

# Pametni medicinski uređaji i tehnologija interneta stvari: budućnost praćenja zdravstvenih podataka pacijenata

Valentina Ješić<sup>1,2</sup>, Lucija Piškorić<sup>3</sup>

<sup>1</sup>Fakulteta za zdravstvene vede Univerze v Novem mestu, Novo mesto, Slovenija

<sup>2</sup>Klinički bolnički centar Sestre milosrdnice, Zagreb, Hrvatska

<sup>3</sup>Opća bolnica „Dr. Ivo Pedišić“, Sisak, Hrvatska

E-pošta: [valentina.matic@yahoo.com](mailto:valentina.matic@yahoo.com); [orcid.org/0000-0001-7947-5233](https://orcid.org/0000-0001-7947-5233)

<https://doi.org/10.69827/bhdmi-34634>

Sažetak: Digitalna transformacija zdravstvenog sustava omogućila je razvoj i primjenu Interneta stvari (IoT), koji povezuje pametne medicinske uređaje i senzore u mreže za prikupljanje, prijenos i analizu zdravstvenih podataka. IoT doprinosi kontinuiranom praćenju pacijenata, personalizaciji skrbi i optimizaciji resursa, uz smanjenje troškova. Ključni izazovi ostaju sigurnost podataka, zaštita privatnosti i interoperabilnost sustava. Proveden je sustavni pregled znanstvene literature u bazama *PubMed*, *Scopus* i *ScienceDirect* za razdoblje 2017. - 2024. godine. Primijenjeni su pojmovi *Internet of Things*, *smart medical devices*, *health data*, *data security*, *interoperability*, *telemedicine*. U analizu je uključeno 22 recenzirana rada, kategorizirana prema temama: a) primjena IoT-uređaja (11 radova), b) sigurnost i privatnost podataka (8 radova), c) interoperabilnost i tehnički izazovi (3 rada). Dodatno su konzultirani relevantni tehnički i regulatorni dokumenti (HL7, FHIR, GDPR). IoT-uređaji omogućuju praćenje vitalnih funkcija u stvarnom vremenu, poboljšavaju upravljanje kroničnim bolestima i smanjuju broj hospitalizacija. Primjeri uključuju senzore za glukozu, pametne narukvice i sustave za daljinsku skrb. Glavne prepreke su fragmentacija sustava, nedostatak standardizacije i kibernetički rizici. Primjena standarda poput HL7 i FHIR te naprednih sigurnosnih protokola povećava interoperabilnost i sigurnost podataka. Tehnologija IoT ima velik potencijal za modernizaciju zdravstvene skrbi, ali njezina puna primjena zahtijeva rješavanje sigurnosnih i tehničkih izazova. Ključni čimbenici su edukacija zdravstvenih djelatnika, regulatorna usklađenost i suradnja svih dionika. Integracija standardiziranih i sigurnih rješenja omogućit će učinkovitiji, dostupniji i kvalitetniji zdravstveni sustav.

*Ključne riječi:* internet stvari; pametni medicinski uređaji; zdravstveni podaci; sigurnost podataka; interoperabilnost; telemedicina.

## Uvod

Digitalna transformacija zdravstvenog sustava otvorila je prostor za primjenu naprednih tehnologija koje uvelike mijenjaju način pružanja i praćenja zdravstvene skrbi. Među najznačajnijim inovacijama ističe se Internet stvari (IoT), mreža pametnih uređaja i senzora koja omogućuje prikupljanje, prijenos i analizu zdravstvenih podataka u stvarnom vremenu. Takav sustav stvara most između pacijenata i zdravstvenih djelatnika jer omogućuje stalan pristup ključnim informacijama o zdravstvenom stanju, neovisno o lokaciji.

Temelj IoT-a je povezivanje uređaja putem interneta, čime se podaci kontinuirano prikupljaju, obrađuju i analiziraju radi donošenja pravovremenih i utemeljenih odluka. U kliničkom okruženju pametni medicinski uređaji, poput nosivih senzora, sustava za daljinski nadzor i automatiziranih bolničkih monitora, sve se češće koriste u svakodnevnoj praksi. Njihova je uloga višestruka jer obuhvaća praćenje vitalnih funkcija pacijenata, ranu detekciju zdravstvenih poteškoća, prilagodbu liječenja i prevenciju komplikacija.

Primjeri uključuju pametne satove koji prate otkucaje srca, tjelesnu aktivnost i razinu kisika u krvi, senzore za kontinuirano praćenje glukoze kod oboljelih od dijabetesa te integrirane sustave u bolničkim sobama koji omogućuju automatski nadzor vitalnih funkcija. Takvi uređaji zdravstvenim djelatnicima pružaju mogućnost brze reakcije na promjene u zdravstvenom stanju, a pacijentima daju veću autonomiju i osjećaj sigurnosti u svakodnevnom životu.

Unatoč brojnim prednostima, primjena IoT-a u zdravstvu suočava se i s izazovima. Najznačajniji su sigurnost i zaštita privatnosti podataka jer se osjetljive informacije prenose i pohranjuju putem digitalnih mreža. Osim toga, interoperabilnost, odnosno povezivanje različitih uređaja i sustava, često predstavlja prepreku učinkovitim uvođenju i širem prihvaćanju tehnologija IoT u zdravstvenom sustavu.

## Metodologija

Analiza se temelji na sustavnom pregledu znanstvene literature s ciljem razumijevanja primjene tehnologije IoT u zdravstvenom sustavu te identificiranja izazova vezanih za sigurnost podataka i interoperabilnost. Pretraživanje je provedeno u bazama *PubMed*, *Scopus* i *ScienceDirect* u razdoblju od 2017. do 2024. godine.

Korišteni su sljedeći ključni pojmovi: internet stvari, pametni medicinski uređaji, zdravstveni podaci, sigurnost podataka, interoperabilnost, telemedicina (i njihovi engleski ekvivalenti: *Internet of Things*, *smart medical devices*, *health data*, *data security*, *interoperability*, *telemedicine*).

Primjer pretraživačkog niza: (*Scopus/Title-Abs-Key*): (*"Internet of Things" OR IoT*) AND (*"healthcare" OR "medical"*) AND (*"smart device" OR wearable OR "remote patient monitoring"*) AND (*"data security" OR privacy OR interoperability*).

Kriteriji uključivanja obuhvaćali su:

- radove objavljene u razdoblju 2017. - 2024.,
- recenzirane znanstvene članke na engleskom ili hrvatskom jeziku,
- fokus na primjenu tehnologija IoT u zdravstvenom sustavu.

Isključeni su radovi izvan zdravstvene domene, radovi bez empirijskih podataka ili oni koji nisu recenzirani.

U analizu su uključena 22 recenzirana znanstvena rada, kategorizirana kako slijedi:

- a) primjena IoT-uređaja – 11 radova,
- b) sigurnost i privatnost podataka – 8 radova,
- c) interoperabilnost i tehnički izazovi – 3 rada.

Dodatno su konzultirani relevantni tehnički i regulatorni dokumenti (npr. HL7, FHIR, GDPR) koji pružaju kontekst za razumijevanje standardizacije i zaštite podataka u digitalnom zdravstvu.

## Rezultati i rasprava

### 3.1. *Primjena IoT-a u zdravstvenoj skrbi*

IoT-uređaji omogućuju prikupljanje zdravstvenih podataka u realnom vremenu, što značajno povećava učinkovitost i kvalitetu pružanja zdravstvene skrbi. Njihova primjena obuhvaća različite aspekte zdravstva, od praćenja vitalnih funkcija do daljinske zdravstvene skrbi, čime se postiže bolja personalizacija tretmana i optimizacija resursa (1,2). Nosivi uređaji, poput pametnih satova, narukvica i drugih senzora, omogućuju kontinuirano praćenje ključnih parametara poput otkucaja srca, tjelesne temperature, razine kisika u krvi i fizičke aktivnosti (3). Takvi uređaji posebno su korisni pacijentima s kroničnim bolestima, poput hipertenzije ili srčanih problema, jer im omogućuju praćenje vlastitog stanja u stvarnom vremenu čime se smanjuje potreba za čestim liječničkim pregledima i omogućuje rano prepoznavanje promjena koje zahtijevaju medicinsku intervenciju.

Jedan od ključnih primjera su senzori za glukozu koji omogućuju kontinuirani monitoring šećera u krvi kod dijabetičara. Navedeni uređaji automatski prikupljaju podatke i šalju ih liječnicima putem povezanih sustava ili mobilnih aplikacija (4). Pristup omogućuje brze intervencije u slučaju abnormalnosti, smanjuje rizik od ozbiljnih komplikacija i olakšava pacijentima svakodnevno upravljanje njihovom bolešću. Osim toga, tehnologija pruža korisnicima veću slobodu u obavljanju svakodnevnih aktivnosti, uz osjećaj sigurnosti da se njihovo stanje prati u svakom trenutku.

U bolničkom okruženju, primjena IoT-uređaja dovodi do stvaranja pametnih bolničkih soba koje omogućuju neprekidan nadzor pacijenata. Sustavi opremljeni sensorima automatski bilježe vitalne funkcije poput tlaka, disanja i temperature te šalju obavijesti medicinskom osoblju u slučaju pogoršanja zdravstvenog stanja (2,5). Time se smanjuje potreba za stalnim fizičkim nadzorom pacijenata, što osoblju omogućuje učinkovitije raspoređivanje resursa i vremena (6). Istovremeno se povećava sigurnost pacijenata, jer su sustavi programirani tako da odmah alarmiraju u slučaju promjene stanja.

Telemedicina i tzv. daljinsko praćenje pacijenata predstavljaju još jedan značajan napredak zahvaljujući tehnologiji IoT (7). Pametni uređaji omogućuju liječnicima da prate zdravstveno stanje pacijenata izvan bolničkog okruženja, neovisno o tome je li riječ o kućnoj njezi starijih osoba, pacijentima u rehabilitaciji ili osobama s kroničnim bolestima (8). Na ovaj način smanjuje se opterećenje bolničkih kapaciteta, a pacijentima se omogućuje pristup zdravstvenoj skrbi iz udobnosti vlastitog doma. Liječnici mogu donositi odluke temeljene na podacima koji se prikupljaju u stvarnom vremenu, čime se osigurava pravovremena i adekvatna intervencija (9).

Sustavi za praćenje starijih osoba dodatno osnažuju primjenu IoT-a u zdravstvenoj skrbi. Senzori za detekciju pada, pametne narukvice ili uređaji za praćenje dnevnih aktivnosti omogućuju neprekidnu brigu o starijim osobama u njihovim domovima, čime se povećava njihova sigurnost i smanjuje potreba za stalnim nadzorom skrbnika (10). Primjerice, u slučaju pada, uređaji mogu automatski obavijestiti obitelj ili hitne službe, omogućujući brzu intervenciju što pridonosi očuvanju autonomije starijih osoba dok istovremeno smanjuju pritisak na zdravstveni sustav.

Tehnologije IoT također igraju ključnu ulogu u prevenciji epidemija. Tijekom pandemije COVID-19, pametni uređaji omogućili su prikupljanje i analizu podataka o simptomima u stvarnom vremenu, što je pomoglo u ranom otkrivanju žarišta i pravovremenim mjerama prevencije (11). Na primjer, pametni termometri i uređaji za praćenje razine kisika u krvi koristili su se za identifikaciju i praćenje zaraženih osoba, dok su sustavi za praćenje kontakata omogućili učinkovitije suzbijanje širenja zaraze. Osim toga, pametni inhalatori za astmu, koji bilježe upotrebu i simptome, omogućuju pacijentima bolje upravljanje njihovim stanjem te pružaju zdravstvenim djelatnicima detaljne podatke za prilagodbu terapije.

Jedan od novih uređaja koji donosi dodatnu vrijednost u navedenoj domeni je prsten *Evie* (slika 1), pametni nosivi uređaj koji korisnicima pruža podršku u boljem razumijevanju simptoma i pripremi za konzultacije s liječnikom, bez pružanja izravnih dijagnostičkih usluga. Posebno je prilagođen privatnosti korisnika, primjenjujući standardnu enkripciju podataka i osiguravajući periodično brisanje spremljenih informacija. Prsten *Evie* time ne prati samo ključne parametre zdravlja, već i nudi dodatnu sigurnost u zaštiti privatnih podataka. Beta-verzija uređaja dostupna je korisnicima od 8. siječnja 2025., i to bez dodatnih troškova, čime se olakšava njegova šira primjena među pacijentima (12).

IoT-uređaji imaju značajan potencijal za smanjenje ugljičnog otiska u zdravstvenom sustavu. Daljinsko praćenje pacijenata putem nosivih uređaja smanjuje potrebu za čestim fizičkim dolascima u bolnice i ambulante, čime se smanjuje emisija ugljičnog dioksida povezana s transportom. Na primjer, pacijenti s kroničnim bolestima, poput dijabetesa ili hipertenzije, mogu redovito slati podatke liječnicima putem IoT platformi, umjesto da često posjećuju zdravstvene ustanove. Osim toga, optimizacija resursa i smanjenje nepotrebnih bolničkih prijema također pridonose energetskej učinkovitosti i smanjenju otpada u zdravstvenom sustavu.



Slika 1. Pametni prsten *Evie Ring* predstavljen na CES 2025.

Prenešeno s: Movano Evie Ring AI Chatbot CES Health Tech Wearables [Internet]. The Verge; 2025 Jan 7 [pristupljeno 10.01.2025.]. Dostupno na: <https://www.theverge.com/2025/1/7/24337403/movano-evie-ring-ai-chatbot-ces-health-tech-wearables>.

Razvoj održivih IoT-uređaja dodatno pojačava njihov doprinos očuvanju okoliša. Proizvođači sve češće uvode uređaje s punjivim baterijama koje smanjuju potrebu za jednokratnim baterijama, što dugoročno smanjuje količinu elektroničkog otpada. Također, korištenje ekološki prihvatljivih materijala, poput reciklirane plastike ili biorazgradivih komponenti, doprinosi smanjenju negativnog utjecaja na okoliš tijekom proizvodnje i odlaganja uređaja. Uz održivi dizajn, IoT-uređaji mogu postati ključni alat ne samo za poboljšanje zdravstvene skrbi, već i za promicanje ekološke odgovornosti u medicinskom sektoru.

Sve navedene primjene tehnologije IoT ne samo poboljšavaju kvalitetu i dostupnost zdravstvene skrbi, već i dovode do značajnog smanjenja troškova. Optimizacija resursa, smanjenje potreba za nepotrebnim bolničkim prijemima i brže donošenje odluka omogućuju učinkovitije funkcioniranje zdravstvenog sustava (13). Istovremeno se podiže razina personalizirane skrbi jer se prikupljeni podaci analiziraju i prilagođavaju individualnim potrebama svakog pacijenta. Ova tehnologija stoga predstavlja ključnu komponentu modernizacije zdravstvenih usluga u budućnosti.

### *Sigurnost podataka i privatnost pacijenata*

Jedan od najvećih izazova primjene tehnologije IoT u zdravstvu je osiguranje sigurnosti podataka i zaštita privatnosti pacijenata. IoT-uređaji svakodnevno prikupljaju velike količine osjetljivih zdravstvenih informacija, koje su posebno podložne rizicima u digitalnom okruženju (13). Nedovoljno osigurani sustavi često postaju meta kibernetičkih napada, što može dovesti do neovlaštenog pristupa, krađe ili zloupotrebe podataka. Takvi incidenti ugrožavaju povjerenje pacijenata i smanjuju učinkovitost implementacije pametnih uređaja u zdravstvenu praksu.

Usklađenost s regulatornim okvirom predstavlja dodatni izazov, jer zakonodavstvo poput Opće uredbe o zaštiti podataka (GDPR, engl. *General Data Protection Regulation*) u Europskoj uniji nameće stroge standarde u vezi s prikupljanjem, pohranom i prijenosom zdravstvenih informacija (14). Organizacije moraju osigurati da se svi podaci prikupljaju uz izričitu privolu pacijenata, dok se prijenos mora odvijati uz primjenu sigurnih metoda kako bi se izbjeglo curenje ili neovlaštena distribucija informacija.

U tom kontekstu, šifriranje i anonimizacija podataka igraju ključnu ulogu u zaštiti privatnosti pacijenata. Napredne metode šifriranja osiguravaju da su podaci zaštićeni tijekom prijenosa i pohrane, dok anonimizacija omogućuje da se identitet pacijenta ne može povezati s prikupljenim informacijama, čak i u slučaju eventualnih sigurnosnih propusta (15,16). Takvi pristupi smanjuju rizik od zloupotrebe podataka i istovremeno osiguravaju da se informacije mogu koristiti za daljnju analizu i istraživanja.

Kako bi se povećala sigurnost IoT-sustava u zdravstvu, nužna je implementacija strožih sigurnosnih protokola. To uključuje primjenu višefaktorske autentifikacije, koja dodatno potvrđuje identitet korisnika prije pristupa podacima, i redovito ažuriranje softvera kako bi se osigurala otpornost na nove vrste kibernetičkih prijetnji (17). Također, organizacije bi trebale razvijati sustave koji omogućuju praćenje aktivnosti na mreži i brzo otkrivanje potencijalnih prijetnji, čime bi se osigurala pravovremena reakcija u slučaju pokušaja napada.

Uz tehnička rješenja, od ključne je važnosti podizanje svijesti i edukacija zdravstvenih djelatnika o važnosti sigurnosti podataka. Redovita obuka osoblja može značajno smanjiti rizik od ljudskih pogrešaka koje često predstavljaju najslabiju kariku u sigurnosnom lancu (18). Kombinacija tehnoloških inovacija, regulatornih okvira i edukacije ključna je za stvaranje sigurnog okruženja u

kojem IoT-uređaji mogu funkcionirati na način koji štiti privatnost pacijenata i povećava povjerenje u digitalnu transformaciju zdravstva.

### *Izazovi interoperabilnosti i integracije sustava*

Interoperabilnost predstavlja jedan od ključnih izazova koji koče širu primjenu tehnologije IoT u zdravstvenom sustavu. Problem proizlazi iz neusklađenosti između različitih uređaja i sustava, što otežava međusobnu povezanost, razmjenu i analizu podataka prikupljenih putem tehnologija IoT (19). Glavni problemi povezani s interoperabilnošću uključuju nedostatak standardizacije i poteškoće u integraciji IoT-uređaja s postojećim sustavima elektroničkih zdravstvenih zapisa (EZZ) (20).

Nedostatak standardizacije jedan je od temeljnih izazova, jer različiti proizvođači pametnih medicinskih uređaja koriste različite protokole za prijenos podataka. Takva fragmentacija sustava otežava komunikaciju između uređaja i infrastrukture, čime se smanjuje učinkovitost razmjene podataka (21). IoT-uređaji prikupljaju zdravstvene informacije u stvarnom vremenu, no ako ti podaci nisu kompatibilni sa sustavima u kojima se pohranjuju ili analiziraju, njihov puni potencijal ostaje neiskorišten. Standardizacija prijenosnih protokola i komunikacijskih formata neophodna je kako bi se postigla bolja povezanost između različitih IoT-uređaja i softverskih rješenja.

Integracija tehnologija IoT sa sustavima elektroničkih zdravstvenih zapisa (EZZ) još je jedan značajan izazov. IoT-uređaji generiraju velike količine podataka koje je potrebno automatski prenositi i pohranjivati u centralizirane sustave poput EZZ-a (22). Trenutni sustavi često nemaju jedinstvena sučelja koja omogućuju neometan prijenos podataka iz IoT-uređaja, što dovodi do nepotrebnih administrativnih opterećenja i potencijalnih pogrešaka u unosu podataka. Rješenje problema leži u razvoju prilagodljivih sučelja koja mogu komunicirati s različitim uređajima i omogućiti učinkovitu sinkronizaciju podataka između IoT-sustava i EZZ-a.

Primjena standarda kao što su HL7 (*Health Level Seven*) i FHIR (*Fast Healthcare Interoperability Resources*) ključna je za unapređenje interoperabilnosti u zdravstvu. HL7 i FHIR omogućuju strukturiranu i standardiziranu razmjenu zdravstvenih podataka između različitih sustava, čime se osigurava njihova kompatibilnost i bolja dostupnost (23). Implementacija tih standarda može značajno poboljšati komunikaciju između IoT-uređaja, bolničkih informacijskih sustava i elektroničkih zdravstvenih zapisa, omogućujući precizniju i bržu obradu podataka.

Konačno, za postizanje potpune interoperabilnosti potrebno je uključiti suradnju između proizvođača medicinskih uređaja, programera softverskih rješenja i zdravstvenih institucija. Razvoj zajedničkih tehnoloških standarda i otvorenih platformi omogućit će povezivanje različitih IoT-sustava i njihovu integraciju u postojeće zdravstvene infrastrukture. Spomenuti pristup unaprijedit će razmjenu podataka, smanjiti administrativno opterećenje i osigurati da zdravstvene informacije prikupljene putem IoT-uređaja budu dostupne i korisne u svakodnevnoj kliničkoj praksi.

## **Zaključak**

Tehnologija IoT donosi značajne prednosti u zdravstvenom sustavu, uključujući kontinuirano praćenje pacijenata, personalizaciju liječenja i optimizaciju resursa. Nosivi uređaji, senzori i pametni sustavi omogućuju bolje upravljanje kroničnim bolestima, prevenciju komplikacija i smanjenje troškova skrbi, dok zdravstvenim djelatnicima pružaju pravovremene informacije za donošenje odluka. Međutim, izazovi poput sigurnosti podataka, zaštite privatnosti i interoperabilnosti sustava moraju se riješiti

kroz napredna sigurnosna rješenja, primjenu standarda poput HL7 i FHIR te usklađenost s regulativama poput GDPR-a.

Buduća istraživanja trebaju se usmjeriti na poboljšanje integracije IoT-a s postojećim sustavima i osiguranje sigurnosti podataka. Uz ulaganje u edukaciju zdravstvenih djelatnika i pacijenata, kao i suradnju između proizvođača tehnologije, regulatornih tijela i zdravstvenih ustanova, moguće je prevladati postojeće izazove. Takva sinergija ključna je za razvoj standardiziranih, interoperabilnih i sigurnih rješenja koja će omogućiti modernizaciju zdravstvenih sustava te unaprijediti učinkovitost, dostupnost i kvalitetu zdravstvene skrbi na globalnoj razini.

## Literatura

1. Osama M, Ateya AA, Sayed MS, Hammad M, Pławiak P, Abd El-Latif AA, et al. Internet of Medical Things and Healthcare 4.0: Trends, Requirements, Challenges, and Research Directions. *Sensors* (Basel). 2023 Aug 25;23(17):7435.  
<https://doi.org/10.3390/s23177435>
2. Abdulmalek S, Nasir A, Jabbar WA, Almuahaya MAM, Bairagi AK, Khan MAM, et al. IoT-Based Healthcare-Monitoring System towards Improving Quality of Life: A Review. *Healthcare* (Basel). 2022 Oct 11;10(10):1993.  
<https://doi.org/10.3390/healthcare10101993>
3. Hughes A, Shandhi MMH, Master H, Dunn J, Brittain E. Wearable Devices in Cardiovascular Medicine. *Circ Res*. 2023 Mar 3;132(5):652-70.  
<https://doi.org/10.1161/CIRCRESAHA.122.322389>
4. Cappon G, Vettoretti M, Sparacino G, Facchinetti A. Continuous Glucose Monitoring Sensors for Diabetes Management: A Review of Technologies and Applications. *Diabetes Metab J*. 2019 Aug;43(4):383-97.  
<https://doi.org/10.4093/dmj.2019.0121>
5. Boikanyo K, Zungeru AM, Sigweni B, Yahya A, Lebekwe C. Remote patient monitoring systems: Applications, architecture, and challenges. *Scientific African*. 2023 July;20:e01638.  
<https://doi.org/10.1016/j.sciaf.2023.e01638>
6. Javaid M, Khan IH. Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. *J Oral Biol Craniofac Res*. 2021;11(2):209-14.  
<https://doi.org/10.1016/j.jobcr.2021.01.015>
7. Gajarawala SN, Pelkowski JN. Telehealth Benefits and Barriers. *J Nurse Pract*. 2021 Feb;17(2):218-21.  
<https://doi.org/10.1016/j.nurpra.2020.09.013>
8. Majumder S, Aghayi E, Noferesti M, Memarzadeh-Tehran H, Mondal T, Pang Z, et al. Smart Homes for Elderly Healthcare-Recent Advances and Research Challenges. *Sensors* (Basel). 2017 Oct 31;17(11):2496.  
<https://doi.org/10.3390/s17112496>
9. Selvaraj S. Utilizing Artificial Intelligence for Patient Risk Predictions: Empowering Doctors with Data - Driven Insights. *IJSR*. 2024 July 5;13(7):371-6.  
<https://doi.org/10.21275/SR24707023233>
10. Vrančić A, Zdravec H, Orehovački T. The Role of Smart Homes in Providing Care for Older Adults: A Systematic Literature Review from 2010 to 2023. *Smart Cities*. 2024 June 26;7(4):1502-50.  
<https://doi.org/10.3390/smartcities7040062>

11. Castiglione A, Umer M, Sadiq S, Obaidat MS, Vijayakumar P. The Role of Internet of Things to Control the Outbreak of COVID-19 Pandemic. *IEEE Internet Things J.* 2021 Nov;8(21):16072-82. <https://doi.org/10.1109/JIOT.2021.3070306>
12. Movano Evie Ring AI Chatbot CES Health Tech Wearables [Internet]. *The Verge*; 2025 Jan 7 [pristupljeno: 10.01.2025.]. Dostupno na: <https://www.theverge.com/2025/1/7/24337403/movano-evie-ring-ai-chatbot-ces-health-tech-wearables>.
13. Al Khatib I, Shamayleh A, Ndiaye M. Healthcare and the Internet of Medical Things: Applications, Trends, Key Challenges, and Proposed Resolutions. *Informatics.* 2024 July 16;11(3):47. <https://doi.org/10.3390/informatics11030047>
14. Bennett CJ. The European General Data Protection Regulation: An instrument for the globalization of privacy standards? Chun SA, Adam NR, Noveck B, editors. *IP.* 2018 June 29;23(2):239-46. <https://doi.org/10.3233/IP-180002>
15. Kruse CS, Smith B, Vanderlinden H, Nealand A. Security Techniques for the Electronic Health Records. *J Med Syst.* 2017 Aug;41(8):127. <https://doi.org/10.1007/s10916-017-0778-4>
16. Shojaei P, Vlahu-Gjorgievska E, Chow YW. Security and Privacy of Technologies in Health Information Systems: A Systematic Literature Review. *Computers.* 2024 Jan 31;13(2):41. <https://doi.org/10.3390/computers13020041>
17. Zakerabasali S, Ayyoubzadeh SM. Internet of Things and healthcare system: A systematic review of ethical issues. *Health Sci Rep.* 2022 Nov;5(6):e863. <https://doi.org/10.1002/hsr2.863>
18. Burke W, Stranieri A, Oseni T, Gondal I. The need for cybersecurity self-evaluation in healthcare. *BMC Med Inform Decis Mak.* 2024 May 23;24(1):133. <https://doi.org/10.1186/s12911-024-02551-x>
19. Torab-Miandoab A, Samad-Soltani T, Jodati A, Rezaei-Hachesu P. Interoperability of heterogeneous health information systems: a systematic literature review. *BMC Med Inform Decis Mak.* 2023 Jan 24;23(1):18. <https://doi.org/10.1186/s12911-023-02115-5>
20. Geneva Tamunobarafiri Igwama, Janet Aderonke Olaboye, Chukwudi Cosmos Maha, Mojeed Dayo Ajegbile, Samira Abdul. Integrating electronic health records systems across borders: Technical challenges and policy solutions. *imsrj.* 2024 July 26;4(7):788-96. <https://doi.org/10.51594/imsrj.v4i7.1357>
21. Renukappa S, Mudiya P, Suresh S, Abdalla W, Subbarao C. Evaluation of challenges for adoption of smart healthcare strategies. *Smart Health.* 2022 Dec;26:100330. <https://doi.org/10.1016/j.smhl.2022.100330>
22. Alam S, Bhatia S, Shuaib M, Khubrani MM, Alfayez F, Malibari AA, et al. An Overview of Blockchain and IoT Integration for Secure and Reliable Health Records Monitoring. *Sustainability.* 2023 Mar 23;15(7):5660. <https://doi.org/10.3390/su15075660>
23. Ayaz M, Pasha MF, Alzahrani MY, Budiarto R, Stiawan D. The Fast Health Interoperability Resources (FHIR) Standard: Systematic Literature Review of Implementations, Applications, Challenges and Opportunities. *JMIR Med Inform.* 2021 July 30;9(7):e21929. <https://doi.org/10.2196/21929>

# Medical Devices and Internet of Things: The Future of Patient Health Data Monitoring

Valentina Ješić<sup>1,2</sup>, Lucija Piškorić<sup>3</sup>

<sup>1</sup>University of Novo mesto Faculty of Health Sciences School of Medicine, Novo mesto, Slovenia

<sup>2</sup>Sestre milosrdnice University Hospital Center, Zagreb, Croatia

<sup>3</sup>“Dr. Ivo Pedišić“ Sisak General Hospital, Sisak, Croatia

E-mail: [valentina.matic@yahoo.com](mailto:valentina.matic@yahoo.com); [orcid.org/0000-0001-7947-5233](https://orcid.org/0000-0001-7947-5233)

<https://doi.org/10.69827/bhdmi-34364>

**Abstract:** The digital transformation of healthcare has enabled the development and application of the Internet of Things (IoT), which connects smart medical devices and sensors into networks for collecting, transmitting, and analyzing health data. IoT supports continuous patient monitoring, personalized care, and resource optimization while reducing costs. However, data security, privacy, and interoperability remain key challenges. A systematic literature review was conducted in PubMed, Scopus, and ScienceDirect databases covering the period 2017–2024. Search terms included Internet of Things, smart medical devices, health data, data security, interoperability, telemedicine. A total of 22 peer-reviewed papers were analyzed, categorized into: a) IoT device applications (11 studies), b) data security and privacy (8 studies), and c) interoperability and technical challenges (3 studies). Relevant technical and regulatory documents (HL7, FHIR, GDPR) were also consulted. IoT devices enable real-time monitoring of vital functions, improve chronic disease management, and reduce hospital admissions. Examples include glucose sensors, smart bracelets, and remote monitoring systems. Major challenges include system fragmentation, lack of standardization, and cybersecurity risks. The adoption of standards such as HL7 and FHIR and advanced security protocols enhances interoperability and data protection. IoT technology holds great potential for modernizing healthcare, but its full implementation requires overcoming security and technical barriers. Key enablers include healthcare professional education, regulatory compliance, and stakeholder collaboration. The integration of standardized and secure solutions will improve healthcare system efficiency, accessibility, and quality.

**Keywords:** *Internet of Things; smart medical devices; health data; data security; interoperability; telemedicine.*