

NADZOR NAD OBDELAVO ZDRAVSTVENIH PODATKOV

Povzetek

Digitalizacija v zdravstvu prinaša številne prednosti, a hkrati povečuje tveganja v zvezi z varnostjo in zagotavljanjem zasebnosti osebnih podatkov. V tem kontekstu je vzpostavitev ustrezne revizijske sledi ključen element nadzora nad obdelavo podatkov, saj zagotavlja sledljivost obdelave osebnih in zdravstvenih podatkov. Prispevek prikaže strukturo in delovanje revizijskih sledi v nacionalnem zdravstvenem informacijskem sistemu eZdravje, s poudarkom na informacijski rešitvi ATNA.

Ključne besede: *zavarovanje osebnih podatkov, revizijska sled, ATNA, informacijske rešitve, eZdravje*

OVERSIGHT OF HEALTH DATA PROCESSING

Abstract

The digitalization of healthcare brings numerous advantages but also increases the risks associated with the security and protection of personal data. In this context, the establishment of an adequate audit trail is a key element of data processing oversight, as it ensures the traceability of the processing of personal and health-related data. This paper presents the structure and functioning of audit trails within the national electronic health information system eZdravje, with a particular focus on the ATNA-based information solution.

Keywords: *personal data protection, audit trail, ATNA, information solutions, eHealth*

1 UVOD

Digitalna obdelava podatkov je že nekaj časa ključna za učinkovito in kakovostno izvajanje zdravstvene oskrbe (NIJZ, 2024a) V Sloveniji osrednje vozlišče informacijskih rešitev v zdravstvu predstavlja nacionalni sistem eZdravje, ki vključuje Centralni register podatkov o pacientih (CRPP), rešitev eNaročanje za elektronsko napotovanje in naročanje na specialistično raven, eRecept za elektronsko predpisovanje receptov, spletni portal za paciente zVEM in druge. Možnost učinkovite obdelave zdravstvenih podatkov na daljavo prinaša tudi nekatere pasti in tveganja, zato je ključna potreba po učinkovitem nadzoru nad tem, kaj se s podatki dogaja (Drev idr., 2023).

Celovit nadzor nad obdelavo osebnih podatkov v zdravstvu tako ni zgolj dobra usmeritev, ki jo narekujejo številne mednarodne smernice, ampak formalna zakonska obveza (Drev idr., 2022). Ta se v različnih oblikah kaže v Zakonu o varstvu osebnih podatkov (ZVOP-2) (2022), Splošni uredbi o varstvu podatkov (GDPR) (2016), Direktivi NIS2 (2022), Zakonu o informacijski varnosti (ZInfV-1) (2025), Zakonu o kritični infrastrukturi (ZKI) (2024) ter Uredbi o zdravstvenem podatkovnem prostoru (EHDS) (2025). Vsi našteti predpisi poudarjajo pomen zagotavljanja celovitosti (integritete) podatkov, kar pomeni, da morajo posamezne institucije zagotoviti tehnične in organizacijske ukrepe za zagotavljanje nadzora nad tem, kaj se s podatki dogaja (Drev idr., 2023). Zapisano drugače: vsaka zdravstvena institucija mora vedeti kdo, kdaj in za kakšen namen obdeluje podatke o njihovih pacientih. Odgovor na ta izziv predstavljajo revizijske sledi, ki omogočajo retrospektivne vpogled v obdelavo podatkov.

Rešitve eZdravja imajo vzpostavljene ločene revizijske sledi na ravni strežnikov in na ravni aplikacij. Najpomembnejša je centralna rešitev ATNA (Audit Trail and Node Authentication), ki omogoča celovito beleženje obdelave zdravstvenih podatkov v CRPP in s povezanimi rešitvami, kot so zVEM, eNaročanje in (v procesu integracije) eRecept (NIJZ, 2016). ATNA posredno omogoča tudi ugotavljanje, kateri izvajalec zdravstvene dejavnosti (IZD) je dostopal do katerih podatkov

v CRPP. Ne omogoča pa – razlog ni primarno tehnični, ampak organizacijski in pravni – nadzora znotraj lokalnih informacijskih sistemov IZD. Te morajo IZD ustrezno nadzirati sami.

V nadaljevanju bo predstavljena rešitev ATNA kot ključen element za zagotavljanje sledljivosti pri obdelavi zdravstvenih podatkov. Prikazani bodo zakonodajni okviri, tehnična zasnova rešitve in vpliv na širši kontekst informacijske varnosti in vzpostavitve zaupanja v zdravstvene informacijske storitve.

2 METODE

Vsebina prispevka je utemeljena z uporabo analize virov in analize regulatornih vsebin (GDPR, ZVOP-2, NIS2, ZInfV, ZKI, EHDS), tehničnih dokumentov (specifikacije in navodila za posamezne rešitve eZdravja, ATNA, ISO/IEC 27001 in 27701, publikacije o arhitekturah revizijskih sledi) ter vsebinsko ustreznih strokovnih in znanstvenih člankov. Analiza pridobljenih podatkov je bila izvedena z deskriptivno metodo, utemeljena pa na študiji primera eZdravje.

3 REZULTATI

3.1 Informacijski sistem ATNA za revizijske sledi eZdravja

Sistem revizijske sledi ATNA (Audit Trail and Node Authentication) predstavlja ključno komponento v arhitekturi sistema eZdravje. Arhitekturno je umeščen v informacijsko rešitev CRPP, in predstavlja eno ključnih funkcionalnosti aplikativne programske opreme, na kateri je zasnovan CRPP (NIJZ, 2024b). CRPP je zasnovan na standardu IHE XDS, ki je temeljni standard zdravstvene informatike za izmenjavo elektronskih zdravstvenih zapisov (NIJZ, 2016). Deluje kot centralna storitev, ki je na voljo vsem aplikativnim rešitvam eZdravja. Omogoča celovito beleženje dogodkov v povezavi z dostopom do zdravstvenih podatkov, ki se obdelujejo v CRPP. ATNA je vzpostavljena kot izhodišče za centralni sistem revizijskih sledi, v katerega so integrirane tudi druge rešitve, npr. zVEM, eNaročanje in (v procesu integracije)

eRecept. ATNA uporablja standardiziran zapis podatkov, ki se ustvarja samodejno prek vmesnika lhAdapter in REST API-ja, kar omogoča beleženje dogodkov iz drugih aplikacij oz. informacijskih rešitev (Bečić idr., 2006).

Vsak revizijski zapis vsebuje ključne podatke za sledljivost: datum in čas nastanka dogodka, vrsto izvedene operacije, identifikator pacienta, identifikator dokumenta, izvajalca zdravstvene dejavnosti, rezultat operacije, podatke o uporabniku (npr. številka profesionalne kartice), uporabljeno aplikacijo ter trajanje operacije. Beleži se tudi podatek o informacijskem sistemu,

iz katerega je bila izvedena operacija, kar je v veliko pomoč pri razreševanju tehničnih napak in neskladnosti. V nekaterih primerih se beleži tudi razširjen nabor podatkov, t.i. »payload«, ki vključuje dodatne parametre, vendar brez občutljivih vsebin zdravstvenih zapisov (Bečić idr., 2007). V primeru poizvedbe v CRPP, razširjen nabor podatkov vsebuje informacije o odločitvenem algoritmu za filtriranje dostopne zdravstvene dokumentacije (Slika 1). Za upravljavca in vzdrževalce rešitev eZdravja je ATNA dragocen pripomoček za analizo težav pri dostopu do CRPP, saj je iz zapisov mogoče ugotoviti vzroke, zakaj določeni podatki niso dostopni.

Slika 1: Revizijska sled - Zapisi kontrolnih mehanizmov pri dostopu do CRPP

Zdravstveni delavec	Izbrani osebni zdravnik	Zdravnik specialist
-poizvedba vrne samo Povzetek podatkov o pacientu	Poizvedba vrne vso dokumentacijo	Poizvedba vrne
0: "role=drugi,,	0: "role=zdravnik,,	0: "role=zdravnik,,
1: "optOut=false,,	1: "isGP=true,,	1: "isGP=false,,
2: "patientSummary"	2: "limitByVzd([302]),"	2: "optIn=false,,
	3: "limitByVzd"	3: "optOut=false,,
		4: "hasReferralV2: hasAppointment_2_3_4: true (uid=324ab964-9ad5-49b5-8831-10b5c81af533::default::2),"
		5: "hasReferral=true,,
		6: "limitByVzd([109, 132]),"
		7: "limitByVzd"

Zapisi o kontrolnih mehanizmih dostopa do CRPP v revizijski sledi

Revizijske sledi se prenašajo v obliki zapisa JSON prek metod POST na vnaprej določeno končno točko, kar omogoča standardizirano integracijo različnih aplikacijskih rešitev v centralni nadzorni sistem ATNA (Bečić idr., 2006). Na ta način sistem eZdravje vzpostavlja poenoteno evidenco vseh dostopov, kar je ključno za zagotavljanje skladnosti z zakonodajo in notranjo revizijo.

3.2 Napredne funkcije za upravljavca in posameznike

Pomembna funkcionalnost sistema ATNA je spletna aplikacija za upravljavca (Slika 2). Omogoča vpogled v transakcije v rešitvah eZdravja v stvarnem času, in vključuje osnovne funkcije za iskanje in filtriranje. Spletna aplikacija za upravljavca omogoča tudi nadzor nad končnimi uporabniki pri upravljavcih, ter sledljivost dostopov do podatkov (prijave v ATNA s strani zaposlenih na NIJZ).

Pri tem ne gre za neposredni dostop do sistemskih dnevniških datotek, saj tovrsten dostop v stvarnem času ne bi bil primeren z vidika tehnične arhitekture, virov in sistemskih obremenitev. Spletna aplikacija dostopa do asinhrono kopije dnevniških zapisov, ki je uporabnikom na voljo za omenjeno časovno obdobje (približno zadnjih 6 mesecev). Omenjeno rešitev uporablja tudi portal zVEM, ki pacientom omogoča vpogled v informacije o obdelavah njihovih podatkov (NIJZ, 2024c).

Slika 2: Spletna rešitev za analizo revizijske sledi

Audit ExplorerTrace logKPIAccess log

admin@stage

Filter

ActioniHAdapter.query...iHAdapter.retrieve...Click to search...

Document typeClick to search...

Document title

Document unique id

Referral unique id

Encounter unique id

From28.05.2025at00:00:00To06.06.2025at00:00:00

Usecase name

Usecase id

Patient id

Class code

Context

Organisation10481OI Ljubljana

User id

Class code

Outcome code fromto

Duration from0to*

Export limit50000Export

SearchReset

Date	Event	Patient id	Document id	Organisation	Outcome	User id	User	Application	Duration
29.05.2025 21:16:05	queryDocuments@iHAdapter	903001933@KZZ		10481OI Ljubljana	403	99934@BPI	ubtest	ThinkClinical (Marand d.o.o.)	2ms
29.05.2025 21:14:38	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	139ms
29.05.2025 21:14:17	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	91ms
29.05.2025 21:13:14	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	533ms
29.05.2025 18:32:07	retrieveDocument@iHAdapter	903001276@KZZ	2.16.840.1.113883.3.711.2.1.4.5.1887071161	10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	335ms
29.05.2025 18:31:48	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	229ms
29.05.2025 18:31:36	queryDocuments@iHAdapter	701094166@KZZ		10481OI Ljubljana	251	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	2ms
29.05.2025 18:31:21	queryDocuments@iHAdapter	701094166@KZZ		10481OI Ljubljana	251	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	3ms
29.05.2025 16:30:13	queryDocuments@iHAdapter	701094166@KZZ		10481OI Ljubljana	403	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	2ms
29.05.2025 18:29:46	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	403	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	2ms
29.05.2025 18:29:25	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	403	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	2ms
29.05.2025 16:34:33	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	191ms
29.05.2025 16:34:21	retrieveDocument@iHAdapter	903001276@KZZ	2.16.840.1.113883.3.711.2.1.4.5.1288750523	10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	323ms
29.05.2025 16:34:06	queryDocuments@iHAdapter	903001276@KZZ		10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	234ms
29.05.2025 16:29:46	retrieveDocument@iHAdapter	903001200@KZZ	2.16.840.1.113883.3.711.2.1.4.5.919795736	10481OI Ljubljana	200	99952@BPI	nitest	ThinkClinical (Marand d.o.o.)	282ms

Poleg nadzora nad transakcijami oz. obdelavami osebnih podatkov, sistem omogoča tudi spremljanje obremenitve in odzivnosti CRPP, kot npr. število transakcij po vrstah, čas izvajanja posameznih transakcij, morebitne napake ali pa

neuspešne transakcije (Slika 3). Omenjene funkcije upravljavcu in vzdrževalcem omogočajo vpogled v delovanje sistema v stvarnem času, spremljanje obremenitev ter pravočasno ukrepanje v primeru ugotovljenih napak in odstopanj.

Slika 3: statistično spremljanje transakcij na sistemu CRPP

Audit ExplorerTrace logKPIAccess log

itotice@prod

Summarypdc-tianiapp-1.ihe.ezdravpdc-tianiapp-2.ihe.ezdravpdc-tianiapp-3.ihe.ezdrav

Summary														
Action	Stats							Errors						
	Count	Avg (ms)	Min (ms)	Max (ms)	50th pct. (ms)	90th pct. (ms)	Failovers	400	403	409	500	541	542	
Better.Better Platform.CompositionResource.createComposition(.)	230954	15	8	20616	15	18	0	0	0	0	0	0	0	
Better.Better Platform.CompositionResource.getComposition(.)	10	2	1	4	2	3	0	0	0	0	0	0	0	
Better.Better Platform.CompositionResource.updateComposition(.)	548954	22	2	10000	22	29	0	0	0	0	30	0	0	
Better.Better Platform.QueryResource.query(.)	459926	13	0	4415	8	19	0	0	0	0	1	0	0	
Better.Better Platform.QueryService.cancel(.)	77796	0	0	0	1	1	0	0	0	0	0	0	0	
Better.Better Platform.QueryService.query(.)	1973628	18	1	1570	10	31	0	0	0	0	0	0	0	
Better.Better Platform.QueryService.queryAsync(.)	77798	0	0	204	1	2	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.commitComposition(.)	617522	12	1	245	12	15	0	0	0	0	4	0	0	
Better.Better Platform.ThinkEhrService.commitContribution(.)	1615200	15	0	421	15	21	0	0	0	0	78	0	0	
Better.Better Platform.ThinkEhrService.createComposition(.)	1271935	2	0	10000	2	3	0	0	0	0	35218	0	0	
Better.Better Platform.ThinkEhrService.createContribution(.)	1799607	0	0	56	1	1	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.createSubjectEhr(.)	3308	17	11	71	16	24	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.deleteComposition(.)	11160	3	1	37	3	5	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.findEhr(.)	25110	0	0	14	1	1	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.modifyComposition(.)	516852	2	0	208	3	5	0	0	0	0	103	0	0	
Better.Better Platform.ThinkEhrService.query(.)	971562	17	2	796	9	18	0	0	0	0	0	0	0	
Better.Better Platform.ThinkEhrService.queryPopulationContent(.)	664874	17	2	835	10	19	0	0	0	0	0	0	0	

Praktična vrednost sistema ATNA se kaže tudi v uporabniški izkušnji pacientov: posamezniki imajo možnost vpogleda v zgodovino dostopov do svojih podatkov prek portala zVEM, kjer so prikazani podatki o tem, kateri zdravstveni delavec je

dostopal do katerih podatkov in kdaj (NIJZ, 2024d). To pomembno krepi tako zaupanje pacientov v varnost informacijskega sistema kot tudi zavedanje zdravstvenih delavcev, da so vpogledi v podatke pacientov dopustni samo za zakonite namene.

3.3 Sistem ATNA in izpolnjevanje zakonodajnih obveznosti upravljavca eZdravja

Sistem ATNA uspešno deluje od vzpostavitve CRPP leta 2015 oz. ob zaključku projekta vzpostavitve nacionalnega eZdravja. Od takrat vseskozi potrjuje pravilnost strateške odločitve o vzpostavitvi centralnega sistema za izmenjavo zdravstvene dokumentacije in pripadajočih sistemskih storitev ter upoštevanja sodobnih mednarodnih standardov. Poleg zagotavljanja skladnosti z nacionalno in evropsko zakonodajo o varstvu osebnih podatkov (ZVOP-2, GDPR), postavlja tudi temelje za implementacijo EHDS. Sistem ATNA bo v pomoč pri zagotavljanju skladnosti z naslednjimi zahtevami EHDS (2025):

- Zagotavljanje pravice fizičnih oseb do informacij o dostopih elektronskih zdravstvenih podatkov (člen 9).
- Vzpostavitev evropske komponente za beleženje (člen 25).
- Zahteve glede varnosti in beleženja (Dodatek II, poglavje 3).

4 RAZPRAVA IN ZAKLJUČEK

Skupaj z napredkom in uporabo informacijskih rešitev v zdravstvu se povečuje potreba po večji transparentnosti in nadzoru nad obdelavo osebnih in zdravstvenih podatkov (NIJZ, 2024a). V tem kontekstu revizijsko sledenje igra ključno vlogo pri zagotavljanju skladnosti z zahtevami zakonodaje, varovanju pacientovih pravic ter krepitevi zaupanja v eZdravje. Centralna rešitev za zagotavljanje revizijskih sledi ATNA zato predstavlja tehnični odgovor na ta izziv.

Rezultati analize kažejo, da sistem ATNA omogoča zanesljivo beleženje vseh pomembnih operacij pri obdelavi zdravstvenih podatkov. Zbiranje podatkov v standardizirani obliki omogoča učinkovito revizijo in forenzične analize ob morebitnih varnostnih incidentih. To je še posebej pomembno v kontekstu CRPP, kjer se nahajajo ključni zdravstveni podatki na nacionalni ravni (NIJZ, 2024b).

Tehnična rešitev temelji na vmesniku REST API in povezovanju ter uporabi strukturiranih sporočil v obliki zapisa JSON, omogoča pa razširljivost in povezovanje različnih informacijskih rešitev v enoten sistem sledljivosti. Pomembno je, da so zapisi samodejni, in jih ni mogoče ročno spreminjati, kar je skladno z dobrimi praksami zagotavljanja informacijske varnosti (Bečić idr., 2006).

Z vidika uporabnikov ima revizijsko sledenje tudi simbolno vrednost. Možnost vpogleda v zgodovino dostopov prek portala zVEM povečuje transparentnost nad obdelavo osebnih podatkov pacientov, hkrati pa omogoča učinkovitejšo uresničevanje pravic, ki jih posameznikom daje GDPR v zvezi z njihovimi osebnimi podatki (NIJZ, 2024d). Predstavlja tudi dobro osnovo za implementacijo EHDS.

V prihodnosti se pričakuje širitev sistema ATNA z integracijo revizijskih sledi iz drugih podsistemov in aplikacij v zdravstvu. Ta centralizacija bo prispevala k celostnemu upravljanju informacijskih tokov, povečala varnost in olajšala nadzor nad obdelavo podatkov pristojnim institucijam.

Na podlagi ugotovitev je mogoče skleniti, da ATNA ni zgolj tehnični pripomoček, ampak eden od ključnih mehanizmov zaupanja v informacijske zdravstvene rešitve, saj omogoča in spodbuja varno, odgovorno ter pregledno obdelavo zdravstvenih podatkov.

LITERATURA



- Bečić B, Lončarić S. Creating an IHE ATNA-based audit repository. *Journal of Digital Imaging* 2006; 19, 307-315.
- Bečić B, Lončarić S. Integrating the Healthcare Enterprise: Implementation of ATNA Audit Trails. *Journal of Digital Imaging* 2007; 20: 140–148.
- Direktiva (EU) 2022/2555 (NIS2) o ukrepih za visoko skupno raven kibernetičke varnosti. Pridobljeno 21.4.2025 iz spletne strani <https://eur-lex.europa.eu/eli/dir/2022/2555/oj?locale=sl>
- Drev M, Stanimirović D. Sustainable growth in the use of eHealth applications – building trust in healthcare digitalisation initiatives. V: *Book of abstracts for the 10th anniversary international symposium: health for all - challenges in ageing societies*. Ljubljana: 2023.
- Drev M, Stanimirović D, Delak B. Implementation of privacy by design model on eHealth information system. V: *Abstracts Proceedings - KM Conference 2022*. Ljubljana: 2022.
- Nacionalni inštitut za javno zdravje (NIJZ). eZdravje – Nacionalni projekt za digitalizacijo zdravstva. Pridobljeno 12.10.2024 (a) s spletne strani <https://ezdrav.si/ezdravje>
- Nacionalni inštitut za javno zdravje (NIJZ). CRPP – Centralni register podatkov o pacientih. Pridobljeno 14.10.2024 (b) s spletne strani <https://ezdrav.si/resitve/crpp>
- Nacionalni inštitut za javno zdravje. ZVEM – Portal za paciente. Pridobljeno 6.12.2024 (c) s spletne strani <https://ezdrav.si/resitve/zvem>
- Nacionalni inštitut za javno zdravje (NIJZ). Sledljivost vpogledov prek zVEM. Pridobljeno 4.12.2024 (d) s spletne strani <https://podpora.ezdrav.si/faq/na-koga-naj-se-obrnem-za-natančneje-podatke-o-vpogledih-v-svojo-zdravstveno-dokumentacijo-ali-lahko-pridobim-poimenske-podatke-oseb-zdravstvenih-delavcev-ki-dostopajo-do-mojih-podatkov>
- Nacionalni inštitut za varovanje zdravja (NIJZ). Revizijsko sledenje – tehnična dokumentacija. *Interni dokument*. Ljubljana: 2016.
- Uredba (EU) 2016/679 o varstvu posameznikov pri obdelavi osebnih podatkov (GDPR). Pridobljeno 15.9.2024 s spletne strani <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32016R0679>
- Uredba (EU) 2025/327 o evropskem zdravstvenem podatkovnem prostoru (EHDS). Pridobljeno 4.6.2025 s spletne strani https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=OJ%3AL_202500327
- Zakon o varstvu osebnih podatkov (ZVOP-2). *Uradni list RS*, št. 163/22. Pridobljeno 7.3.2024 s spletne strani <https://pisrs.si/pregledPredpisa?id=ZAKO7959>
- Zakon o informacijski varnosti (ZInfV-1). *Uradni list RS*, št. 30/18, 61/20. Pridobljeno 4.6.2025 s spletne strani <https://pisrs.si/pregledPredpisa?id=ZAKO8934>
- Zakon o kibernetički varnosti (ZKI). *Uradni list RS*, št. 80/23. Pridobljeno 24.4.2025 s spletne strani <https://pisrs.si/pregledPredpisa?id=ZAKO9003>