjuje višefaktorska autentikacija (engl. *Multi Factor Authentication - MFA*), što je ujedno i preporuka Nacionalnog centra za kibernetičku sigurnost (19).[51] U slučaju pokušaja neovlaštenog korištenja nečije lozinke, drugi faktor autentikacije služi kao dodatna zaštita. Primjena MFA značajno povećava razinu sigurnosti korisničkih računa i osjetljivih podataka, a u praksi se najčešće koristi kombinacija lozinke s jednokratnim kodom, mobilnom aplikacijom, biometrijskim podacima ili sigurnosnim tokenom.

U cilju smanjenja mogućnost neovlaštenog pristupa osjetljivim podacima preporučuje se po ostvarenoj prijavi na mrežni resurs koristiti načelo minimalno potrebnih prava pristupa (engl. *least privilege*), čime se korisnicima dodjeljuju samo ona prava koja su nužna za obavljanje njihovih zadataka.

Primjena različitih kontrolnih mjera za umanjene utvrđenih rizika i povećanje sigurnosti je nužna. Međutim upravljanje sigurnošću informacijskog sustava zahtijeva pažljivo usklađivanje odnosa operativne učinkovitosti i kompleksnosti kontrola kako bi se postigla ravnoteža između zaštite i nesmetanog poslovanja. Potrebno je postići optimalni odnos između razine sigurnosti i operative učinkovitosti kako je prikazano na slici 10.



Slika 10. Prikaz uzajamne ovisnosti operativne učinkovitosti i kompleksnosti kontrola (izvor: izrada autora)

Kibernetički napad: ne ako, već kada se dogodi

Prema godišnjem izvješću Nacionalnog CERT-a od ukupno obrađenih incidenata u Hrvatskoj u 2024. godini, čak njih 58% je povezano s *phishingom*, kao pokušajem navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala poput e-pošte, URL-a i sl.) (20).[52] Pokušaji krađe podatka su iznimno učestali, dok neke analize pokazuju da je čak 82% proboja u organizacije rezultat korištenja ukradenih lozinki odnosno identiteta. Dok je 22% organizacija je bilo napadnuto *ransomware*-napadom uzrokovanim kompromitiranim računima. Identiteti na računalnoj mreži ili digitalni identiteti pored osoba uključuju sustave i aplikacije, uređaje i automatizirane servise.

[51] Nacionalni centar za kibernetičku sigurnost - NCSC HR: *Prioritetne preporuke za zaštitu od kibernetičkih napada*, str. 2. [pristupljeno: 08.10.2025.]. Dostupno na: https://ncsc.hr/UserDocsImages/ostalo/Prioritetne_preporuke_za_zastitu_od_kibernetickih_napada.pdf?vel=677572,

[52] Nacionalni CERT - CERT.hr, *Godišnji izvještaj Nacionalnog CERT a za 2024. godinu* [pristupljeno: 28.11.2025.]. Dostupno na: https://www.cert.hr/ godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2024-godinu/,

I u nedavnom kibernetičkom napadu tijekom 2024. koji je zahvatio KBC Zagreb, napadači su za realizaciju prijetnje koristili tehniku krađe identiteta. Kao krajnji oblik napada implementiran je *ransomware*, s namjerom ugrožavanja sigurnosti podataka i poslovnih procesa, pri čemu se uobičajeno za oporavak taži otkupnina. U objavi o napadu na društvenoj mreži X, odgovornost za napad je preuzela kriminalna *cyber*-grupa *LockBit3.0*. Jasno je vidljivo da je napadač znao kako je za metu napada odabrana ustanova iz zdravstvenog sektora s određenim parametrima poput broja zaposlenih, godišnjeg budžeta i sl. Predmetno potvrđuje prethodna nerazmatranja toga da povećanje složenosti digitalne okoline ujedno povećava izloženost subjekta kibernetičkim prijetnjama. Međutim, to ne znači da su drugi subjekti izuzeti od napada. Vrlo je jasno kako zapravo svi digitalni subjekti mogu postati metom kibernetičkog napada.

Praksa je pokazala da će napadač pokušati odabrati najosjetljiviji dio dana, tj. vrijeme iza ponoći, kada se očekuje najmanje aktivnosti na računalnoj mreži, kako bi u svojim aktivnostima ostao što duže nezamijećen, te maksimizirao efekte pokrenutog napada.

Po utvrđivanju neuobičajenih aktivnosti i potvrdi incidenta važna je brza reakcija i poduzimanje mjera i aktivnosti na izolaciji prijetnje, te ograničenju širenja i prevencije štetnih posljedica.

U postupku oporavka ključna je učinkovita komunikacija između svih internih i vanjskih timova te drugih dionika uključenih u proces oporavka. Posebno je važno pravodobno izvješćivanje i koordinacija aktivnosti s nadležnim državnim tijelima, kao i transparentna komunikacija prema javnosti. Primarno se to odnosi na suradnju s nadležnim Timom za oporavak nakon incidenta (CSIRT), ali i na uključivanje svih ugovornih strana koje pružaju upravljane usluge za oporavak kritičnih sustava.

Također, u skladu s javno objavljenim stavom Vlade RH da s napadačima nema pregovora, svi raspoloživi resursi su posvećeni što skorijem oporavku informacijskih sustava i servisa bolnice.

Kibernetičkim napadom KBC Zagreb nije trajno onesposobljen u pružanju skrbi za bolesnike, radilo se otežano i usporeno, ali sustav u cjelini nije prestao s radom. Bolesnicima je pružena potrebna skrb, a do oporavka središnjeg ispisnog rješenja liječnici su potrebne nalaze pisali ručno. Recentni primjer pokazuje kako je kibernetičkim napadom način rada iz digitalnog oblika u trenutku vraćen na ručni ispis, tj. na desetke godina unatrag. Sukcesivnim oporavkom pojedinih servisa bolnica je tijekom narednih dana vraćena u puni kapacitet pružanja zdravstvene skrbi.

Iskustva kibernetičkih napada jasno ukazuju da potpuna sigurnost nije ostvariva, no nužno je razvijati sposobnost zaštite. Statistički gledano, nije pitanje hoće li se kibernetički napad dogoditi, već kada će se dogoditi. Proces jačanja kibernetičke otpornosti zahtijeva sustavno upravljanje internim i vanjskim resursima uključujući odgovarajuća stručna znanja i kapacitete, s posebnim naglaskom na upravljanje sigurnošću lanca dobave.

Sustavna briga za nacionalni kibernetički prostor

Bitno je istaknuti da u Hrvatskoj postoji sustavna briga za zaštitu nacionalnog kibernetičkog prostora koja se ogleda kroz ulogu nadležnog CSIRT-a za zdravstveni sektor, te donošeni zakonski okvir za jačanje kibernetičke otpornosti subjekata.

Nadležni tim za odgovor na kibernetičke incidente tj. CSIRT (engl. *Computer Security Incident Response Team*) za sektor zdravstva, obavlja svoje zadaće u sklopu Nacionalnog centra za

kibernetičku sigurnost (NCSC-HR) ustrojenog u okviru Sigurnosno-obavještajne agencije (SOA). Proaktivna uloga nadležnog CSIRT-a se ostvaruje uključenjem bolničkih ustanova u SK@UT, nacionalni sustav za otkrivanje kibernetičkih prijetnji i zaštitu kibernetičkog prostora, putem distribuirane mreže senzora i alata za kibernetičku zaštitu. Reaktivna uloga CSIRT-a se ostvaruje kroz aktivno sudjelovanje i pružanje pomoći subjektu u upravljanju procesom odgovora na incident kao i samog opravka nakon incidenta. Takva pomoć se pokazuje kao iznimno važna i ključna u sprečavanju širenja incidenta i smanjenju posljedica kibernetičkog napada (7).

Kada je u pitanju zakonodavni okvir vezan uz kibernetičku sigurnost treba istaknuti kako je Republika Hrvatska među prvim članicama Europske transponirala direktivu NIS2 u lokalno zakonodavstvo kroz Zakon o kibernetičkoj sigurnosti – ZKS i Uredbu o kibernetičkoj sigurnosti – UKS (6, 7).

Primjena zakona i provedba mjera u području kibernetičke sigurnosti obuhvaća niz ključnih aktivnosti koje između ostalog uključuju: provedbu je kategorizacije obvezujućih subjekata, obvezu izvještavanja o incidentima nadležnih tijela o kibernetičkim incidentima, upravljanje rizicima i primjenu mjera kibernetičke sigurnosti, te upravljanje sigurnošću lanca dobave.

Uredba o kibernetičkoj sigurnosti obuhvaća 13 mjera i 109 podmjera, čijim se provođenjem osigurava sustavan pristup zaštiti podataka i infrastrukture obveznih subjekata. Posebnu važnost pri tome ima sigurnost dobavljačkog lanca, budući da je sigurnost samog subjekta neraskidivo povezana s kibernetičkim prijetnjama koje mogu dolaziti od ugovornih strana koje isporučuju robu i pružaju ključne usluge za poslovanje subjekta. Kod provedbe nabave i sklapanja ugovora potrebno je voditi računa da su uključeni minimalni sigurnosni zahtjevi, poput definiranja razine kvalitete usluga (engl. *Service Level Agreement - SLA*), odredbe o povjerljivosti (engl. *Non-Disclosure Agreement - NDA*), pravo na audit, obveze izvještavanja o incidentima, posjedovanje relevantnih certifikata i drugo. Na taj način se osigurava da dobavljački lanac ne postane slaba karika u sustavu, već da aktivno doprinosi jačanju ukupne kibernetičke otpornosti organizacije (7).

Zakonom su za utvrđene nesukladnosti propisane novčane kazne. Međutim, opća je preporuka da organizacije primarno usmjere pažnju na osiguravanje informacijske i kibernetičke sigurnosti vlastitog poslovanja. Usklađenost sa Zakonom i Uredbom bi trebala biti posljedica sustavno implementiranih mjera kibernetičke sigurnosti (6, 7).

Upotreba UI-a u digitalnoj medicini i sigurnosti

UI već danas daje izniman doprinos digitaliziranim procesima u medicini kroz optimizaciju rutinskih poslova. Potencijali primijene UI-a u zdravstvu su različiti. Od pomoći u laboratorijskoj, radiološkoj, patološkoj dijagnostici, ubrzanju tijeka kliničkih ispitivanja, razvoju novih lijekova, preciznijoj primjeni lijekova, sprječavanja neautoriziranih aktivnosti do boljeg upravljanja troškovima, podrške učinkovitijim administrativnim i kliničkim procesima.

Sljedeća faza trebala bi biti automatizacija složenijih medicinskih procesa. Naime prednost UI-a se iskazuje u analizi, povezivanju i interpretaciji velikog broja medicinskih podataka, ali i mogućnosti donošenja prediktivnih zaključaka. Tako integriranje UI-a u medicinarske radne procese u bolnici može omogućiti vrijednu pomoć medicinskom osoblju u donošenju odluka o skrbi pacijenta, prije svega kroz povezivanje različitih izvora podataka laboratorijskih, radioloških, patoloških i drugih dijagnostičkih sustava, zatim bolničkog kartona pacijenta, povijesnih podataka pacijenta iz

elektroničkog kartona pacijenta na CEZIH-u, kao i drugih izvora podataka o medicinskim znanjima, protokolima, lijekovima, relevantnim istraživanjima i sl.

Tijekom pregleda i kliničke obrade bolesnika liječnici bi mogli dobivati vrijedne rezultate pretraživanja utemeljene na dokazima o tretmanu, dijagnostici i postupcima u realnom vremenu. Promatranjem vitalnih znakova bolesnika primjerice u intenzivnoj njezi, UI može upozoriti liječnika o povećanju nekih čimbenika rizika i promjeni trenutnog stanja bolesnika. UI to može raditi tijekom 24 sata i bez odmora.

UI na taj način može biti odličan digitalni asistent liječnicima u svakodnevnom radu, pomažući u bržoj i točnijoj dijagnostici, primjeni lijekova, praćenju stanja pacijenta, donošenju odluka o tijeku liječenja i u konačnici postizanju boljeg očekivanog ishoda liječenja.

Kada je riječ o upotrebi UI-a u informacijskoj sigurnosti onda je njezina uloga je dvojaka. S jedne strane UI se pojavljuje kao alat za stvaranje novih sofisticiranih prijetnji. Primjerice, UI značajno unaprjeđuje phishing i socijalni inženjering, pa je danas gotovo nemoguće jednostavno prepoznati koje su poruke i sadržaji autentični, a koji zapravo predstavljaju prijevarne aktivnosti. Iznimno vjerno generirani *phishing-mailovi* putem UI, zatim lažno generirane tj. sintetizirane glasovne poruke, video ili slikovni sadržaji (engl. *deepfake*), lažni korisnički servisi (engl. *chatbot*) i sl. usmjereni su na krađu identiteta, osobnih podataka korisnika, krađu podataka o bankovnim karticama i sl. s ciljem ostvarenja financijskih prijevarnih radnji, kompromitacije sustava, reputacijske štete i drugih posljedica. Bolnice su također izložene svim navedenim oblicima kibernetičkih prijetnji.

S druge strane UI se koristi i kao alat za otkrivanje prijetnji i povećanje kibernetičke otpornosti. U tim odnosima primjene UI-a prisutan je fenomen asimetrije. Naime napadači jednostavno „putuju brže“ u primjeni tehnoloških rješenja u ostvarenju svojih kriminalnih aktivnosti. Asimetrija zapravo nije novi pojam u kibernetičkoj sigurnosti, a UI je još dodatno povećava.

Pristup poboljšanju otpornosti organizacija se temelji na izgradnji mrežne arhitekture nultog povjerenja (engl. *zero trust*), koja podrazumijeva da se nikome tj. niti jednom digitalnom identitetu, ne vjeruje unaprijed, već se svaki pristup mora kontinuirano provjeravati. Nulto povjerenje u mrežnoj arhitekturi osigurava da sustavi budu otporniji na kibernetičke prijetnje kroz strogu kontrolu i segmentaciju. Ključni element takvog pristupa je identitet u središtu zaštite (engl. *identity first*), što znači da je zaštita korisničkih računa i osjetljivih podataka kojima ti računi mogu pristupati temelj sigurnosne strategije.

Uloga UI-a ključna je u otkrivanju i prevenciji nepoželjnih obrazaca aktivnosti na računalnoj mreži, bilo da se radi o korisnicima ili uređajima, odnosno svim digitalnim identitetima unutar mreže. Takav se nadzor provodi neprekidno, 24 sata dnevno, što značajno nadilazi mogućnosti samog ljudskog angažmana. Zbog toga je UI postala nezaobilazan element suvremenih sigurnosnih sustava.

Zaključak

Digitalna transformacija poslovanja donosi brojne prednosti, ali i izazove povezane s intenzivnim korištenjem digitalnih tehnologija, pri čemu je jedan od ključnih aspekata digitalna sigurnost.

Medicina postaje sve više digitalna i u budućnosti će to biti još izraženije. Prednosti tehnologije u brzom povezivanju i ažuriranju, automatizacija posebno onih ponavljajućih procesa, korištenje suvremenih medicinskih uređaja i opreme, te potencijal korištenja UI-a, podržava suvremenu

medicinu i pomaže liječnicima u svakodnevnom radu. Međutim odgovornost za način korištenja digitalnih asistenata, donošenje odluka o tijeku liječenja i ishode liječenja bolesnika i dalje ostaje na liječnicima.

Unatoč visokoj razini tehnološke razvijenosti i primjeni naprednih rješenja za zaštitu i detekciju prijetnji iz digitalnog prostora, ljudski faktor ostaje presudan u očuvanju podataka. Zato su edukacija i podizanje svijesti zaposlenika o prijetnjama poput primjerice *phishinga* i socijalnog inženjeringa od ključne važnosti za smanjenje rizika i jačanje informacijske otpornosti bolničkih ustanova. Kibernetička sigurnost, kao sastavni dio informacijske sigurnosti, danas je neodvojiva od našeg svakodnevnog života u digitalnom okruženju. Upravo zbog toga ona mora biti temeljni segment poslovanja bolničkih poslovnih sustava.

Važno je istaknuti da je informacijska sigurnost odgovornost svakog pojedinca u organizaciji. Ona mora biti integrirana u korporativno upravljanje i kulturu organizacije, jer nada da se sigurnosni incident neće dogoditi ne predstavlja strategiju u jačanju otpornosti na kibernetičke prijetnje. Ulaganje u informacijsku sigurnost nije trošak, već investicija u zaposlenike, bolesnike te sigurnost i kontinuitet poslovanja bolničkih sustava, kao i u kvalitetno pružanje zdravstvene skrbi.

Literatura

1. Leonhard G. „How The Future works?“ [video na internetu]. Gerd Leonhard, 03.03.2020. [pristupljeno: 02.12.2025.]. Dostupno na: https://www.futuristgerd.com/howthefutureworks/ ?gclid=EAIaIQobChMIj-TRteWG6AIVWfBRCh241QxFEAAYASAAEgL6pfD_BwE.

2. Spremić M. Digitalna transformacija poslovanja. Zagreb, Sveučilište u Zagrebu, Ekonomski fakultet, 2017.

3. Advanced Research Projects Agency Network (ARPANET) [internet]. Dostupno na: https://en.wikipedia.org/wiki/ARPANET. Pristupljeno: 10.12.2025.

4. Smjernice OECD-a za multinacionalna poduzeća o odgovornom poslovnom ponašanju [internet]. Hrvatska nacionalna kontaktna točka, 2023. [pristupljeno: 12.12.2025.]. Dostupno na : https://investcroatia.gov.hr/wp-content/uploads/2023/11/NKT_Smjernice_odgovorno-poslovno-pona%C5%A1anje.

5. Zakon o sustavu unutarnjih kontrola u javnom sektoru. Narodne novine, br. 78/2015 [pristupljeno: 10.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2015_07_78_1492.html

6. Zakon o kibernetičkoj sigurnosti. Narodne novine, br. 14/2024 [pristupljeno: 05.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html

7. Uredba o kibernetičkoj sigurnosti. Narodne novine, br. 135/2024. [pristupljeno: 14.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_135_2217.html

8. Belani H, Fišter K., (2025.), Who should do what to help mitigate cyber threats in health care: narrative review of practical approaches and actionable recommendations. Int. J. Health Gov. 2025 Jun;30(3):282–292.
https://doi.org/10.1108/IJHG-03-2025-0030

9. Huić D, Lovrec P. 60 Godina – Klinički zavod za nuklearnu medicinu i zaštitu od zračenja. Zagreb, Medicinska naklada, 2019.

10. Subbiah V, Kurzrock R. Challenging Standard-of-Care Paradigms in the Precision Oncology Era. Trends Cancer. 2018 Feb;4(2):101-109.
https://doi.org/10.1016/j.trecan.2017.12.004

11. Nacionalna strategija razvoja zdravstva 2012.– 2020. [internet]. Vlada Republike Hrvatske, 2012. [pristupljeno: 25.11.2025.]. Dostupno na: https://zdravlje.gov.hr/UserDocsImages/dokumenti/Programi,%20projekti%20i%20strategije/Skracena%20Nacionalna%20strategija%20razvoja%20zdravstva%20-%20HRV%20-%20za%20web.pdf

12. Nacionalni plan razvoja zdravstva za razdoblje od 2021. do 2027. godine [internet]. Vlada Republike Hrvatske, 2021. [pristupljeno: 02.12.2025.]. Dostupno na: https://zdravlje.gov.hr/UserDocsImages/2022%20Objave/Nacionalni%20plan%20razvoja%20zdravstva%202021.-2027..pdf

13. HL7 International [internet]. HL7 International, 2025. [pristupljeno: 25.11.2025.]. Dostupno na: https://www.hl7.org/index.cfm.

14. Digital Imaging and Communications in Medicine – DICOM [internet]. DICOM® Secretariat, 2025. [pristupljeno: 25.11.2025.]. Dostupno na: https://www.dicomstandard.org/

15. 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 (Opća uredba o zaštiti podataka). Službeni list Europske unije, br. 119/2016 [pristupljeno: 03.12.2025.]. Dostupno na: https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=hr.

16. ISO/IEC 27001 Standard – Information Security Management Systems [internet]. International Organization for Standardization, 2022. [pristupljeno: 03.12.2025.]. Dostupno na: https://www.iso.org/standard/27001

17. What Is the CIA Triad? [internet]. Fortinet, Inc., 2025. [pristupljeno: 03.12.2025.]. Dostupno na: https://www.fortinet.com/resources/cyberglossary/cia-triad

18. Pravilnik o načinu obrade zdravstvenih i drugih osobnih podataka u zdravstvenim nacionalnim i institucionalnim informacijskim sustavima u zdravstvu. Narodne novine, br. 150/2024. [pristupljeno: 13.12.2025.]. Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/full/2024_12_150_2465.html

19. Prioritetne preporuke za zaštitu od kibernetičkih napada [internet]. Nacionalni centar za kibernetičku sigurnost - NCSC HR, 2025. [pristupljeno: 08.10.2025.]. Dostupno na: https://ncsc.hr/UserDocsImages/ostalo/Prioritetne_preporuke_za_zastitu_od_kibernetickih_napada.pdf?vel=677572

20. Godišnji izvještaj Nacionalnog CERT a za 2024. godinu [internet]. Nacionalni CERT - CERT.hr, 2025. [pristupljeno: 28.11.2025.]. Dostupno na: https://www.cert.hr/godisnji-izvjestaj-rada-nacionalnog-cert-a-za-2024-godinu/

Bilt. Hrvat. druš. med. inform. 2025:31(1-2)
PROFESSIONAL ARTICLE

Digital Transformation and Information Security Challenges in Hospital Operations

Dražen Milković[1]
[1] University Hospital Centre Zagreb, Zagreb, Croatia
E-mail: drazen.milkovic@kbc-zagreb.hr

https://doi.org/10.69827/bhdmi-39976

Abstract: The challenges of increased demand for various specialist medical services, as well as the growing complexity of medical operations, can be mitigated through the automation and integration of business processes and the application of new innovative solutions. The intensive use of numerous information technologies, along with increasing connectivity and mobility, exposes hospital operations to risks arising from the digital environment, while simultaneously setting new requirements regarding security and business continuity. The digital footprint of each individual is also expanding, making them more vulnerable to information security threats, which we are often not sufficiently aware of. Agile improvement of business processes in medical practice, supported by advanced information technology solutions, is becoming a necessity in today's era of digital business transformation. In providing healthcare to patients, large amounts of medical data are created, collected, and processed, which must be appropriately protected from unauthorized use. The aim of this consideration is to provide insight into how technological progress affects changes in hospital operations and the provision of healthcare to patients. The intensive use of digital technologies is inevitably linked to risks that arise from the digital environment in which everything is interconnected. In the digital environment, changes are becoming faster and more visible, from the digital tools available to us, the opportunities they provide and the challenges of digital security they bring. For all these reasons, the management of healthcare institutions faces new challenges that must be addressed through responsible governance, so that organizations can safely achieve their goals in the context of digital transformation and information security.

Keywords: digital transformation; information security; cybersecurity; corporate governance; business processes; artificial intelligence.