Na osnovu člana 10. i člana 12. Zakona o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025) i Uredbe o bližem sadržaju akta o bezbednosti informaciono-komunikacionih sistema od posebnog značaja, Dr Tijana donosi

Akt o bezbednosti IKT sistema — Dr Tijana

POVERLJIVO — dokument firme „Dr Tijana“ sadrži mere zaštite i procedure IKT sistema. Ne distribuirati van BDB tima i ovlašćenih lica klijenta.

Datum generisanja: 07.11.2026. 23:12

Dokument je pripremljen na osnovu Analize rizika, u skladu sa čl. 10 Zakona o informacionoj bezbednosti („Sl. glasnik RS“, br. 91/2025) i Uredbom o bližem sadržaju akta o bezbednosti IKT sistema od posebnog značaja. Pre usvajanja od strane organa upravljanja, sadržaj proveriti, dopuniti i urediti.

Član 1. Predmet akta

Ovim aktom o bezbednosti IKT sistema (u daljem tekstu: Akt) određuju se mere zaštite, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti informaciono-komunikacionog sistema od posebnog značaja Dr Tijana (u daljem tekstu: IKT sistem), kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema.

Član 2. Pojmovi i definicije

Pojedini izrazi upotrebljeni u ovom Aktu imaju sledeće značenje:

1) IKT sistem je tehnološko-organizaciona celina koja obuhvata elektronske komunikacione mreže, uređaje ili grupe međusobno povezanih uređaja kod kojih se vrši automatska obrada podataka, podatke koji se čuvaju, obrađuju, pretražuju ili prenose, organizacionu strukturu i softver putem kojih se tim sistemom upravlja;

2) informaciona bezbednost je sposobnost IKT sistema i mreža da se, uz određeni stepen pouzdanosti, odupru događajima koji mogu da ugroze raspoloživost, integritet, autentičnost, neporecivost i poverljivost podataka koji se čuvaju, prenose ili obrađuju;

3) poverljivost je svojstvo da podatak nije dostupan niti otkriven neovlašćenim licima;

4) integritet je svojstvo očuvanosti izvornog sadržaja i kompletnosti podatka;

5) raspoloživost je svojstvo da je podatak dostupan i upotrebljiv na zahtev ovlašćenih lica onda kada im je potreban;

6) autentičnost je svojstvo koje omogućava proveru da je podatak stvorilo ili poslalo lice za koje je deklarisano da je tu radnju izvršilo;

7) neporecivost je sposobnost dokazivanja da se dogodila određena radnja ili nastupio određeni događaj, tako da ga naknadno nije moguće poreći;

8) rizik je mogućnost nastanka štete izražena kao kombinacija verovatnoće nastanka incidenta i njegovih posledica;

9) upravljanje rizikom je sistematičan proces identifikovanja, procene i tretiranja rizika kako bi se oni održali u prihvatljivim okvirima;

10) incident je događaj koji ugrožava ili narušava informacionu bezbednost;

11) informaciona dobra su podaci, programski kod, konfiguracija uređaja, tehnička i korisnička dokumentacija, evidencije i drugi resursi IKT sistema koji podležu zaštiti;

12) operator IKT sistema je pravno ili fizičko lice koje koristi IKT sistem za obavljanje delatnosti.

Član 3. Ciljevi akta

Ciljevi donošenja ovog akta su:

1. određivanje načina i procedura za postizanje i održavanje adekvatnog nivoa bezbednosti IKT sistema;

2. sprečavanje i ublažavanje posledica incidenata kojima se ugrožava ili narušava informaciona bezbednost;

3. podizanje svesti zaposlenih o značaju informacione bezbednosti, rizicima i merama zaštite prilikom korišćenja IKT sistema;

4. propisivanje ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema;

5. sveukupno unapređenje informacione bezbednosti i praćenje usklađenosti primenjenih mera zaštite sa ovim aktom.

Član 4. Obaveza primene

Dr Tijana, kao operator IKT sistema, odgovara za bezbednost IKT sistema i preduzimanje mera zaštite propisanih ovim aktom.

Primena mera iz ovog akta obavezna je za sve zaposlene Dr Tijana, kao i za angažovane treće strane kojima je odobren pristup IKT sistemu, u delu koji se na njih odnosi.

[IME ODGOVORNOG LICA] odgovoran je za praćenje primene mera iz ovog akta i za proveru da su informaciona dobra zaštićena na način utvrđen ovim aktom i pratećim internim dokumentima.

Član 5. Odgovornost zaposlenih

Zaposleni su dužni da pristupaju informacijama i resursima IKT sistema isključivo radi obavljanja poslovnih aktivnosti, i da o uočenim bezbednosnim slabostima i incidentima blagovremeno obaveste [IME ODGOVORNOG LICA].

Nepoštovanje odredaba ovog akta, kao i svako ugrožavanje ili narušavanje informacione bezbednosti, povlači disciplinsku odgovornost zaposlenog, u skladu sa opštim aktima Dr Tijana.

Član 6. Organizaciona struktura (tačka 1. člana 10. stav 4. Zakona)

Odgovornost za svaki sistem i proces u okviru [NAZIV FIRME] formalno se utvrđuje i dokumentuje, čime se obezbeđuje jasna linija odgovornosti za ključne poslovne procese, uključujući zakazivanje i vođenje medicinske dokumentacije pacijenata. Za nadzor nad informacionom bezbednošću na nivou organizacije zadužen je [IME ODGOVORNOG LICA], direktor i osnivač ordinacije, koji je ujedno odgovoran i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. U okviru organizacione strukture uspostavlja se formalno telo ili lice posebno zaduženo za informacionu bezbednost, čije se nadležnosti, ovlašćenja i procedure rada bliže uređuju aktima [NAZIV FIRME] koji regulišu upravljanje informacionom bezbednošću.

Formalno telo ili osoba posebno zadužena za informacionu bezbednost u ovom trenutku nije uspostavljena, dok je odgovornost za nadzor nad informacionom bezbednošću trenutno koncentrisana kod direktora, uz odsustvo posebne organizacione jedinice koja bi se posvećeno bavila ovom oblašću. Imajući u vidu da ključni poslovni proces zavisi od kontinuiranog funkcionisanja IKT sistema i poverljivosti osetljivih zdravstvenih podataka pacijenata, odsustvo formalno uspostavljene funkcije informacione bezbednosti povećava rizik od neblagovremenog prepoznavanja i reagovanja na bezbednosne pretnje, kao i rizik od neadekvatnog nadzora nad merama zaštite usled preopterećenosti postojećeg nosioca odgovornosti drugim poslovnim funkcijama.

Član 7. Prikupljanje podataka o pretnjama (tačka 2. člana 10. stav 4. Zakona)

[NAZIV FIRME] prikuplja podatke o bezbednosnim pretnjama relevantnim za delatnost zdravstvene zaštite kroz sistematsko praćenje bezbednosnih biltena, obaveštenja nadležnog CERT tima i učešće u razmeni informacija o pretnjama sa drugim organizacijama i industrijskim grupama. Prikupljeni podaci koriste se za blagovremeno prepoznavanje pretnji specifičnih za sektor zdravstva i prilagođavanje mera zaštite Bolničkog

informacionog sistema i medicinske dokumentacije pacijenata. Za sprovođenje ove mere odgovoran je [IME ODGOVORNOG LICA], direktor, koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti.

Mera trenutno nije ispunjena, jer [NAZIV FIRME] ne učestvuje u razmeni informacija o bezbednosnim pretnjama sa drugim organizacijama ili industrijskim grupama, niti sistematski prati bezbednosne biltene, CERT obaveštenja i stručne izvore relevantne za sektor zdravstva. Ovakvo odstupanje povećava rizik od zakasnelog prepoznavanja novih pretnji usmerenih na zdravstveni sektor, što može negativno uticati na blagovremenost zaštite Bolničkog informacionog sistema i poverljivost zdravstvenih podataka pacijenata, s obzirom na to da incident direktno ugrožava kontinuitet pružanja zdravstvenih usluga.

Član 8. Bezbednost rada na daljinu (tačka 3. člana 10. stav 4. Zakona)

Rad na daljinu u [NAZIV FIRME] dozvoljava se isključivo uz primenu bezbedne udaljene veze (VPN ili ekvivalentno rešenje), enkriptovanu komunikaciju i mere zaštite od neovlašćenog pristupa sa udaljenih i mobilnih uređaja kojima se pristupa sistemima koji sadrže podatke o zakazivanju i medicinsku dokumentaciju pacijenata. Odgovornost za primenu ove mere, uključujući odobravanje pristupa sa udaljenih lokacija i nadzor nad bezbednošću takvog pristupa, snosi [IME ODGOVORNOG LICA], direktor. Detaljna pravila uređena su posebnim dokumentom — Politika rada od kuće.

Mera trenutno nije ispunjena jer rad na daljinu ne obuhvata bezbednu udaljenu vezu, enkriptovanu komunikaciju niti mehanizme zaštite od neovlašćenog pristupa sa udaljenih i mobilnih uređaja. Ovo odstupanje nosi visok rizik za sistem zdravstvene ordinacije, s obzirom na to da se preko udaljenog pristupa mogu obrađivati osetljivi zdravstveni podaci pacijenata, pa neovlašćen pristup ili presretanje komunikacije može direktno ugroziti poverljivost medicinske dokumentacije i kontinuitet pružanja zdravstvenih usluga.

Član 9. Osposobljenost lica koja koriste sistem (tačka 4. člana 10. stav 4. Zakona)

Sva lica koja koriste IKT sistem [NAZIV FIRME], uključujući zaposlene koji pristupaju Bolničkom informacionom sistemu i drugim sistemima od posebnog značaja, prolaze redovnu obuku iz informacione bezbednosti, uključujući prepoznavanje socijalnog inženjeringa, fišing pokušaja i rizika povezanih sa upotrebom alata zasnovanih na veštačkoj inteligenciji. Detaljna pravila u pogledu sadržaja, dinamike i načina sprovođenja obuke uređena su posebnim dokumentom — Plan obuke i podizanja svesti. Za organizovanje, sprovođenje i nadzor nad realizacijom obuke odgovoran je direktor, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedura primene mere podrazumeva periodično sprovođenje obuka za sva lica koja koriste sistem, kao i evidentiranje njihovog učešća u skladu sa Planom obuke i podizanja svesti.

Mera trenutno nije ispunjena, s obzirom na to da zaposleni dosad nisu prolazili obuku iz informacione bezbednosti, nisu osposobljeni za prepoznavanje socijalnog inženjeringa i fišing napada, niti su upoznati sa rizicima AI-generisanih prevara i merama zaštite podataka unetih u AI alate. Obrazloženje ovog odstupanja leži u tome što uspostavljanje sistematskog programa obuke tek predstoji, u skladu sa usvojenim Planom obuke i podizanja svesti. Odsustvo osposobljenosti zaposlenih značajno povećava rizik od uspešnih napada socijalnog inženjeringa i neovlašćenog otkrivanja osetljivih zdravstvenih podataka pacijenata, s obzirom na to da ljudski faktor predstavlja jednu od najčešćih tačaka kompromitovanja IKT sistema, naročito u sektoru zdravstva gde se obrađuju naročito osetljivi podaci o ličnosti.

Član 10. Dovoljno resursa (tačka 5. člana 10. stav 4. Zakona)

[NAZIV FIRME] ovim aktom obezbeđuje dovoljno finansijskih, tehničkih i ljudskih resursa za primenu i održavanje mera informacione bezbednosti, kroz posebno planiranje sredstava u okviru godišnjeg budžeta. Za planiranje i odobravanje budžeta namenjenog informacionoj bezbednosti odgovoran je direktor i osnivač ordinacije, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procena potrebnih resursa vrši se periodično, uzimajući u obzir značaj IKT sistema za ključne poslovne procese, posebno za zakazivanje i vođenje medicinske dokumentacije pacijenata, kao i rizike kojima su izloženi podaci i sistemi [NAZIV FIRME].

Poseban budžet namenjen informacionoj bezbednosti trenutno nije uspostavljen, što predstavlja odstupanje od propisane mere. Ovakvo stanje povećava rizik od nedovoljnog i neblagovremenog finansiranja tehničkih i organizacionih mera zaštite, što je posebno osetljivo imajući u vidu da incident u IKT sistemu [NAZIV FIRME] može direktno ugroziti kontinuitet pružanja zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka pacijenata. [KLIJENT DA DOPUNI: okvirni rok i plan uspostavljanja posebne budžetske stavke za informacionu bezbednost].

Član 11. Zaštita pri promeni poslova zaposlenih (tačka 6. člana 10. stav 4. Zakona)

Pristup IKT sistemima, uključujući Bolnički informacioni sistem, menja se ili oduzima zaposlenom odmah po prestanku radnog odnosa ili promeni radne pozicije, kako bi se obim ovlašćenja uvek usklađivao sa aktuelnim poslovnim potrebama zaposlenog. Za pokretanje i sprovođenje postupka oduzimanja odnosno izmene pristupa odgovoran je [IME ODGOVORNOG LICA], direktor i osnivač ordinacije, koji ujedno vrši nadzor nad informacionom bezbednošću i praćenje usklađenosti sa propisima. Detaljna pravila u vezi sa dodelom, izmenom i ukidanjem pristupnih prava uređena su posebnim dokumentom — Politika upravljanja pristupom.

[KLIJENT DA DOPUNI: tačan opis procedure za hitno oduzimanje pristupa pri prestanku radnog odnosa ili promeni pozicije, rokovi za sprovođenje, kao i dokaz da je procedura

formalizovana i primenjena u praksi]. Procena uticaja ovog odstupanja: s obzirom na to da [NAZIV FIRME] obrađuje osetljive zdravstvene podatke pacijenata kroz Bolnički informacioni sistem, odsustvo jasno definisane procedure za hitno oduzimanje pristupa predstavlja rizik od neovlašćenog pristupa medicinskoj dokumentaciji od strane lica kojima je radni odnos prestao ili čija se pozicija promenila, što može ugroziti poverljivost podataka i kontinuitet pružanja zdravstvenih usluga.

Član 12. Identifikovanje informacionih dobara (tačka 7. člana 10. stav 4. Zakona)

[NAZIV FIRME] vodi i redovno ažurira registar informacionih dobara koji obuhvata sve lokacije, hardver, softver, zaposlene, informacije i treće strane relevantne za poslovanje ordinacije. Registar obuhvata lokacije (glavnu ordinaciju na Vračaru, filijalu na Novom Beogradu i serversku sobu na glavnoj lokaciji), hardver (lokalni fajl/aplikativni server, radne stanice, mrežnu opremu, službene mobilne uređaje lekara i mrežne štampače/skenere), softver (sistem elektronskog kartona pacijenata, poslovnu e-poštu u oblaku, računovodstveni softver, veb sajt za online zakazivanje i AI alat za transkripciju nalaza koji je u fazi razmatranja), zaposlene (direktora ordinacije, lekare i medicinske sestre, administrativno/recepcijsko osoblje i spoljnog IT saradnika), informacije (medicinske kartone i nalaze pacijenata, lične i kontakt podatke pacijenata, kadrovske podatke zaposlenih i finansijske/računovodstvene podatke) i treće strane (spoljnog IT saradnika i hosting provajdera, eksternu laboratoriju, dobavljača softvera za elektronski karton i spoljnu knjigovodstvenu agenciju). Za vođenje, ažuriranje i tačnost registra informacionih dobara odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA]. Popis se vrši po svim navedenim kategorijama dobara radi obezbeđenja potpunog uvida u resurse koji podržavaju ključni poslovni proces zakazivanja i vođenja medicinske dokumentacije pacijenata, a svaka promena u sastavu informacionih dobara (uvođenje novog sistema, uređaja ili angažovanje nove treće strane) unosi se u registar najkasnije pre početka njegovog korišćenja u poslovanju.

Član 13. Klasifikacija podataka (tačka 8. člana 10. stav 4. Zakona)

Svi podaci koji se obrađuju u okviru [NAZIV FIRME] klasifikuju se prema nivou osetljivosti, pri čemu se posebno izdvaja kategorija osetljivih zdravstvenih podataka pacijenata koji se obrađuju u vezi sa zakazivanjem i vođenjem medicinske dokumentacije. Detaljna pravila klasifikacije i upravljanja podacima, uključujući kriterijume za razvrstavanje po nivoima osetljivosti i postupanje sa svakim nivoom, uređena su posebnim dokumentom — Politika klasifikacije i upravljanja podacima. Za primenu ove mere, kao i za nadzor nad usklađenošću sa njom, odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA].

Politika klasifikacije i upravljanja podacima na koju ovaj Akt upućuje u trenutku usvajanja ovog Akta nije formalno doneta, usled čega postupak klasifikacije podataka još uvek nije uspostavljen u praksi. Imajući u vidu da ključni poslovni proces [NAZIV FIRME]

podrazumeva obradu osetljivih zdravstvenih podataka pacijenata, odsustvo formalizovane klasifikacije podataka predstavlja povećan rizik po poverljivost tih podataka i otežava primenu adekvatnih mera zaštite srazmernih nivou osetljivosti, te će se otklanjanje ovog nedostatka sprovesti donošenjem i primenom navedene politike.

Član 14. Zaštita nosača podataka (tačka 9. člana 10. stav 4. Zakona)

Upotreba USB portova i prenosivih medijuma na svim računarima u okviru [NAZIV FIRME] dozvoljena je isključivo nakon prethodne kontrole i skeniranja na prisustvo zlonamernog softvera, čime se obezbeđuje zaštita poverljivosti i integriteta zdravstvenih podataka pacijenata koji se obrađuju u okviru poslovnih procesa zakazivanja i vođenja medicinske dokumentacije. Za nadzor nad primenom ove mere odgovoran je [IME ODGOVORNOG LICA], direktor i osnivač ordinacije, koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedura podrazumeva da se svaki prenosivi medijum pre priključivanja na radnu stanicu ili server proverava odgovarajućim alatom za skeniranje, a tek po potvrdi da medijum ne sadrži zlonamerni sadržaj dozvoljava se njegova dalja upotreba.

Član 15. Ograničenje pristupa (tačka 10. člana 10. stav 4. Zakona)

Pristup podacima i IKT sistemima u [NAZIV FIRME] dodeljuje se isključivo po principu najmanje privilegije, odnosno samo onim zaposlenima kojima je pristup neophodan za obavljanje radnih zadataka, uz periodičnu proveru dodeljenih prava i uklanjanje onih koja više nisu potrebna. Za primenu ove mere odgovoran je [IME ODGOVORNOG LICA], direktor, koji ujedno vrši i nadzor nad usklađenošću sa ovom merom. Detaljna pravila dodele, provere i ukidanja pristupnih prava uređena su posebnim dokumentima — Politikom upravljanja pristupom i Politikom upravljanja lozinkama, dok se kontrola neovlašćene izmene ili otkrivanja ključnih podataka, uključujući medicinsku dokumentaciju pacijenata, sprovodi u skladu sa istim aktima.

Mera trenutno nije u potpunosti primenjena, s obzirom na to da kriterijumi za dodelu pristupa podacima nisu formalno definisani, periodična provera dodeljenih prava pristupa se ne sprovodi, a kontrole koje sprečavaju neovlašćenu izmenu ili otkrivanje ključnih podataka nisu jasno uspostavljene. [KLIJENT DA DOPUNI: rok do kog se planira uspostavljanje formalnih kriterijuma za dodelu pristupa i periodične provere prava pristupa]. Odsustvo ovih kontrola predstavlja povećan rizik po poverljivost i integritet zdravstvenih podataka pacijenata, s obzirom na to da neovlašćen ili preširok pristup medicinskoj dokumentaciji može dovesti do neovlašćenog otkrivanja ili izmene osetljivih podataka i direktno ugroziti kontinuitet ključnog poslovnog procesa zakazivanja i vođenja medicinske dokumentacije pacijenata.

Član 16. Odobravanje ovlašćenog pristupa (tačka 11. člana 10. stav 4. Zakona)

Pristup podešavanjima IKT sistema odobrava se isključivo ovlašćenim administratorima, dok je svim ostalim korisnicima takav pristup izričito onemogućen. Odgovornost za dodelu, izmenu i ukidanje ovlašćenog pristupa snosi [IME ODGOVORNOG LICA], direktor, kao lice odgovorno za nadzor nad informacionom bezbednošću u [NAZIV FIRME]. Postupak zahtevanja, odobravanja i periodične provere ovlašćenog pristupa sproveden je u skladu sa procedurama utvrđenim posebnim dokumentom — Politika upravljanja pristupom. Primena ove mere od posebnog je značaja imajući u vidu da se kroz IKT sisteme [NAZIV FIRME] obrađuju osetljivi zdravstveni podaci pacijenata, zbog čega je ograničavanje pristupa podešavanjima sistema na ovlašćene administratore neophodan preduslov za očuvanje poverljivosti i integriteta medicinske dokumentacije.

Član 17. Odgovornost korisnika (tačka 12. člana 10. stav 4. Zakona)

Svaki korisnik IKT sistema [NAZIV FIRME] dužan je da resurse informaciono-komunikacione tehnologije koristi isključivo u skladu sa definisanim pravilima prihvatljive upotrebe i da snosi ličnu odgovornost za radnje preduzete pod sopstvenim korisničkim nalogom, uključujući lozinke koje su strogo lične i ne smeju se deliti sa drugim licima. Za nadzor nad primenom ove mere odgovoran je [IME ODGOVORNOG LICA], direktor. Detaljna pravila u pogledu dozvoljenog korišćenja IT opreme i interneta uređena su posebnim dokumentom — Politika prihvatljive upotrebe IT opreme, dok su pravila o ličnoj upotrebi lozinki i zabrani deljenja naloga uređena dokumentom Politika upravljanja lozinkama.

Status primene mere u delu koji se odnosi na politiku dozvoljenog korišćenja IT opreme i interneta nije moguće jednoznačno utvrditi na osnovu raspoloživih dokaza, s obzirom na to da je odgovor na pitanje o postojanju takve politike evidentiran kao nedefinisano. [KLIJENT DA DOPUNI: da li je Politika prihvatljive upotrebe IT opreme formalno usvojena, od kog datuma važi i da li je sa njenom sadržinom upoznato osoblje ordinacije]. Dok ova nedoumica ne bude otklonjena, postoji rizik da korisnici IKT sistema ne budu u dovoljnoj meri upoznati sa granicama dozvoljenog korišćenja opreme i interneta, što u kontekstu obrade osetljivih zdravstvenih podataka pacijenata povećava izloženost riziku od neovlašćenog pristupa, zloupotrebe ili curenja podataka iz medicinske dokumentacije.

Član 18. Kriptografske kontrole (tačka 13. člana 10. stav 4. Zakona)

Osetljivi podaci, uključujući medicinsku dokumentaciju pacijenata koja se obrađuje u okviru poslovanja [NAZIV FIRME], štite se primenom kriptografskih kontrola, pri čemu se enkripcija primenjuje na podatke u mirovanju, uključujući rezervne kopije, čija se uspešnost obnavljanja periodično proverava. Odgovornost za uspostavljanje, sprovođenje i nadzor nad primenom kriptografskih kontrola, kao i za testiranje rezervnih kopija, snosi [IME ODGOVORNOG LICA], direktor. Pri izboru i implementaciji kriptografskih rešenja razmatra

se i otpornost primenjenih algoritama na buduće pretnje, uključujući razvoj kvantnog računarstva, radi obezbeđenja dugoročne poverljivosti zdravstvenih podataka.

Mera trenutno nije ispunjena, s obzirom na to da osetljivi podaci nisu enkriptovani niti se sprovodi redovno testiranje uspešnosti obnavljanja rezervnih kopija, a rizik od budućeg probijanja enkripcije kvantnim računarstvom nije razmotren. Imajući u vidu da se radi o zdravstvenim podacima pacijenata čija poverljivost predstavlja osnovu za pružanje zdravstvenih usluga, odsustvo enkripcije i neproverena mogućnost obnavljanja podataka iz rezervnih kopija predstavljaju povećan rizik od neovlašćenog pristupa, gubitka ili nepovratnog oštećenja podataka, što bi moglo neposredno ugroziti kontinuitet poslovnih procesa zakazivanja i vođenja medicinske dokumentacije. [KLIJENT DA DOPUNI: rok do kog se planira uvođenje enkripcije osetljivih podataka i uspostavljanje redovnog testiranja rezervnih kopija].

Član 19. Zaštita od oticanja podataka (tačka 14. člana 10. stav 4. Zakona)

Oticanje osetljivih podataka, uključujući podatke iz medicinske dokumentacije pacijenata, sprečava se primenom kontrola koje ograničavaju neovlašćeno deljenje, prenos ili otkrivanje podataka putem elektronske pošte, štampe, prenosivih medija i spoljnih alata, uključujući alate zasnovane na veštačkoj inteligenciji. Pravila o načinu deljenja osetljivih podataka i dozvoljenim kanalima komunikacije uređena su Politikom klasifikacije i upravljanja podacima i Politikom prihvatljive upotrebe IT opreme, koje se primenjuju na sve zaposlene sa pristupom podacima pacijenata. Za uspostavljanje, nadzor i doslednu primenu kontrola zaštite od oticanja podataka, uključujući kontrolu korišćenja AI alata, odgovoran je [IME ODGOVORNOG LICA], direktor i osnivač ordinacije, koji prati usklađenost sa propisima o informacionoj bezbednosti i preduzima mere u slučaju utvrđenih odstupanja.

Mera trenutno nije u potpunosti primenjena jer pravila o deljenju osetljivih podataka putem elektronske pošte i štampe nisu formalno definisana, ne postoji tehnička kontrola koja sprečava neovlašćenu izmenu ili otkrivanje ključnih podataka, a zaposleni nisu upoznati sa rizicima AI-generisanih prevara niti su podaci uneti u AI alate zaštićeni. Ovo odstupanje značajno povećava rizik od neovlašćenog otkrivanja osetljivih zdravstvenih podataka pacijenata i izlaže [NAZIV FIRME] riziku gubitka poverljivosti medicinske dokumentacije, što može direktno ugroziti kontinuitet pružanja zdravstvenih usluga i dovesti do povrede propisa o zaštiti podataka o ličnosti. Do uspostavljanja potpune kontrole, rizik se ublažava postojećim organizacionim merama iz povezanih internih akata, dok se puna usklađenost planira kroz dalju razradu tehničkih i proceduralnih mera zaštite od oticanja podataka.

Član 20. Fizička zaštita objekata (tačka 15. člana 10. stav 4. Zakona)

Prostorije u kojima se nalazi oprema za obradu i čuvanje podataka u [NAZIV FIRME] štite se od požara, prodora vode, prekomerne vlage i prašine, pri čemu se temperatura i vlažnost redovno nadgledaju, a oprema se dodatno štiti od elektromagnetnih smetnji odgovarajućim

uzemljenjem i prostornim razmeštajem. Pored navedenog, prostorije sa opremom obezbeđuju se mehanizmima fizičke kontrole pristupa, uključujući brave, alarmni sistem i video nadzor. Za sprovođenje i nadzor nad primenom ove mere odgovoran je direktor, [IME ODGOVORNOG LICA]. Procedure fizičke zaštite primenjuju se u obimu koji obuhvata sve prostorije u kojima se nalazi oprema od značaja za rad Bolničkog informacionog sistema i drugih IKT resursa [NAZIV FIRME].

Mehanizmi fizičkog obezbeđenja prostorija sa opremom — brave, alarmni sistem i video nadzor — u trenutku usvajanja ovog Akta nisu uspostavljeni, dok su mere zaštite od požara, vode, vlage i elektromagnetnih smetnji već sprovedene. Odsustvo fizičke kontrole pristupa i nadzora povećava rizik od neovlašćenog fizičkog pristupa prostorijama u kojima se obrađuju i čuvaju osetljivi zdravstveni podaci pacijenata, što s obzirom na delatnost [NAZIV FIRME] predstavlja značajan rizik po poverljivost medicinske dokumentacije i kontinuitet pružanja zdravstvenih usluga. [KLIJENT DA DOPUNI: rok do kog će biti uspostavljeni brave, alarmni sistem i video nadzor, kao i nosilac realizacije te mere].

Član 21. Zaštita od gubitka (tačka 16. člana 10. stav 4. Zakona)

[NAZIV FIRME] obezbeđuje zaštitu podataka i sistema od gubitka kroz kombinaciju mera rezervnog napajanja ključne opreme, procedure za prijavu gubitka ili krađe opreme, enkripciju osetljivih podataka, redovno testiranje uspešnosti obnavljanja rezervnih kopija, čuvanje rezervnih kopija na način koji onemogućava njihovo brisanje čak i sa kompromitovanog naloga, kao i primenu mera specifično usmerenih protiv ransomver napada, uključujući nepromenljive kopije podataka i segmentaciju mreže. Za sprovođenje i nadzor nad primenom ove mere odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedure primene mere obuhvataju redovnu proveru ispravnosti rezervnog napajanja, prijavljivanje gubitka ili krađe opreme nadležnom licu, periodično testiranje obnavljanja podataka iz rezervnih kopija i primenu tehničkih kontrola za zaštitu kopija od neovlašćenog brisanja ili izmene.

Mera trenutno nije u punom obimu primenjena, s obzirom na to da osetljivi podaci nisu enkriptovani, uspešnost obnavljanja rezervnih kopija se ne testira, rezervne kopije nisu zaštićene od brisanja sa kompromitovanog naloga, niti su uspostavljene mere specifično usmerene protiv ransomver napada. S obzirom na to da ključni poslovni proces [NAZIV FIRME] — zakazivanje i vođenje medicinske dokumentacije pacijenata — u potpunosti zavisi od raspoloživosti i integriteta IKT sistema, ovo odstupanje predstavlja značajan rizik po kontinuitet pružanja zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka, naročito u slučaju ransomver napada ili kompromitacije naloga sa pristupom rezervnim kopijama, kada bi mogućnost oporavka podataka bila dovedena u pitanje.

Član 22. Ispravnost sredstava (tačka 17. člana 10. stav 4. Zakona)

Ispravnost medijuma za skladištenje podataka u [NAZIV FIRME] proverava se redovnim postupkom kontrole funkcionalnog stanja uređaja na kojima se čuvaju podaci iz medicinske dokumentacije pacijenata, kako bi se obezbedila dostupnost i integritet tih podataka. Za sprovođenje i nadzor ove mere odgovoran je [IME ODGOVORNOG LICA], direktor, koji prati usklađenost sa propisima o informacionoj bezbednosti i stara se o primeni mera zaštite IKT sistema. Provera ispravnosti medijuma sprovodi se kroz periodičnu procenu stanja uređaja za skladištenje, uz evidentiranje uočenih nepravilnosti i preduzimanje mera za njihovo otklanjanje.

Na osnovu dostupnih podataka iz procene rizika nije moguće utvrditi da li se, i u kom obimu, postupak redovne provere ispravnosti medijuma za skladištenje zaista sprovodi, s obzirom na to da je odgovor na relevantno pitanje iz Kataloga pretnji „ne znam". Ovakva neizvesnost nosi potencijalni uticaj na bezbednost IKT sistema, imajući u vidu da eventualni kvar medijuma bez pravovremenog otkrivanja može ugroziti dostupnost i integritet medicinske dokumentacije pacijenata, odnosno kontinuitet ključnog poslovnog procesa zakazivanja i vođenja zdravstvene evidencije. [KLIJENT DA DOPUNI: tačan status sprovođenja provere ispravnosti medijuma, učestalost provera i dokaz o njihovom sprovođenju, odnosno rok do kog će se uspostaviti redovan postupak provere].

Član 23. Procedure za računarstvo u klaudu (tačka 18. člana 10. stav 4. Zakona)

[NAZIV FIRME] primenjuje procedure za računarstvo u klaudu kojima se uređuje korišćenje usluga spoljnih provajdera cloud infrastrukture za potrebe obrade i čuvanja podataka, uključujući medicinsku dokumentaciju pacijenata. Ovim procedurama definišu se bezbednosne obaveze koje snosi [NAZIV FIRME] kao korisnik usluge, u odnosu na obaveze koje snosi cloud provajder, kao i kriterijumi za izbor provajdera, uključujući posedovanje relevantnih nezavisnih bezbednosnih sertifikata i poznavanje lokacije fizičkog skladištenja podataka. Za primenu ove mere, uključujući procenu uslova ugovora sa cloud provajderom i mogućnosti prelaska na drugog provajdera bez ugrožavanja kontinuiteta poslovanja, odgovoran je direktor, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti.

Na osnovu dostavljenih odgovora iz procene rizika nije utvrđeno da li [NAZIV FIRME] raspolaže jasnim saznanjima o podeli bezbednosnih obaveza sa cloud provajderom, o postojanju nezavisnog bezbednosnog sertifikata provajdera, o lokaciji fizičkog skladištenja podataka, niti o mogućnosti promene provajdera bez značajnog poremećaja poslovanja, usled čega je status mere ocenjen kao nejasan. [KLIJENT DA DOPUNI: podaci o ugovoru i uslovima saradnje sa cloud provajderom, dokaz o postojanju sertifikata provajdera, lokacija skladištenja podataka i procena mogućnosti promene provajdera]. S obzirom na to da ključni poslovni proces zakazivanja i vođenja medicinske dokumentacije pacijenata zavisi od ovakve infrastrukture, nedostatak jasnog uvida u ove elemente predstavlja rizik po

kontinuitet pružanja zdravstvenih usluga i po poverljivost osetljivih zdravstvenih podataka, te zahteva hitno dopunjavanje raspoloživih informacija radi konačne ocene usklađenosti.

Član 24. Praćenje sistema (tačka 19. člana 10. stav 4. Zakona)

[NAZIV FIRME] uspostavlja kontinuirano praćenje rada IKT sistema, uključujući nadzor iskorišćenosti kapaciteta sistema (prostor, memorija) i blagovremeno uočavanje neuobičajenih aktivnosti koje mogu ukazivati na bezbednosni incident. Za sisteme koji podržavaju zakazivanje i vođenje medicinske dokumentacije pacijenata uspostavlja se plan postupanja u slučaju prestanka rada ključnog sistema, radi očuvanja kontinuiteta pružanja zdravstvenih usluga i zaštite poverljivosti zdravstvenih podataka. Za primenu ove mere, uključujući definisanje procedura praćenja i plana postupanja u slučaju prekida rada sistema, odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA]. Procedure praćenja i postupanja se dokumentuju i redovno preispituju u cilju unapređenja otkrivanja i odgovora na bezbednosne incidente.

Mera trenutno nije primenjena, s obzirom na to da ne postoji uspostavljen mehanizam za praćenje iskorišćenosti kapaciteta sistema niti za detekciju neuobičajene aktivnosti, a plan za slučaj prestanka rada ključnog sistema nije izrađen. Odsustvo ovih mehanizama značajno povećava rizik od neblagovremenog uočavanja tehničkih problema i bezbednosnih incidenata, što s obzirom na osetljivost zdravstvenih podataka i zavisnost ključnih poslovnih procesa od IKT sistema predstavlja povišen rizik po dostupnost usluga i poverljivost podataka pacijenata. [KLIJENT DA DOPUNI: rok do kog se planira uspostavljanje sistema za praćenje kapaciteta i detekciju neuobičajenih aktivnosti, kao i izrada plana za slučaj prestanka rada ključnog sistema].

Član 25. Ograničenje pristupa veb prezentacijama (tačka 20. člana 10. stav 4. Zakona)

Pristup zaposlenih internetu i veb prezentacijama ograničava se primenom tehničkih mehanizama kontrole i filtriranja sadržaja, kojima se sprečava pristup potencijalno malicioznim ili neovlašćenim veb lokacijama sa računara i uređaja koji se koriste za pristup Bolničkom informacionom sistemu i drugim IKT resursima [NAZIV FIRME]. Za uspostavljanje, konfigurisanje i redovno ažuriranje mehanizama filtriranja, kao i za nadzor nad njihovom efikasnošću, odgovoran je [IME ODGOVORNOG LICA], direktor. Postupanje zaposlenih prilikom korišćenja interneta i IT opreme, uključujući obaveze i ograničenja u vezi sa pristupom veb sadržajima, detaljnije je uređeno posebnim dokumentom — Politika prihvatljive upotrebe IT opreme.

Mera trenutno nije ispunjena, s obzirom na to da pristup zaposlenih potencijalno malicioznim veb sajtovima nije tehnički kontrolisan niti filtriran. Odsustvo ovakve kontrole povećava rizik od infekcije radnih stanica malverom, kompromitovanja pristupnih podataka i neovlašćenog pristupa Bolničkom informacionom sistemu putem veb vektora napada, što,

s obzirom na prirodu podataka koje [NAZIV FIRME] obrađuje, predstavlja povećan rizik po poverljivost zdravstvenih podataka pacijenata i kontinuitet pružanja zdravstvenih usluga.

Član 26. Zaštita od zlonamernog softvera (tačka 21. člana 10. stav 4. Zakona)

Zaštita svih uređaja u okviru IKT sistema [NAZIV FIRME] od zlonamernog softvera sprovodi se primenom odgovarajućeg antivirusnog i srodnog zaštitnog rešenja na svim radnim stanicama, serverima i drugim uređajima koji učestvuju u obradi podataka, uključujući i podatke iz medicinske dokumentacije pacijenata. Mera se primenjuje u punom obimu, na svim uređajima bez izuzetka, s obzirom na to da kompromitacija bilo kog uređaja može direktno ugroziti kontinuitet zakazivanja i vođenja medicinske dokumentacije, kao i poverljivost osetljivih zdravstvenih podataka. Za primenu i nadzor nad funkcionisanjem zaštite od zlonamernog softvera odgovoran je [IME ODGOVORNOG LICA], direktor. Procedura podrazumeva redovno ažuriranje definicija pretnji i zaštitnog softvera, kontinuiran rad zaštite u realnom vremenu na svim uređajima, kao i periodičnu proveru ispravnosti i pokrivenosti zaštite na celokupnoj IT infrastrukturi.

Član 27. Rezervne kopije podataka (tačka 22. člana 10. stav 4. Zakona)

Rezervne kopije podataka od značaja za zakazivanje i vođenje medicinske dokumentacije pacijenata izrađuju se redovno, u obimu koji obuhvata sve podatke neophodne za nesmetan nastavak pružanja zdravstvenih usluga u slučaju bezbednosnog incidenta ili gubitka podataka. Za organizovanje, sprovođenje i nadzor nad procesom izrade rezervnih kopija odgovoran je [IME ODGOVORNOG LICA], direktor [NAZIV FIRME]. Procedura izrade rezervnih kopija sprovodi se u unapred utvrđenim vremenskim intervalima, čime se obezbeđuje mogućnost oporavka podataka i kontinuitet ključnih poslovnih procesa [NAZIV FIRME].

Član 28. Čuvanje podataka o događajima (tačka 23. člana 10. stav 4. Zakona)

Evidencije (logovi) o aktivnostima u IKT sistemu [NAZIV FIRME] čuvaju se u propisanom obimu i redovno se proveravaju radi blagovremenog uočavanja bezbednosnih incidenata, sa posebnim naglaskom na aktivnosti koje se odnose na pristup medicinskoj dokumentaciji pacijenata. Evidencije se tehničkim i organizacionim merama štite od neovlašćene izmene ili brisanja, čime se obezbeđuje njihova pouzdanost kao dokaza u slučaju bezbednosnog incidenta. Za primenu ove mere, uključujući uspostavljanje postupka čuvanja i provere evidencija i kontrolu pristupa tim evidencijama, odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA], koji je zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti.

Mera trenutno nije ispunjena, jer evidencije o aktivnostima u IKT sistemu [NAZIV FIRME] ne čuvaju se i ne proveravaju redovno, niti su zaštićene od neovlašćene izmene ili brisanja. Imajući u vidu da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — zavisi od integriteta i poverljivosti podataka u IKT sistemu, odsustvo adekvatnog čuvanja i zaštite evidencija značajno otežava mogućnost pravovremenog otkrivanja neovlašćenih radnji i rekonstrukcije toka eventualnog bezbednosnog incidenta, čime se povećava rizik po poverljivost osetljivih zdravstvenih podataka i kontinuitet pružanja zdravstvenih usluga. Direktor ordinacije zadužen je za uspostavljanje tehničkih i organizacionih mera kojima će se ovo odstupanje otkloniti.

Član 29. Integritet softvera (tačka 24. člana 10. stav 4. Zakona)

Integritet softvera koji se koristi u okviru IKT sistema [NAZIV FIRME] obezbeđuje se primenom kontrole verzija i obaveznom potvrdom pre izvršenja trajnih izmena nad važnim podacima, uključujući medicinsku dokumentaciju pacijenata. Softver koji se koristi u poslovanju preuzima se isključivo iz pouzdanih, zvaničnih izvora, čime se sprečava unošenje neovlašćenih ili kompromitovanih komponenti u IKT sistem. Za primenu ove mere, uključujući nadzor nad izvorima preuzimanja softvera i kontrolom verzija, odgovoran je direktor i osnivač ordinacije, [IME ODGOVORNOG LICA]. Procedura podrazumeva da se svaka trajna izmena važnih podataka vrši uz prethodnu proveru i odobrenje, a da se instalacija ili ažuriranje softvera sprovodi isključivo preuzimanjem iz zvaničnih distributivnih kanala proizvođača.

Član 30. Zaštita od zloupotrebe slabosti (tačka 25. člana 10. stav 4. Zakona)

[NAZIV FIRME] redovnim ažuriranjem softvera i operativnih sistema sprečava zloupotrebu poznatih tehničkih slabosti na IKT sistemima koji podržavaju proces zakazivanja i vođenja medicinske dokumentacije pacijenata, uključujući sve mrežne uređaje koji su deo infrastrukture, kao što su mrežni štampači i skeneri. Za primenu ove mere, uključujući planiranje i sprovođenje ažuriranja softvera, operativnih sistema i perifernih mrežnih uređaja, odgovoran je direktor, [IME ODGOVORNOG LICA]. Procedura primene mere podrazumeva redovnu proveru dostupnosti bezbednosnih ažuriranja za operativne sisteme i softver, kao i proveru da su svi mrežni uređaji ažurirani i zaštićeni lozinkom pre njihovog uključivanja u mrežu.

[KLIJENT DA DOPUNI: status ažuriranosti i zaštite lozinkom mrežnih štampača/skenera, budući da je odgovor na ovo pitanje iz procene rizika označen kao „nedefinisano"]. Dok se ne utvrdi i dokumentuje stvarno stanje ovih uređaja, postoji mogućnost da neažurirani ili lozinkom nezaštićeni mrežni štampači/skeneri predstavljaju tačku ranjivosti kroz koju bi mogao biti ostvaren neovlašćen pristup mreži na kojoj se obrađuju osetljivi zdravstveni podaci pacijenata, što bi moglo ugroziti poverljivost medicinske dokumentacije i kontinuitet pružanja zdravstvenih usluga.

Član 31. Zaštita pri revizorskom testiranju (tačka 26. člana 10. stav 4. Zakona)

Testiranje IKT sistema [NAZIV FIRME], uključujući sisteme u kojima se obrađuje medicinska dokumentacija pacijenata, sprovodi se planski i periodično, pri čemu se tehnike i obim testiranja (uključujući testiranje penetracije) utvrđuju u skladu sa značajem sistema koji se testira i rizicima kojima je izložen. Testiranje se sprovodi tako da se ne ugrozi dostupnost, integritet i poverljivost podataka niti kontinuitet ključnih poslovnih procesa, posebno procesa zakazivanja i vođenja medicinske dokumentacije pacijenata, a pre sprovođenja testiranja definišu se njegov obim, metodologija i mere zaštite produkcionog okruženja. Za planiranje, odobravanje i nadzor nad sprovođenjem revizorskog testiranja odgovoran je direktor i osnivač ordinacije, [IME ODGOVORNOG LICA], koji ujedno prati usklađenost sprovedenih aktivnosti sa propisima o informacionoj bezbednosti.

Politika redovnog testiranja penetracije trenutno nije uspostavljena niti formalno usvojena, zbog čega mera nije ispunjena. Imajući u vidu da ključni poslovni proces zakazivanja i vođenja medicinske dokumentacije pacijenata zavisi od IKT sistema, odsustvo redovnog penetracionog testiranja povećava rizik od neotkrivenih ranjivosti čija bi eksploatacija mogla ugroziti dostupnost zdravstvenih usluga i poverljivost osetljivih zdravstvenih podataka pacijenata, te predstavlja bezbednosni rizik koji je potrebno otkloniti uspostavljanjem odgovarajuće politike testiranja.

Član 32. Zaštita podataka u mrežama (tačka 27. člana 10. stav 4. Zakona)

Mrežni saobraćaj i komunikacija koji obuhvataju prenos podataka o pacijentima, uključujući VPN konekcije i prenos fajlova, štite se primenom enkripcije kako bi se obezbedila poverljivost i integritet podataka u tranzitu. Ova mera primenjuje se na sve kanale komunikacije kojima se prenose osetljivi zdravstveni podaci iz medicinske dokumentacije pacijenata. Za primenu i nadzor nad ovom merom odgovoran je direktor [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedure primene enkripcije mrežnog saobraćaja sprovode se u skladu sa internim pravilima zaštite podataka u mrežama [NAZIV FIRME].

Status primene ove mere trenutno je nejasan, budući da ne postoje pouzdani podaci o tome da li je mrežni saobraćaj, uključujući VPN i prenos fajlova, u potpunosti zaštićen enkripcijom. Nedostatak jasnih dokaza o primeni enkripcije predstavlja rizik po poverljivost zdravstvenih podataka pacijenata koji se prenose mrežom, s obzirom na to da bi eventualni nedostatak zaštite omogućio neovlašćen uvid u osetljive medicinske podatke tokom prenosa, što bi imalo direktan uticaj na poverljivost podataka i na kontinuitet pružanja zdravstvenih usluga. [KLIJENT DA DOPUNI: tačan status primene enkripcije za VPN i prenos fajlova, korišćeni protokoli i dokazi o implementaciji].

Član 33. Bezbednost podataka u komunikaciji (tačka 28. člana 10. stav 4. Zakona)

Mrežni saobraćaj i komunikacija, uključujući VPN konekcije i prenos fajlova koji sadrže podatke iz medicinske dokumentacije pacijenata, štite se primenom enkripcije u obimu koji obuhvata sve kanale prenosa osetljivih zdravstvenih podataka van i unutar IKT sistema [NAZIV FIRME]. Za primenu i nadzor nad ovom merom odgovoran je direktor i osnivač ordinacije, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedure primene enkripcije mrežnog saobraćaja i prenosa fajlova sprovode se u skladu sa internim pravilima [NAZIV FIRME] o zaštiti podataka u komunikaciji.

Na osnovu dostupnih podataka iz procene rizika nije moguće utvrditi da li je i u kom obimu mrežni saobraćaj i prenos fajlova zaštićen enkripcijom, s obzirom na to da odgovor klijenta na relevantno pitanje glasi „ne znam“. [KLIJENT DA DOPUNI: status primene enkripcije za VPN konekcije i prenos fajlova, uključujući korišćene protokole i dokaz implementacije]. Imajući u vidu da se putem IKT sistema obrađuju osetljivi zdravstveni podaci pacijenata, nedostatak enkripcije u komunikaciji nosi visok rizik od neovlašćenog pristupa i povrede poverljivosti podataka tokom prenosa, što bi moglo direktno ugroziti kontinuitet pružanja zdravstvenih usluga i izložiti [NAZIV FIRME] pravnim i reputacionim posledicama.

Član 34. Zahtevi tokom životnog ciklusa (tačka 29. člana 10. stav 4. Zakona)

Zahtevi bezbednosti ugrađuju se u sve faze životnog ciklusa razvoja i izmene IKT sistema [NAZIV FIRME], uključujući nabavku, razvoj, testiranje i puštanje u produkcioni rad. Sve izmene na kritičnim sistemima, uključujući sisteme koji podržavaju zakazivanje i vođenje medicinske dokumentacije pacijenata, podležu proveri od strane drugog lica koje nije izvršilac izmene (princip „drugog para očiju"), kao i prethodnom testiranju u kontrolisanom okruženju pre primene na produkcionom sistemu. Podešavanja sistema proveravaju se u odnosu na definisane bezbednosne zahteve pre puštanja u rad. Za primenu ove mere, uključujući uspostavljanje procedura provere i testiranja izmena, odgovoran je [IME ODGOVORNOG LICA], direktor i osnivač ordinacije.

Mera trenutno nije ispunjena jer ne postoji uspostavljena procedura nezavisne provere kritičnih IT izmena, niti je definisan i dosledno primenjen proces testiranja i provere podešavanja pre puštanja sistema u produkcioni rad. Odstupanje predstavlja povećan rizik od neovlašćenih ili grešnih izmena na sistemima koji obrađuju osetljive zdravstvene podatke i podržavaju zakazivanje i vođenje medicinske dokumentacije pacijenata, što može dovesti do narušavanja integriteta podataka, prekida pružanja zdravstvenih usluga i povrede poverljivosti podataka pacijenata. [KLIJENT DA DOPUNI: rok do kog se planira uspostavljanje procedure provere „drugog para očiju" i testiranja izmena pre produkcije]

Član 35. Zaštita test podataka (tačka 30. člana 10. stav 4. Zakona)

Prilikom testiranja IKT sistema u [NAZIV FIRME] koriste se isključivo podaci koji ne sadrže stvarne lične, odnosno osetljive zdravstvene podatke pacijenata, a ukoliko se za potrebe testiranja neizbežno koriste podaci izvedeni iz produkcionog okruženja, isti se prethodno anonimizuju ili maskiraju na način koji onemogućava identifikaciju pacijenata. Za sprovođenje i nadzor nad primenom ove mere odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA]. Procedura primene podrazumeva proveru porekla i sadržaja test podataka pre svakog testiranja IKT sistema, kao i odobravanje njihove upotrebe od strane odgovornog lica.

[KLIJENT DA DOPUNI: konkretan opis postupka pripreme/anonimizacije test podataka koji se trenutno primenjuje, odnosno potvrda da li se za testiranje uopšte koriste podaci iz produkcionog okruženja]. Status primene ove mere ocenjen je kao nejasan, s obzirom na to da trenutno dostupni podaci ne omogućavaju utvrđivanje da li se u praksi test podaci posebno zaštićuju. Ovakva neizvesnost predstavlja potencijalni rizik po poverljivost osetljivih zdravstvenih podataka pacijenata, imajući u vidu da bi eventualno korišćenje stvarnih podataka u test okruženjima, koje po pravilu ima niži nivo zaštite od produkcionog, moglo da dovede do neovlašćenog pristupa ili curenja podataka. [NAZIV FIRME] će po pribavljanju potpunih podataka o postojećoj praksi testiranja ažurirati ovu odredbu Akta i, po potrebi, uspostaviti dodatne kontrole zaštite test podataka.

Član 36. Procedure čuvanja i brisanja (tačka 31. člana 10. stav 4. Zakona)

Podaci se čuvaju isključivo u rokovima propisanim zakonom i ugovornim obavezama, a po isteku tih rokova nepovratno se brišu, uključujući podatke kojima raspolažu angažovani provajderi usluga obrade podataka. Za sprovođenje procedura čuvanja i brisanja podataka, kao i za nadzor nad njihovom primenom kod trećih lica kojima se podaci poveravaju, odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA]. Pre uspostavljanja ili obnavljanja ugovornog odnosa sa provajderom koji obrađuje podatke [NAZIV FIRME], pribavlja se i proverava pisano objašnjenje načina na koji provajder trajno briše podatke po raskidu ugovora, a postupak nepovratnog brisanja internih podataka sprovodi se po isteku propisanog ili ugovorenog roka čuvanja za sve kategorije medicinske dokumentacije pacijenata.

Mera trenutno nije ispunjena jer se nepovratno brisanje podataka po isteku propisanog ili ugovorenog roka čuvanja ne sprovodi, a [NAZIV FIRME] ne raspolaže informacijama o načinu na koji angažovani provajder trajno briše podatke nakon raskida ugovora. [KLIJENT DA DOPUNI: razlog zašto procedura brisanja još nije uspostavljena i okvirni rok do kada se planira njeno uvođenje]. Ovo odstupanje izlaže [NAZIV FIRME] riziku neovlašćenog pristupa ili zadržavanja osetljivih zdravstvenih podataka pacijenata duže od dozvoljenog roka, što može dovesti do povrede poverljivosti podataka i neusklađenosti sa propisima o zaštiti podataka o ličnosti, a posredno i do ugrožavanja kontinuiteta procesa zakazivanja i vođenja medicinske dokumentacije.

Član 37. Zaštita sredstava dostupnih pružaocima (tačka 32. člana 10. stav 4. Zakona)

[NAZIV FIRME] obezbeđuje da pristup sredstvima i resursima koji su dostupni pružaocima usluga (dobavljačima i trećim stranama uključenim u rad IKT sistema) bude regulisan ugovorom koji sadrži odredbe o postupanju po zahtevu državnih organa, pružanju podrške u slučaju bezbednosnog incidenta i obradi ličnih podataka, u skladu sa primenljivim propisima. Detaljna pravila uređena su posebnim dokumentom — Politika upravljanja trećim stranama. Za primenu ove mere, uključujući zaključivanje i proveru ugovornih odredbi sa pružaocima usluga, odgovoran je direktor, [IME ODGOVORNOG LICA]. Procedura podrazumeva proveru postojećih i budućih ugovora sa pružaocima usluga radi utvrđivanja da li sadrže navedene odredbe, pre njihovog potpisivanja odnosno obnavljanja.

[KLIJENT DA DOPUNI: status i dokaz o tome da li su postojeći ugovori sa pružaocima usluga definisani u pogledu postupanja po zahtevu državnih organa, podrške u slučaju incidenta i obrade ličnih podataka; ukoliko nisu, navesti razloge i rok za usklađivanje]. S obzirom na to da ključni poslovni proces [NAZIV FIRME] — zakazivanje i vođenje medicinske dokumentacije pacijenata — zavisi od angažovanja pružalaca usluga u IKT sistemu, nedostatak jasno definisanih ugovornih odredbi o obradi ličnih podataka i postupanju u slučaju incidenta predstavlja rizik po poverljivost osetljivih zdravstvenih podataka i kontinuitet pružanja zdravstvenih usluga u slučaju bezbednosnog incidenta kod pružaoca usluge.

Član 38. Održavanje ugovorenog nivoa usluge (tačka 33. člana 10. stav 4. Zakona)

Nivo usluge ugovoren sa dobavljačima IKT usluga, uključujući cloud provajdere, prati se u obimu koji obezbeđuje neprekidnost ključnih poslovnih procesa [NAZIV FIRME] — pre svega zakazivanja pregleda i vođenja medicinske dokumentacije pacijenata. Za nadzor nad održavanjem ugovorenog nivoa usluge i za procenu mogućnosti zamene dobavljača bez štetnog uticaja na poslovanje odgovoran je [IME ODGOVORNOG LICA], direktor. Detaljna pravila u vezi sa izborom, ugovaranjem i praćenjem trećih strana, uključujući uslove za promenu provajdera usluga, uređena su posebnim dokumentom — Politika upravljanja trećim stranama.

Na osnovu dostupnih podataka nije utvrđeno da li bi [NAZIV FIRME] mogla da promeni cloud provajdera bez značajnog poremećaja poslovanja, s obzirom na to da odgovor na ovo pitanje u proceni rizika glasi „ne znam", što ukazuje na to da trenutno ne postoji jasno dokumentovana analiza zavisnosti od postojećeg provajdera niti plan za eventualnu migraciju. Ovakvo odsustvo jasnoće predstavlja rizik po kontinuitet poslovanja i dostupnost Bolničkog informacionog sistema u slučaju prestanka ili pogoršanja kvaliteta usluge dobavljača, naročito imajući u vidu osetljivost zdravstvenih podataka koji se obrađuju. [KLIJENT DA DOPUNI: analiza mogućnosti i uslova za promenu cloud provajdera,

uključujući procenu zavisnosti od postojećeg dobavljača i rok do kog će ova analiza biti sprovedena].

Član 39. Prevencija incidenata (tačka 34. člana 10. stav 4. Zakona)

[NAZIV FIRME] ovim aktom uspostavlja skup tehničkih i organizacionih mera prevencije bezbednosnih incidenata koje se primenjuju na sve IKT sisteme od posebnog značaja, uključujući zaštitu od napada uskraćivanjem usluga (DoS/DDoS), zaštitu od ransomver napada putem nepromenljivih rezervnih kopija i segmentacije mreže, kao i ugovorno definisanje postupanja po zahtevu državnih organa i pružanja podrške u slučaju incidenta od strane trećih lica. Za primenu i nadzor nad ovim merama odgovoran je direktor, [IME ODGOVORNOG LICA], kao lice odgovorno za nadzor nad informacionom bezbednošću i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Operativne procedure postupanja u slučaju incidenta uređene su posebnim dokumentom — Plan reagovanja na incidente, dok se mere prevencije iz ove tačke primenjuju kao dopuna tom dokumentu, sa ciljem sprečavanja nastanka incidenata pre njihove eskalacije.

Mera trenutno nije ispunjena, s obzirom na to da nije utvrđeno postojanje zaštite od DoS/DDoS napada, ne postoje specifične mere usmerene protiv ransomver napada (nepromenljive kopije podataka i segmentacija mreže), niti je ugovorima sa relevantnim trećim licima definisano postupanje po zahtevu državnih organa i pružanje podrške u slučaju incidenta. Imajući u vidu da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — u potpunosti zavisi od raspoloživosti IKT sistema, odsustvo mera prevencije ransomver napada i DoS/DDoS napada predstavlja visok rizik po kontinuitet pružanja zdravstvenih usluga i po poverljivost osetljivih zdravstvenih podataka pacijenata. Nedefinisanost ugovornih obaveza trećih lica u pogledu postupanja po zahtevu državnih organa i podrške u slučaju incidenta dodatno otežava blagovremeno i usklađeno reagovanje u slučaju nastanka bezbednosnog događaja. [KLIJENT DA DOPUNI: rok do kojeg se planira uspostavljanje zaštite od DoS/DDoS napada, mera protiv ransomver napada i ugovornog definisanja postupanja trećih lica].

Član 40. Kontinuitet poslova (tačka 35. člana 10. stav 4. Zakona)

Kontinuitet poslovnih procesa [NAZIV FIRME] obezbeđuje se merama planiranja oporavka i redundanse koje obuhvataju kritičnu IKT infrastrukturu, uključujući sisteme koji podržavaju zakazivanje i vođenje medicinske dokumentacije pacijenata. Detaljna pravila uređena su posebnim dokumentima — Planom kontinuiteta poslovanja (BCP) i Planom oporavka od katastrofe (DRP), koji definišu postupke oporavka u slučaju prirodnih nepogoda, kvara ključnog hardvera i softvera, kao i zamenu za ključne IT uloge u slučaju odsustva. Za uspostavljanje, sprovođenje i ažuriranje ovih planova, kao i za nadzor nad njihovom primenom, odgovoran je [IME ODGOVORNOG LICA], direktor. Rezervna internet/telekom veza obezbeđena je kao deo mere otpornosti na prekid primarne konekcije.

Plan oporavka u slučaju velike prirodne nepogode, plan zamene za ključne IT uloge, rezervna oprema za ključni hardver/softver, kao i mehanizam za uočavanje neuobičajene aktivnosti i plan za slučaj prestanka rada ključnog sistema trenutno nisu uspostavljeni, zbog čega mera nije u potpunosti primenjena. Odstupanje je posledica toga što [NAZIV FIRME] do sada nije formalizovala navedene segmente plana kontinuiteta poslovanja, iako je rezervna telekomunikaciona veza obezbeđena. S obzirom da ključni poslovni proces — zakazivanje i vođenje medicinske dokumentacije pacijenata — direktno zavisi od raspoloživosti IKT sistema, odsustvo plana oporavka od katastrofe, zamene za ključne IT uloge i mehanizma za detekciju prekida rada sistema predstavlja značajan rizik za kontinuitet pružanja zdravstvenih usluga i za zaštitu poverljivosti osetljivih zdravstvenih podataka u slučaju dužeg prekida ili gubitka ključnog osoblja. [KLIJENT DA DOPUNI: rok do kog se planira izrada i usvajanje nedostajućih segmenata BCP/DRP dokumentacije].

Član 41. Usvajanje dokumenata (tačka 36. člana 10. stav 4. Zakona)

[NAZIV FIRME] usvaja i primenjuje pisana uputstva za rad sa ključnim IKT sistemima, uključujući sisteme koji se koriste za zakazivanje i vođenje medicinske dokumentacije pacijenata, u obimu koji obuhvata sve zaposlene koji imaju pristup tim sistemima. Za izradu, usvajanje i ažuriranje ovih dokumenata odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA], koji je ujedno zadužen i za praćenje usklađenosti sa propisima o informacionoj bezbednosti. Procedura primene obuhvata izradu uputstava za rad sa ključnim sistemima, njihovo dostavljanje zaposlenima pre početka rada sa predmetnim sistemima i periodičnu proveru njihove usklađenosti sa aktuelnim stanjem sistema i poslovnih procesa.

[KLIJENT DA DOPUNI: da li pisana uputstva za rad sa ključnim sistemima postoje, u kom obimu i za koje sisteme, kao i dokaz o njihovoj izradi i dostavljanju zaposlenima]. Odgovor dobijen u postupku procene rizika ne pruža dovoljno podataka za utvrđivanje stvarnog stanja primene ove mere, usled čega postoji rizik da zaposleni u radu sa sistemom koji sadrži osetljive zdravstvene podatke pacijenata postupaju bez jasno definisanih pravila, što može negativno uticati na doslednost primene bezbednosnih kontrola i na poverljivost i integritet medicinske dokumentacije.

Član 42. Multifaktorska autentifikacija (tačka 37. člana 10. stav 4. Zakona)

Pristup ključnim sistemima [NAZIV FIRME], uključujući sisteme u kojima se obrađuju zdravstveni podaci pacijenata i podaci neophodni za zakazivanje i vođenje medicinske dokumentacije, obezbeđuje se primenom višefaktorske autentifikacije (MFA) kao obaveznog mehanizma kontrole pristupa. Za primenu ove mere, uključujući određivanje sistema na koje se MFA odnosi i nadzor nad njenim sprovođenjem, odgovoran je direktor ordinacije, [IME ODGOVORNOG LICA]. Postupci izdavanja, korišćenja i obnavljanja autentifikacionih kredencijala sprovode se u skladu sa posebnim dokumentom — Politika upravljanja lozinkama, koji detaljnije uređuje tehničke i organizacione aspekte autentifikacije korisnika.

Status primene ove mere je, na osnovu sprovedene procene rizika, ocenjen kao nejasan, s obzirom na to da odgovor dobijen u okviru procene rizika na pitanje o korišćenju višefaktorske autentikacije za pristup ključnim sistemima glasi „nedefinisano", čime nije utvrđeno da li je MFA tehnički implementirana na svim relevantnim sistemima niti u kom obimu. Dok se ovo stanje ne razjasni i dokumentuje, postoji rizik da pristup sistemima koji sadrže osetljive zdravstvene podatke i podatke o zakazivanju pacijenata bude zaštićen isključivo jednofaktorskom autentifikacijom, što bi, imajući u vidu prirodu podataka i zavisnost ključnih poslovnih procesa od ovih sistema, moglo značajno povećati izloženost neovlašćenom pristupu i ugroziti poverljivost i kontinuitet pružanja zdravstvenih usluga. [KLIJENT DA DOPUNI: tačan status primene MFA po sistemima, obim primene i rok do kada će stanje biti usaglašeno i dokumentovano].

Stupanje na snagu

Ovaj akt stupa na snagu danom usvajanja od strane nadležnog organa upravljanja Dr Tijana, a primenjuje se od narednog dana.

U _____, ____.____._____. godine

Broj: _____

M.P.

Ovlašćeno lice:

_____