Zdravstveni dom Brežice

Černelčeva cesta 8, 8250 Brežice
info@zd-brezice.si
07 4991 400
07 4991 450

Družini prijazno podjetje

Na podlagi člena 32 Splošne uredbe (EU) o varstvu podatkov (v nadaljevanju: Splošna uredba EU) ter 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 - UPB; v nadaljevanju: ZVOP-1) izdaja direktor **ZDRAVSTVENEGA DOMA BREŽICE**, Dražen Levojević, univ. dipl. prav.

PRAVILNIK
O ZAGOTAVLJANJU VARNOSTI OSEBNIH PODATKOV

I. SPLOŠNE DOLOČBE

1. člen
(področje urejanja)

(1) S tem pravilnikom se določajo organizacijski in tehnični postopki ter ukrepi za varnost osebnih podatkov v javnem zdravstvenem zavodu Zdravstveni dom Brežice (v nadaljevanju zavod) z namenom, da se **fizično prepreči slučajno ali namerno nepooblaščeno uničevanje, sprememba ali izguba** varovanih osebnih podatkov, ter **nepooblaščen dostop, uporaba, iznos, posredovanje ali druga obdelava** varovanih osebnih podatkov.

(2) S prilogo tega pravilnika se določajo tudi kategorije oseb, ki so odgovorne za določene zbirke osebnih podatkov, in osebe, ki lahko zaradi narave njihovega dela obdelujejo določene osebne podatke.

(3) **Namen** izvajanja tega pravilnika je zagotavljanje **informacijske varnosti**, ki pomeni varovanje:

- zaupnosti: varovanje podatkov pred razkritjem nepooblaščenim osebam ter zagotavljanje odgovornosti za njihova dejanja;
- celovitosti: varovanje podatkov pred neavtoriziranimi spremembami in zagotavljanje njihove verodostojnosti, točnosti, popolnosti in nespremenljivosti;
- razpoložljivosti: varovanje podatkov in sistema pred prekinitvami v delovanju ter zagotavljanje podatkov pooblaščenim uporabnikom v času, ko jih potrebujejo.

(4) Za **varovane osebne podatke** štejejo tisti podatki, glede katerih ni podane pravne podlage za razkritje podatka javnosti in se nanašajo na lastnosti, stanja ali razmerja fizičnih oseb oziroma posameznikov – pacientov, njihovih svojcev, uslužbencev zavoda (vključno z osebami, ki začasno opravljajo delo v zavodu), zunanjih pogodbenih sodelavcev in poslovnih strank ter obiskovalcev ne glede na obliko, v kateri so podatki izraženi in ne glede na vrsto nosilca osebnih podatkov (v nadaljevanju osebni podatki). Za osebne podatke gre takrat, če se podatki nanašajo na določenega ali vsaj določljivega posameznika, torej takrat, ko je možno na podlagi podatkov (neposredno) ali spremljajočih okoliščin in informacij (posredno) identificirati posameznika.

(5) Uslužbenci, ki pri svojem delu obdelujejo osebne podatke, **morajo biti seznanjeni** z osnovnimi pravili, ki jih določa veljavni zakon o varstvu osebnih podatkov, z vsebino tega pravilnika ter z drugimi internimi akti s področja varovanja informacij in zasebnosti. S tem pravilnikom morajo biti seznanjeni tudi pogodbeni obdelovalci in, če je to potrebno, drugi zunanji sodelavci zavoda.

2. člen
(drugi spremljajoči interni akti)

(1) Opis zbirk, katerih upravljavec je zavod in opis obdelav osebnih podatkov se vodi v interni **evidenci dejavnosti obdelave**, ki je **PRILOGA A** tega pravilnika, in ki se vodi v skladu z določbami 30. člena Splošne uredbe EU v papirni in elektronski obliki. Evidenca se ažurira glede na dejanske spremembe pri obdelavi osebnih podatkov. Odgovorne osebe so določene v tej evidenci.

(2) Zavod vodi ažurno **evidenco osebnih pooblastil (PRILOGA B** tega pravilnika), iz katerega je za vsakega uslužbenca oziroma delovno mesto razvidno, katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno **zbirko osebnih podatkov iz prejšnjega odstavka**. Po potrebi se določi tudi obseg dostopa oziroma omejitve, npr. administrativni podatki, osnovni podatki o pacientu, zdravstveni podatki, področne omejitve po specialnostih, branje in/ali zapisovanje podatkov. **Za sisteme Promedica, LABIS, IPPO, GRAD ter zobni RTG se vodi ažuren seznam uporabnikov oziroma pooblastil, ki je sestavni del PRILOGE B – ta seznam se vodi v samem sistemu in se po potrebi natisne.** Osebam se uporabniške pravice dodeljujejo glede na **dejanske potrebe delovnih zadolžitev** (*need to know* princip), ter se ob spremembi delovnih nalog ponovno preverijo ter po potrebi razširijo ali omejijo.

(3) **Druge priloge** tega akta, vključno s sprejetimi varnostnimi politikami so navedene v ustreznih členih oziroma poglavjih.

3. člen
(pojmovnik)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Zbirka osebnih podatkov - je vsak strukturiran (sistematično urejen) niz osebnih podatkov;
2. Obdelava osebnih podatkov - pomeni kakršnokoli ravnanje z osebnimi podatki. Kot obdelava štejejo zlasti zbiranje, pridobivanje, vpis, urejanje, shranjevanje, prilagajanje ali spreminjanje, priklic, vpogled, uporaba, razkritje s prenosom, sporočanje, širjenje ali drugo dajanje na razpolago, razvrstitev ali povezovanje, blokiranje, anonimiziranje, izbris ali uničenje;
3. Uslužbenci zavoda za potrebe tega pravilnika so:
   - zaposleni v zavodu,
   - zunanji pogodbeni sodelavci, ki imajo pravico opravljati delo v zavodu, vključno s praktikanti, pripravniki, specializanti ipd.,
   - posamezniki, ki v prostorih zavoda ali izven opravljajo delo za pogodbenega obdelovalca osebnih podatkov za zavod ter
   - člani sveta zavoda.
4. Uporabnik osebnih podatkov oziroma zunanji uporabnik - je fizična ali pravna oseba ali druga oseba javnega ali zasebnega sektorja, ki se ji posredujejo ali razkrijejo osebni podatki upravljavca. Po Splošni uredbi EU uporabnik ni javni organ, če gre za pridobitev podatkov na podlagi posamične

zahteve;

5. Nosilec osebnih podatkov - so vse vrste sredstev, na katerih so zapisani ali posneti osebni podatki, na primer papirni dokumenti, mape, spisi, računalniška oprema vključno z magnetnimi, optičnimi ali drugimi računalniški mediji (npr. strežniško diskovno polje, CD, DVD, USB ključki, prenosni diski), fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.

4. člen
(lokacijski domet določb)

Določbe tega pravilnika se uporabljajo za delovne prostore:

- **v glavni stavbi zavoda v Brežicah**,
- **v zobnih ambulantah: OŠ Artiče, OŠ Cerklje ob Krki, OŠ Dobova in OŠ Brežice, zobna ambulanta na Trdinovi 1, zobna ambulanta Bizeljsko in zobna ambulanta Pišece,**
- **v ambulanti v DSO Impoljca, enota Brežice in**
- **v ambulanti SNMP v Urgentnem centru Brežice**,

in sicer ob ustreznem upoštevanju specifik posameznih prostorov oziroma lokacije.

II. VAROVANJE PROSTOROV, NOSILCEV PODATKOV, STROJNE IN PROGRAMSKE OPREME

5. člen
(varovanje prostorov in nosilcev osebnih podatkov)

(1) **Varovana območja ali varovani prostori** so prostori, v katerih se trajno ali občasno nahajajo papirni in elektronski nosilci osebnih podatkov, strojna in programska oprema. Varovani prostori v zavodu so:

- ambulante ne glede na lokacijo in vrsto ter laboratorij,
- recepcija oziroma informacijski pult,
- pisarne, vključno s pisarnami kadrovske in računovodske službe,
- vsi arhivi zdravstvene dokumentacije in
- območje računalniškega informacijskega sistema in območje komunikacijskega sistema (strežniško-komunikacijska soba, vodi, delovne postaje, druga premična oprema, celotna oprema videonadzornega sistema).

(2) Varovani prostori morajo biti varovani tako, da je nepooblaščenim osebam onemogočen dostop do podatkov, in sicer s **stalnim nadzorstvom (prisotnostjo) zaposlenih**.

Kadar to ni mogoče (tj. ob kratkotrajni ali daljši odsotnosti zaradi delovnih obveznosti ali po zaključku dela), se varovanje zagotovi z naslednjimi ukrepi:

- **zaklepanje vseh dostopov (vrat)**,
- **zaklepanje** omar, pisalnih miz in podobno,
- **odstranitev nosilcev osebnih podatkov** z odprtih površin pisarniške opreme ali z drugih lahko dostopnih mest,
- **odjavljanje** iz informacijskega sistema ter **zaklepanje ali izklapljanje računalnikov**,
- **odstranitev nepooblaščenih oseb**.

(3) Pooblaščen dostop do varovanih prostorov je dopusten le v rednem delovnem času, izven

tega časa pa samo na podlagi dovoljenja ali ob vednosti direktorja, pomočnikov direktorja ali vodje notranje organizacijske enote ali osebe odgovorne za posamezno zbirko, ki se nahaja v varovanem prostoru.

(4) **Ključi** se ne puščajo v ključavnici v vratih na zunanji strani. Ključi se ne puščajo v ključavnicah omar ali predalnikov.

(5) Izven običajnega delovnega časa morajo biti:
- nosilci osebnih podatkov **pospravljeni** v omare, predale ali druge varne prostore,
- omare, predalniki in drugi varni prostori z nosilci osebnih podatkov **zaklenjeni**,
- računalniki in druga strojna oprema (npr. medicinski aparati, ki so hkrati nosilci osebnih podatkov) **izklopljeni ali fizično oziroma programsko zaklenjeni**.

(6) **Politika čiste mize**: Uslužbenci **ne smejo brez stalnega nadzora puščati nosilcev osebnih podatkov** (npr. papirna dokumentacija, zunanji diski, CD-ji, DVD-ji in USB ključi) na mizah, pultih, policah, stolih in drugih odlagalnih mestih odprtega tipa, ki so neposredno dostopni osebam, ki nimajo pravice do seznanitve.

(7) Uslužbenci, ki pri izvajanju svojih delovnih nalog kopirajo ali tiskajo dokumente, ki vsebujejo osebne podatke, na napravah, ki jih uporablja večje število zaposlenih, **po končanem kopiranju ali tiskanju ne smejo puščati dokumentov v, na ali ob napravah**.

(8) **Nosilci osebnih podatkov se ne smejo hraniti izven varovanih prostorov**, tj. izven prostorov, ki se zaklepajo ali so pod stalnim nadzorom uslužbencev. Izven varovanih prostorov je dopustna le začasna hramba ali druga obdelava zaradi potreb delovnega procesa.

(9) Vhodna vrata, vrata v posamezne prostore uprave, strežniško-komunikacijsko sobo, posamezne ambulante ter druge varovane prostore so varovani s **klasičnimi ključavnicami**, zadnji uslužbenski vhod tudi z elektronsko ključavnico na čip. Biometrijski ukrepi se ne izvajajo. Ključi se dodeljujejo po principu *»need to use«*. **Vsa vrata se morajo sistematično in brezpogojno zapirati oziroma zaklepati, če v prostorih ni zagotovljenega učinkovitega nadzora.**

(10) **Zaklepanje vrat ob kakršnikoli odsotnosti je obvezno tudi za informacijsko pisarno (sprejemnico)**.

(11) Uslužbenci morajo neznane obiskovalce, ki prihajajo, se nahajajo ali odhajajo iz prostorov, ki običajno niso namenjeni obiskovalcem, ali ki se pojavljajo ob neobičajnem času ali brez nadzorstva, **povprašati po namenu obiska oziroma zadrževanja** v prostorih, jih ustrezno napotiti in v primeru sumljivih okoliščin takoj obvestiti vodstvo.

(12) Uslužbenci **ne smejo nosilcev osebnih podatkov odnašati izven prostorov** zavoda, razen kadar gre za zakonito posredovanje dokumentacije drugemu uporabniku ali kadar je to, na podlagi dovoljenja ali vednosti vodstva ali drugih pooblaščenih uslužbencev, neizogibno potrebno za zagotovitev izvajanja delovnih nalog.

(14) Zavod zagotavlja predpisano **požarno varnost** v sodelovanju z zunanjim pogodbenikom.

(15) Zavod zagotavlja tehnično varovanje z **alarmom** s povezavo na zunanjo varnostno službo za potrebe intervencij. Zavod na ključnih mestih izvaja tudi **videonadzor v skladu s sklepom o uvedbi**

videonadzora (december 2020), ki se šteje kot sestavni del tega pravilnika.

(16) *Tekoča (aktivna) zdravstvena dokumentacija* se hrani po ambulantah, v **kovinskih kartotečnih omarah s ključavnicami**. *Kadrovska in računovodska dokumentacija* se hranita v **zaklenjenih kovinskih arhivskih omarah v upravi zavoda** in v posebnem arhivskem prostoru.

(17) **Glede prevzemov oziroma oddaj ključev se vodi evidenca**.

(18) Na lokalnih postajah (računalnikih) se **ne sme nameščati datotek z osebnimi podatki ali zbirk osebnih podatkov.** Smiselno **enako velja za skupne mape, ki so dostopne vsem notranjim uporabnikov**. Izjeme so:

- lokalni računalniki za posebne potrebe z vednostjo in odobritvijo pooblaščene osebe, pristojne za informatiko,
- nujne začasne datoteke, ki pa morajo biti takoj odstranjene, tudi iz koša ter
- lastni osebni podatki, za katere je uporabnik odgovoren sam.

(19) Na kakršni koli »oglasni ali informacijski deski« ali na podobnih površinah, ki so redoma dostopne pacientom in drugim obiskovalcem, ne sme biti objavljenih osebnih podatkov (npr. morebitni seznami oziroma razporedi pacientov), razen osebnih podatkov, ki se nanašajo na zaposlene in so izpolnjeni pogoji za javno objavo po zakonu, ki ureja dostop do informacij javnega značaja.

6. člen
(prostori z osrednjo informacijsko in komunikacijsko opremo)

V tehnični oziroma strežniški sobi, v kateri je nameščena osrednja informacijska in komunikacijska oprema za obdelavo osebnih podatkov (strežnik, diskovne enote, usmerjevalniki in podobno), poleg drugih pravil, določenih s tem pravilnikom, veljajo še naslednja pravila:

- **zadrževanje uslužbencev** v teh prostorih, razen tistih, ki v njih opravljajo svoje delovne obveznosti, **ni dovoljeno**;
- **obiski zunanjih vzdrževalcev opreme ali drugih pogodbenih strank** (npr. za čiščenje, inštalacijska, elektro in obnovitvena dela) so dovoljeni na **poziv ali z vednostjo vodstva**;
- **prepovedna** je kakršnakoli uporaba **odprtega ognja**;
- **prepovedana** je hramba **vnetljivih materialov**;
- vsi vhodi morajo biti **stalno zaklenjeni**;
- prostori morajo biti zavarovani pred škodljivim fizičnim delovanjem (izlitje vode, požar, ipd.);
- oprema mora biti nameščena v skladu s pogoji, ki so skladni s tehničnimi specifikacijami opreme.

7. člen
(monitorji in zaklepanje računalnikov)

(1) V prostorih, ki so namenjeni poslovanju s pacienti, morajo biti računalniški **monitorji nameščeni tako, da nepooblaščene osebe nimajo vpogleda vanje**, če se obdelujejo osebni podatki. Izjeme so :

- če se v času prisotnosti druge osebe obdelujejo le osebni podatki te osebe;
- če zahteve po zdravem in ergonomskem delovnem mestu tega objektivno ne dopuščajo;
- če velikost in ureditev prostora tega objektivno in brez nesorazmernih stroškov ne dopušča.

V primeru iz zadnjih dveh alinej, je treba nedostopnost podatkov omogočiti kako drugače (npr. programske rešitve, fizično prekrivanje, obračanje monitorja ipd.).

(2) Vse delovne postaje morajo imeti vklopljeno funkcijo **avtomatskega zaklepanja računalnika ali monitorja**, ki se vklopi po določenem času neaktivnosti. Čas neaktivnosti je odvisen od frekvence rabe delovne postaje, narave dela, obstoja drugih varnostnih mehanizmov in narave osebnih podatkov, ki se obdelujejo, in ne sme biti daljši kot 15 minut. Standardni čas neaktivnosti je 5 minut.

8. člen
(vzdrževanje opreme)

Vzdrževanje in popravila strojne računalniške in druge opreme lahko izvaja **informatik zavoda ali po navodilih oziroma z vednostjo vodstva ali informatika zavoda zunanji pogodbeni vzdrževalec**, če ima z zavodom sklenjeno tudi pogodbo o obdelavi osebnih podatkov.

9. člen
(zadrževanje drugih oseb v varovanih prostorih)

(1) Vzdrževalci prostorov, strojne in programske opreme, obiskovalci, pacienti in pogodbene stranke se smejo gibati v varovanih prostorih samo z **upravičenim namenom** in **ob prisotnosti** vsakokrat pooblaščenega uslužbenca ali izjemoma vsaj z **dovoljenjem oziroma vednostjo** vodstva ali drugega pooblaščenega uslužbenca zavoda.

(2) Uslužbenci, ki ne izvajajo strokovnih nalog v zvezi z zbirkami osebnih podatkov, se lahko izven delovnega časa oziroma brez prisotnosti pooblaščenega uslužbenca zavoda gibljejo samo z upravičenim namenom in v tistih varovanih prostorih, kjer jim je praviloma (če je to objektivno možno zagotoviti) onemogočen vpogled v osebne podatke (nosilci podatkov so shranjeni v zaklenjenih omarah in pisalnih mizah, računalniki in strojna oprema pa izklopljeni ali kako drugače fizično ali programsko zaklenjeni).

III. POSEBNE DOLOČBE O VAROVANJU SISTEMSKE IN APLIKATIVNO PROGRAMSKE RAČUNALNIŠKE OPREME

10. člen
(omejitev dostopa)

(1) Lokalni ali oddaljeni dostop do programske opreme se dovoli v skladu z 8. členom tega pravilnika.

(2) Uslužbencem se lahko omogoči oddaljen dostop do službene elektronske pošte ali zbirk osebnih podatkov preko **VPN šifrirane povezave (uporaba sistemov za varni dostop) in z uporabo varnih metod za avtorizacijo in avtentikacijo**.

(3) Varen oddaljen dostop se prek terminalskega strežnika omogoči tudi zunanjim ambulantam (gl. 4. člen Pravilnika).

(4) Če službeni notesniki, ki jih uslužbenci za službene potrebe iznašajo iz službenih prostorov vsebujejo osebne podatke pacientov, se diske praviloma programsko **šifrira**. Enako velja za morebitne službene/zasebne USB ključke in prenosne diske.

(5) Pri večjih prenosih celotnih zbirk podatkov o pacientih (npr. sprememba lokacije hrambe, začasne baze, strežniške kopije podatkov) se podatke praviloma programsko **šifrira ali vsaj psevdonimizira**.

11. člen
(omejitev poseganja v opremo)

(1) Popravljanje, spreminjanje in dopolnjevanje sistemske in aplikativne programske opreme se dovoli v skladu z 8. členom tega pravilnika.

(2) Izvajalci morajo spremembe in dopolnitve sistemske in aplikativne programske opreme ustrezno dokumentirati.

(3) **Zaposleni uslužbenci zavoda nimajo administratorskih pravic**, z izjemo informatika zavoda.

12. člen
(uporaba drugih določb)

Za shranjevanje in varovanje aplikativne programske opreme veljajo enaka pravila, kot za ostale podatke iz tega pravilnika.

13. člen
(varstvo pred računalniškimi virusi, drugo zlonamerno programsko opremo in vdori)

(1) Vsebina diskov mrežnega strežnika in lokalnih delovnih postaj, kjer se nahajajo osebni podatki, se **sprotno preverja glede prisotnosti računalniških virusov in zlonamernih kod**. Ob pojavu neželenih pojavov se te čim prej odpravi s pomočjo informatika zavoda ali pogodbenega vzdrževalca opreme, obenem pa se ugotovi vzrok pojavov ter se izda navodilo za preprečitev podobnih varnostnih dogodkov.

(2) Vsi osebni podatki in programska oprema, ki so namenjeni uporabi v računalniškem informacijskem sistemu in prispejo v zavod na medijih za prenos računalniških podatkov ali preko telekomunikacijskih kanalov, morajo biti **pred uporabo preverjeni glede prisotnosti zlonamerne programske opreme**, zlasti če gre za vire (upravljavce), s katerimi zavod nima vzpostavljenih rednih ali zaupnih stikov.

(3) Uslužbenci morajo, če sumijo, da na informacijskem sistemu deluje zlonamerna programska oprema, **takoj prenehati delati z njim in obvestiti vodstvo**. Uslužbenci **ne smejo zaganjati sumljive elektronske pošte, programske opreme, ki ni del notranjega informacijskega sistema**. Uslužbenci prav tako **ne smejo zaganjati sumljivih dokumentov (npr. dokumentov na tujih nepreverjenih pomnilniških medijih, priponk v sumljivi elektronski pošti)**. Tako opremo oziroma dokumente je treba na varen način preveriti, ali obstaja okuženost z zlonamerno programsko opremo.

(4) V informacijskem sistemu zavoda mora biti nameščen:
- **protivirusni program;**
- **požarni zid novejšega tipa;**

- ***anti-spyware, anti-adware, anti-grayware* zaščita;**
- ***anti-spam* filter;**
- **sistem poročanja o varnostnih incidentih.**

Uporabljena programska oprema za zaščito pred zlonamerno programsko opremo se mora redno posodabljati, prav tako pa se mora redno izvajati pregledovanje trdih diskov in prenosnih medijev.

(5) Brezžični dostop do interneta mora biti omejen (geselni dostop).

(6) Podrobne tehnične specifikacije konkretnih varnostnih rešitev se določi v dokumentih pogodbenega vzdrževalca programske in strojne opreme. **Varnostno politiko na področju informacijske varnosti sestavljajo ta pravilnik in tehnične specifikacije rešitev, ki so bile implementirane**.

14. člen
(nameščanje nove opreme)

Uslužbenci **ne smejo sami nameščati programske in pomembne stacionarne strojne opreme** brez vednosti ali sodelovanja osebe, zadolžene za delovanje računalniškega informacijskega sistema (informatika zavoda ali zunanjega vzdrževalca). Prav tako ne smejo odnašati programske in pomembne stacionarne strojne opreme iz prostorov zavoda brez odobritve ali vednosti pooblaščene osebe.

15. člen
(dodeljevanje, uporaba in varovanje gesel)

(1) Dostop do podatkov preko aplikativne programske opreme se varuje s sistemom gesel za avtorizacijo in identifikacijo uporabnikov programov oziroma podatkov.

(2) Sistem gesel mora omogočati tudi možnost naknadnega ugotavljanja, kdaj so bili posamezni osebni podatki vneseni v zbirko podatkov, uporabljeni ali drugače obdelovani ter kdo je to storil.

(3) V zavodu velja naslednja **politika gesel:**

- Geslo uporabnika sistema je namenjeno samo njegovi uporabi, zato so uporabniki sistemov odgovorni za vse akcije, ki se zgodijo z uporabo njihove identitete;
- Uslužbenci s svojimi osebnimi gesli ravnajo kot s strogo zaupnimi informacijami in jih ne smejo razkrivati oziroma posojati drugim osebam, niti ožjim sodelavcem. Če uslužbenec zasledi malomarno ali zlonamerno ravnanje z gesli, to takoj sporoči vodstvu;
- Geslo mora uporabnik spremeniti takoj, če obstaja sum na razkritje gesla;
- Geslo ne sme vsebovati: besed iz slovarja, imen in priimkov uslužbenca in družinskih članov ali drugih pojmov, ki so v tesni osebni zvezi z uporabnikom, katerekoli oblike datuma, imena, oznake ali številke zavoda, zaporednih števil, enakih znakov kot uporabniška imena, in tudi ne očitnih, pogosto uporabljenih oziroma ustaljenih besed ali znakov (npr. »Brežice«, »pacient«, »geslo«, »geslo1«, »računalnik«, »vstop«, »odpri«, »password«, »123abc«, »321cba«, »00000«, »11111«, »zdbrežice«, »zdb123«, »ambulanta« in podobno;
- Gesla morajo biti sestavljena iz črk in številk in so dolga najmanj 8 znakov, kar zlasti velja za program Promedica, druge programske rešitve, namenjene zdravstveni oskrbi (npr. IPPO, LABIS in zobni RTG) ter za računovodsko ter kadrovsko zbirko oziroma program (GRAD);
- Hramba gesel v neberljivi obliki se izvaja v podatkovnih bazah IS, do katerega ima dostop pooblaščeni informatik;

- Za različne namene se ne uporablja enakih gesel;
- Začasna gesla je uslužbencem treba pošiljati oziroma izročati na varen način. Pooblaščeni informatik zavoda, ki je odgovoren za dodelitev začasnega gesla, uslužbencu sporoči geslo, ki ga uslužbenec spremeni ob prvi prijavi;
- Če uslužbenec geslo pozabi, mu pooblaščeni informatik zavoda dodeli novo začasno geslo, ki ga uporabnik spremeni ob prvi prijavi;
- Gesla zaposleni ne smejo zapisovati na papir ali shranjevati na kakršenkoli drug način, ki bi drugi osebi lahko omogočil dostop do gesla;
- Ni dovoljeno sporočanje gesel sodelavcem (razen izjemoma za potrebe zagotovitve nemotenega poslovanja po predhodnem dogovoru) in pošiljanje gesel po e-pošti;
- Za administratorska gesla veljajo enaka pravila. Ta gesla se, skupaj z uporabniškim imenom, hranijo tudi v zaprti kuverti (tako, da odpiranje brez poškodb ni možno) na varnem in skritem mestu, kjer je onemogočen dostop nepooblščenim osebam. Na kuverto se zapiše ime sistema oziroma aplikacije in datum zadnje spremembe ter podpis uporabnika. Nujno odprtje kuverte se zabeleži na sami kuverti (razlog, datum, osebno ime), ki se jo še naprej hrani.

(4) Računalniška gesla morajo uslužbenci **spreminjati na 3 mesece**, pri čemer se sistem programsko nastavi na **avtomatsko opominjanje** na spremembo gesla. Sistem je lahko nastavljen le na opominjanje ali praviloma na predhodno opominjanje z ukinitvijo veljavnosti gesla po poteku roka za spremembo.

(5) Uvedba **skupinskih uporabniških pravic v zavodu ni dovoljena**.

(6) Uporabniških imen in gesel ni treba uporabljati le za dostope do zbirk, aplikacij oziroma sistemov, ki ne vsebujejo osebnih podatkov.

16. člen
(uporaba programa Promedica, drugih programskih rešitev za podporo zdravstveni oskrbi LABIS, IPPO in zobni RTG ter računovodskega/kadrovskega programa GRAD)

(1) Vsak uporabnik se mora v program prijaviti s **svojim uporabniškim imenom in geslom**.

(2) Po zaključku delovnega dne, ob menjavi uporabnikov iste delovne postaje ali ob daljši odsotnosti uslužbenca med delovnim časom, se mora uslužbenec **odjaviti** iz sistema.

(3) **Vpogled in druga uporaba osebnih podatkov, ki jih uslužbenec ne potrebuje za opravljanje dela (nenamenski vpogledi in obdelava) je prepovedana** in predstavlja prekršek na področju varstva osebnih podatkov.

(4) Prejšnji odstavek velja tudi za dokumentarno gradivo (zdravstveno in računovodsko dokumentacijo), ki se vodi v papirni obliki.

(5) Praktikantom, specializantom ali študentom se v informacijskih sistemih dodelijo **ločene uporabniške pravice** od mentorjevih, vendar le tiste, ki so neizogibno potrebne za izvajanje zakonitih nalog po pogodbi.

17. člen
(varnostne kopije podatkov)

(1) Za potrebe restavriranja računalniškega sistema ob okvarah in ob drugih izjemnih situacijah se

zagotavlja **redna izdelava kopij vsebine mrežnega strežnika in lokalnih postaj**, če se podatki na teh nahajajo.

(2) Podatki se arhivirajo dnevno na zunanji lokaciji.

18. člen
(zagotavljanje sledljivosti v informacijskih sistemih)

(1) **Interni informacijski sistemi zagotavljajo sledljivost** obdelave podatkov, in sicer tako, da je omogočeno poznejše ugotavljanje, kdaj so bili posamezni osebni podatki vneseni v zbirko, uporabljeni ali kako drugače obdelani (npr. posredovani, vpogledani, spremenjeni) in kdo je to storil.

(2) Popolne sledljivosti z beleženjem dostopov, sprememb podatkov ter beleženjem tako izvornih kot popravljenih podatkov (beleženje kdo in kdaj je dostopal do podatka, ga spreminjal, kakšen je bil prvotni podatek in v kaj je bil popravljen), ni potrebno zagotavljati.

(3) Pri poizvedbah po seznamih s prikazom več zadetkov (npr. ko se kot iskalni kriterij uporabi ime, ki pripada več pacientom) se sledljivost zagotavlja tako, da se poizvedba zabeleži pri vsakem od pacientov, katerega osebni podatki so bili prikazani v določenem trenutku na izhodni enoti (pri posamezniku se mora zabeležiti, kdo in kdaj je s pomočjo poizvedbe dostopal do osebnih podatkov posameznika). Sledljivost se lahko zagotavlja tudi tako, da se beleži rezultat poizvedbe v času (zabeleži se, kdo je izvedel poizvedbo, kdaj in kakšen je bil rezultat poizvedbe v tem času).

(4) Podatki o sledljivosti (dnevnik sledljivosti ali *log file*) se **hranijo neomejeno vendar ne manj kot 5 let.**

19. člen
(posebna pravila za videonadzor – nadzor nad registratorji delovnega časa)

Nadzor nad registratorji delovnega časa je uveden na podlagi **Sklepa o uvedbi videonadzora (2018), ki se šteje kot sestavni del tega pravilnika**. Sklep vsebuje pravila o podlagi, namenu, uvedbi, izvajanju, hrambi podatkov, omejitvah pri dostopu oziroma pri uporabi posnetkov in o evidentiranju vpogledov ter o zavarovanju sistema.

IV. UPORABA E-POŠTE IN INTERNETA

20. člen
(elektronska pošta in uporaba druge programske opreme na računalniku)

(1) Računalniki in elektronska pošta se uporabljajo v službene namene.

(2) Ne glede na prejšnji odstavek se elektronska pošta in ostala programska oprema na računalniku lahko uporabljata v omejenem obsegu in razumnih mejah (tj. v obsegu, ki ne moti delovnega procesa) tudi v zasebne namene. Vsebina elektronske pošte v zasebne namene ne sme biti neprimerna ali žaljiva.

(3) Pooblaščeni uslužbenec, zadolžen za delovanje računalniškega informacijskega sistema (informatik zavoda ali pogodbenik), lahko na posebej utemeljeno pisno zahtevo uprave zavoda, v

prisotnosti še dveh članov komisije, **v izrednih primerih (nenadna odpoved delavca oziroma dolgotrajna odsotnost delavca brez kontaktov, smrt delavca ali drug izreden dogodek) vpogleda v delavčevo vhodno ali izhodno elektronsko pošto** le, če je to neizogibno in nujno potrebno za vodenje delovnega procesa oziroma poslovanje zavoda, ker bi sicer lahko nastala nepopravljiva škoda. Primarno se vpogleda le v prometne podatke (pošiljatelj/prejemnik, naslov sporočila, velikost in ime priponke, čas), izjemoma pa tudi vsebino domnevno relevantnih e-sporočil. Vpogledi se izvajajo le v sporočila, za katere se upravičeno domneva, da so službene narave, ter da je njihova vsebina v skladu z razlogi za uvedbo pregleda pošte. Tričlansko komisijo imenuje direktor. V njej mora biti vsaj en predstavnik zaposlenih, ki ni vodstveni delavec. O vpogledu mora komisija napisati zapisnik.

(4) Če se pojavi utemeljen sum, da uslužbenci ne spoštujejo omejitev iz drugega odstavka tega člena, lahko pooblaščeni uslužbenec, zadolžen za delovanje računalniškega informacijskega sistema (informatik zavoda ali pogodbenik), na posebej utemeljeno pisno zahtevo direktorja opravi nadzor količine uporabe elektronske pošte, praviloma z vidika obsega priponk, ki obremenjujejo strežnik. Pri tem se ne sme pregledovati drugih prometnih podatkov (razen skupnega števila prejetih ali oddanih sporočil) in vsebine elektronske pošte.

(5) Šteje se, da je z objavo tega pravilnika uslužbenec na primeren način obveščen o namenu uporabe elektronske pošte in ostale programske opreme iz prvega in drugega odstavka tega člena ter o možnosti nadzora iz tretjega in četrtega odstavka tega člena.

(6) Vpogled v telefonske prometne podatke priključkov, katerih lastnik je zavod, lahko zavod zahteva od operaterjev telekomunikacijskih storitev le takrat, kadar pride med zavodom in uslužbencem do kakršnegakoli spora glede višine stroškov porabe konkretnega telefonskega priključka. Zavod nikoli ne sme preverjati identitete oziroma lastništva klicanih ali klicočih številk.

(7) Ob prenehanju delovnega razmerja ali drugega pogodbenega razmerja se uslužbencu **ukinejo vse uporabniške pravice** v informacijskem sistemu oziroma na računalniku. Ukinitev se izvede najkasneje naslednji delovni dan po dnevu prenehanja razmerja. Uslužbenec ima možnost, da pred prenehanjem delovnega razmerja z računalnika in druge opreme izbriše ali kopira zasebno pošto in zasebne datoteke, prav tako lahko kopira osebne podatke, ki se nanašajo nanj. Po izbrisu oziroma kopiranju ali izjavi uslužbenca, da pravice ne bo izkoristil, ima zavod pravico, da se vsi za zavod nepotrebni podatki in nepotrebna elektronska pošta nepovratno izbriše.

(8) V primeru iz prejšnjega odstavka, **preusmeritev e-pošte na drugega uslužbenca ni dopustna**, pač pa se pošiljatelju samodejno sporoči, da predal ni aktiven in kakšen je nov naslov za pošiljanje.

Internet
21. člen

(1) Internet se uporablja v službene namene.

(2) Ne glede na prejšnji odstavek se internet lahko uporablja v omejenem obsegu in razumnih mejah tudi v zasebne namene. Internetne strani, ki se pregledujejo v zasebne namene, ne smejo biti z neprimerno ali žaljivo vsebino.

(3) Zavod lahko odredi blokado določenih spletnih strani, zaradi obiskovanja katerih bi lahko bil moten delovni proces ali učinkovitost dela v zavodu.

(4) **Intranet** v zavodu lahko omogoča neposreden odprt dostop le do nevarovanih oz. javnih osebnih podatkov uslužbencev zavoda (npr. osebna imena, nazivi, funkcije oz. delovna mesta, naloge, kontaktni podatki ipd. kar je tesno povezano z delovnim razmerjem in porabo javnih sredstev).

(5) Ob uvedbi **elektronskega naročanja** prek spletne strani zavoda mora biti pot podatkov **šifrirana** (https protokol). V primeru **naročanja prek e-pošte**, povratna sporočila pacientom ne smejo vsebovati konkretnih podatkov o zdravstvenem stanju, pač pa le osnovne podatke o naročeni storitvi (npr. zdravnik, ambulanta, čas, razna splošna navodila).

V. STORITVE, KI JIH PRI OBDELAVI OSEBNIH PODATKOV OPRAVLJAJO ZUNANJE PRAVNE ALI FIZIČNE OSEBE

22. člen
(pogodbena obdelava osebnih podatkov)

(1) Z vsako zunanjo pravno ali fizično osebo, ki za (v imenu) oziroma namesto zavoda opravlja posamezna opravila v zvezi obdelovanjem osebnih podatkov (pogodbeni obdelovalec), se sklene pisna pogodba o pogodbeni obdelavi osebnih podatkov v skladu s 28. členom Splošne uredbe EU, kot samostojni akt ali kot del temeljne pogodbe. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

(2) Vzorec pogodbe o obdelavi osebnih je **PRILOGA C** tega pravilnika.

(3) O pogodbenih obdelovalcih se vodi seznam na obrazcu, ki je **PRILOGA D** tega pravilnika.

VI. SPREJEM IN EVIDENTIRANJE VHODNIH DOKUMENTOV

23. člen
(ravnanje z vhodno pošto)

(1) Uslužbenec, ki je zadolžen za sprejem in morebitno evidentiranje vhodne pošte, lahko odpira in z namenom evidentiranja ter nadaljnjega posredovanja pregleduje vso vhodno pošto (tudi tisto, ki jo prinesejo pacienti, njihovi svojci ali kurir), razen v primeru iz drugega odstavka tega člena.

(2) Uslužbenec, ki je zadolžen za sprejem in evidenco vhodne pošte, **ne odpira**:
- pošiljk, ki so naslovljene na drugo organizacijo in so pomotoma dostavljene,
- pošiljk, na katerih je označba, da vsebujejo občutljive osebne podatke, neposredni naslovnik (uslužbenec ali notranja organizacijska enota) pa je jasno naveden,
- pošiljk, za katere iz označb na ovojnici izhaja, da se nanašajo na razpis,
- pošiljk, naslovljenih na določenega uslužbenca, pri čemer je na ovojnici jasno zapisana klavzula osebne vročitve (»vročiti osebno«, »osebno v roke«, ipd.),
- pošiljk, naslovljenih na določenega uslužbenca, pri čemer je na ovojnici jasno navedeno osebno ime delavca brez označbe njegovega delovnega mesta ali funkcije v zavodu, hkrati pa je osebno ime navedeno pred nazivom zavoda,
- pošiljk naslovljenih na določenega uslužbenca, ki se po posebnih predpisih (npr. v

kazenskem, pravdnem in upravnem postopku) vročajo osebno.

VII. POSREDOVANJE OSEBNIH PODATKOV ZUNANJIM UPORABNIKOM IN NOTRANJA SLEDLJIVOST ZA ARHIV

24. člen
(splošno o načinu posredovanja)

(1) Osebne podatke je dovoljeno prenašati z informacijskimi, telekomunikacijskimi in drugimi sredstvi (npr. klasična pošta, kurir) le ob izvajanju postopkov in ukrepov, ki nepooblaščenim osebam preprečujejo odvzem, uničevanje in spreminjanje osebnih podatkov ter preprečujejo neupravičeno seznanjanje z njihovo vsebino.

(2) Dokumenti z osebnimi podatki se pošiljajo v **zaprtih ovojnicah**. **Na ovojnicah so lahko zapisani le podatki, ki so nujni za poštno dostavo pošiljke – na ovojnici ali prek prozornega okenčka ne sme biti razvidnih drugih osebnih podatkov** (npr. interna številka pacienta, vrsta storitve, rojstni datum, ZZZS številka, datum storitve, opis vsebine dokumenta).

(3) Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da **ni omogočeno**, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnice z običajno lučjo **vidna vsebina ovojnice**. Prav tako mora ovojnica zagotoviti, da **odprtja ovojnice in seznanitve z njeno vsebino ni mogoče izvesti brez vidne sledi odpiranja ovojnice**.

(4) Pošiljanje poštnih pošiljk na način »**priporočeno s povratnico**« se praviloma izvaja:
- če gre za pošiljanje večjega števila pomembnih dokumentov ali
- če gre za pošiljanje originalne zdravstvene dokumentacije (zdravstvenih kartonov).

(5) Zdravstvena dokumentacija se ZZZS-ju pošilja praviloma po kurirju; MDPŠ-ju, ZPIZ-u in drugim institucijam pa po klasični pošti ali kurirju. Če gre za pošiljanje po kurirju, se mora zagotavljati enako učinkovita sledljivost, kot velja za klasično pošto.

25. člen
(posredovanje občutljivih oziroma posebnih kategorij osebnih podatkov po e-pošti)

Če se osebni podatki, ki razkrivajo:
- zdravstveno stanje (anamneza, terapija/zdravstvene storitve/postopki/posegi, tudi preventivne storitve, diagnoza, prognoza, stanje telesnega in duševnega zdravja ipd.)
- rasno ali etnično poreklo,
- politično mnenje,
- versko ali filozofsko prepričanje,
- članstvo v sindikatu,
- genetske informacije,
- biometrične informacije za namene edinstvene identifikacije posameznika,
- posameznikovo spolno življenje ali spolno usmerjenost, ali
- kazenske obsodbe in prekrške (posebne kategorije podatkov),

pošiljajo znotraj zavoda (med uslužbenci) ali izven zavoda (drugim izvajalcem zdravstvene dejavnosti, pacientom, ZZZS, NIJZ in drugim uporabnikom) **po elektronski pošti**, morajo biti podatki na poti **šifrirani**. Le če gre pri notranji komunikaciji za zaprte interne sisteme (npr. lastni poštni strežnik), šifriranje ni potrebno.

26. člen
(formalne zahteve pri posredovanju osebnih podatkov zunanjim uporabnikom)

(1) **Vsako posredovanje osebnih podatkov zunanjim uporabnikom** (npr. oblastni organi, nadzorni organi oziroma organizacije, ZZZS, ZPIZ, MDPŠ, pogodbeni obdelovalci) se zaradi zagotavljanja sledljivosti beleži v **evidenco posredovanj osebnih podatkov na obrazcu - PRILOGA E** tega pravilnika, iz katere mora biti razvidno, kateri osebni podatki oziroma dokumenti so bili posredovani, komu, kdaj ter kdo je to storil. To velja ne glede na to, ali se posreduje originalna dokumentacija, kopije ali zgolj posamični podatki, ter ne glede na način posredovanja (papir/e-pošta/telefon). Evidenca se **hrani 5 let od zadnjega posredovanja**.

Izpolnjevanje zgornje evidence lahko izjemoma nadomesti:
- v izvorno dokumentacijo vložena vloga uporabnika in vložen odgovor zavoda, s katerim so bili posredovani osebni podatki uporabniku;
- uradni zaznamek (s podatki iz priloge E) na ohranjenem izvirniku posredovanega dokumenta;
- v informacijskem sistemu (IS) evidentirana vhodna in izhodna pošta;
- avtomatska elektronska sledljivost v IS (z enakimi podatki, kot so navedeni v prilogi E);
- ročni zapis v papirno ali elektronsko vodeno zdravstveno dokumentacijo.

(2) Namesto evidence iz priloge E, se lahko uporabljajo tudi druge pomožne evidence, če zagotavljajo enako raven sledljivosti. Posredovanje kopij zdravstvene dokumentacije pacientom ali izvedba osebnih vpogledov (oboje zlasti v primeru ustnih zahtev) se praviloma beleži v pacientovi zdravstveni dokumentaciji na obrazcu **PRILOGA E.1**.

(3) O posredovanju osebnih podatkov zunanjim uporabnikom (tudi državnim organom na posamično zahtevo) se **odloča centralizirano** – primarno o tem odloča direktor (npr. sporni primeri, neznane pravne podlage, večji obseg podatkov). Posredovanje podatkov pacientom in njihovim zastopnikom ter svojcem se lahko izvaja decentralizirano; tudi v tem primeru se posredovanje zabeleži v evidenco ali v zdravstveno dokumentacijo. Decentralizirano se lahko o posredovanju odloča tudi, če gre za redna posredovanja osebnih podatkov oziroma dokumentacije (npr. ZZZS za potrebe imenovanega zdravnika ali komisije).

(4) Zdravstvene dokumentacije se **brez pisne privolitve pacienta ne sme pošiljati drugemu izvajalcu medicine dela** za potrebe preventivnih zdravstvenih pregledov delavcev. Enako velja v razmerju med zaposlenimi v zavodu in izvajalcem medicine dela pri zavodu. Obe pravili ne veljata za druge vrste pregledov pri MDPŠ.

(5) O vpogledih v videonadzorni sistem in iznosu posnetkov ali podatkov se vodi posebna evidenca sledljivosti, ki je priloga sklepa o uvedbi videonadzora.

27. člen
(sledljivost iznosov iz arhiva ter drugih ravnanj)

(1) **Vsak iznos zdravstvene dokumentacije (mape ali posameznega dokumenta) iz arhivskih zbirk** se dokumentira posebej na obrazcu, ki je **PRILOGA F** tega pravilnika. Podatki v zbirki se **hranijo 5 let od zadnje aktivnosti.**

(2) Zavod lahko sprejme oziroma uporablja tudi:
- druge evidence oziroma obrazce kot je priloga F, če so primerljive s prilogo F,
- evidence oziroma obrazce za naročilo dviga dokumentacije iz arhiva,
- evidence oziroma obrazce za oddajo gradiva v arhiv in
- evidence oziroma obrazce za oddajo dokumentacije iz arhiva v uničenje.

VIII. IZBRIS OSEBNIH PODATKOV

28. člen
(način izbrisa podatkov)

(1) Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija brisanih podatkov.

(2) Podatki na klasičnih medijih (listine, kartoteke, register, seznami...) se uničijo na način, ki onemogoča branje vseh ali dela uničenih podatkov. Na enak način se uničuje pomožno gradivo (npr. matrice, izračune in grafikone, skice, poskusne oziroma neuspešne izpise ipd.).

(3) **Prepovedano je odmetavati nosilce podatkov, ki vsebujejo osebne podatke, na način, ki omogoča obnovitev ali razpoznavnost osebnih podatkov** (npr. celi listi v koš za smeti). **Osebni podatki v papirni obliki ali na podobnih nosilcih ter na CD/DVD-jih se uničijo z rezalnikom papirja ali na drug zanesljiv način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv**.

(4) Tekoča dokumentacija, ki je zaposleni za delo ne potrebujejo več, in jo je dopustno uničiti (npr. neuspeli izpisi dokumentov, ki vsebujejo osebne podatke, napačno izpolnjeni dokumenti) mora biti, na način iz prejšnjega odstavka, popolnoma oziroma nepovratno uničena še **isti dan**.

(5) Pri prenosu elektronskih nosilcev osebnih podatkov (npr. starih diskov) ali večjega števila nosilcev v papirni obliki (npr. uničevanje kartonov) na mesto uničenja je potrebno zagotoviti ustrezno zavarovanje tudi v času prenosa. Prenos teh nosilcev podatkov na mesto uničenja ter uničevanje nosilcev osebnih podatkov nadzoruje tričlanska komisija, ki jo določi direktor, in ki o uničenju sestavi tudi ustrezen zapisnik ali zaznamek. Uničevanje lahko namesto zavoda izvaja zunanji izvajalec, ki mora uničenje dokumentirati (kaj, kdaj in kako je bilo uničeno ter kdo je odgovorna oseba). Uničenje mora biti nepovratno.

IX. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

29. člen
(odgovorne osebe)

K izvajanju in nadzorovanju postopkov in ukrepov za zagotavljanje varnosti osebnih podatkov so

zavezani vsi uslužbenci, vključno z zunanjimi pogodbenimi izvajalci.

30. člen
(izjava o varovanju osebnih podatkov)

(1) Vsak, ki obdeluje osebne podatke, je dolžan izvajati v tem pravilniku predpisane postopke in ukrepe za varnost podatkov.

(2) Pred nastopom dela, kjer se obdelujejo osebni podatki, mora uslužbenec podpisati posebno **izjavo na obrazcu - PRILOGI G** tega pravilnika, ki jo opozarja in zavezuje k varovanju osebnih podatkov.

31. člen
(odgovornost)

(1) Za kršitev pravil o varovanju osebnih podatkov v smislu prejšnjega člena so uslužbenci disciplinsko, prekrškovno in kazensko odgovorni, če bi nastala škoda pa tudi odškodninsko.

(2) Uslužbenci so dolžni o aktivnostih, ki so povezane z odkrivanjem ali nepooblaščenim uničenjem osebnih podatkov, zlonamerni ali nepooblaščeni uporabi, prilaščanju, spreminjanju ali poškodovanju osebnih podatkov takoj obvestiti neposredno nadrejenega, sami pa morajo poskusiti z zakonitimi ukrepi takšno aktivnost preprečiti.

(3) Vsaka kršitev določb tega pravilnika predstavlja delovnopravno kršitev. Težja kršitev ima lahko za posledico odpoved delovnega razmerja. Razmejitev težje in lažje kršitve je odvisna od okoliščin konkretnega primera, pri čemer se upošteva:
- narava kršitve,
- posledice ravnanja ali opustitve (npr. konkretna škoda, velika nevarnost, konkretna prizadetost pacientov, prizadetost sodelavcev, prizadetost delovanja sistema),
- raven posega v zasebnost,
- razlogi ali nagibi za ravnanje ali opustitev,
- vrsta osebnih podatkov,
- število prizadetih posameznikov,
- enkratno ali večkratno ravnanje ali opustitev,
- obseg osebnih podatkov oziroma obdelave,
- ravnanje po kršitvi,
- soodgovornost,
- ali gre hkrati za kršitev zakonskih pravil in
- procesne oziroma sistemske pomanjkljivosti, ki so pripeljale do kršitve.

X. INTERNE REVIZIJE IN POSEBNE DOLOČBE GLEDE IDENTIFIKACIJE OSEB V KONTAKTU

32. člen
(izvajanje notranjih revizij)

V skladu z (d) točko prvega odstavka 32. člena in (b) točko prvega odstavka 39. člena Splošne

uredbe (EU) zavod **periodično (najmanj enkrat letno – redna revizija, ali po potrebi večkrat letno – izredna revizija zaradi zaznanih pomanjkljivosti ali incidentov) izvede notranjo revizijo (pregled, presojo) zagotavljanja varnosti podatkov v skladu s predpisi in s tem pravilnikom ter jo ustrezno dokumentira**. Pri reviziji se ugotavlja dejanska skladnost ter predlaga ukrepe za izboljšanje zagotavljanja varnosti podatkov oziroma splošne skladnosti s predpisi. Revizija je lahko celostna ali pa usmerjena v določeno področje (npr. zagotavljanje šifriranja, beleženje posredovanja dokumentacije in podatkov, zaklepanje prostorov, varnostno kopiranje podatkov itd.).

33. člen
(identifikcija oseb v kontaktu za potrebe sporočanja osebnih podatkov ali predaje dokumentacije)

(1) **Avtentikacja (identifikacija) klicatelja pri klicih ali pošiljtelja pri e-poštni komunikaciji** se glede obstoječih pacientov izvaja s pomočjo varnega elektronskega podpisa ali tako, da klicatelj oziroma pošiljatelj razkrije osebno ime **in** ustrezne kombinacije:

- dodeljene interne številke pacienta in/ali
- rojstnega datuma in/ali
- naslova in/ali
- ZZZS številke in/ali
- poznavanja drugih individualnih dejstev in okoliščin (npr. številka in datum izvida, osebno ime zdravnika, zdravstveni problem, izvedene zdravstvene storitve).

Identiteta se lahko preverja tudi na način predhodno javljene telefonske številke oziroma e-naslova.

(2) **Za prevzem dokumentacije v informacijski (sprejemni) pisarni, v tajništvu direktorja ter v ambulantah morajo**:

- pacienti predložiti kartico ZZ ali osebni dokument s sliko, če ni zagotovljen drug način identifikacije (npr. osebno poznanstvo, predhodni dogovor, poznavanje vsebine in izdajatelja dokumentov);
- pacientovi svojci oziroma pooblaščenci predložiti pacientovo kartico ZZ ali/in svoj osebni dokument s sliko ali/in pooblastilo, če ni zagotovljen drug način identifikacije.

(3) Če se uslužbenec ne more prepričati o identiteti ali/in upravičenosti do podatkov, zahtevo za posredovanje podatkov oziroma dokumentacije zavrne ter osebi v kontaktu predlaga osebni obisk ali drug način izkazovanja identitete ali/in upravičenosti do podatkov.

XI. POLITIKA UPRAVLJANJA Z VARNOSTNIMI INCIDENTI

34. člen
(splošno)

(1) Varnostni incident predstavlja enega ali več nezaželenih ali nepričakovanih dogodkov, za katere je zelo verjetno, da bodo lahko ogrozili normalno poslovanje zavoda oziroma zaupnost, celovitost ali razpoložljivost osebnih podatkov v upravljanju.

(2) Incidenti so:

- izguba, uničenje ali zloraba osebnih podatkov (podatki v elektronski obliki, papirni dokumenti itd.), ki vpliva na zaupnost, celovitost ali razpoložljivost podatkov;

- namerno ali nenamerno poškodovanje ali zloraba računalniškega informacijskega sistema (uničenje ali poškodbe strojne opreme, okužbe z zlonamerno programsko opremo, vdori v računalniški informacijski sistem), ki vpliva na razpoložljivost podatkov;
- kraja opreme (strojne ali programske);
- izpad delovanja računalniškega informacijskega sistema (strojna oprema, programska oprema, komunikacije), ki vpliva na razpoložljivost podatkov in izvajanje zdravstvenih ter podpornih storitev;
- kršitve zakonodaje (kršitev prepisanih pravil varstva osebnih podatkov glede varnosti ali kršitev prepovedi in pravnih podlag za obdelavo);
- neupoštevanje določil varnostnih politik s strani uslužbencev ali drugih oseb.

(3) Vsi uslužbenci kot uporabniki informacijskega sistema so dolžni interno prijavljati zaznane incidente **pooblaščeni osebi za varstvo osebnih podatkov**. Prijava incidentov lahko poteka ustno, telefonsko, preko elektronske pošte ali namenskih aplikacij. **Pri interni prijavi incidenta je potrebno navesti**:

- kaj se je zgodilo (kdo, kje, kdaj, kako, s čim, zakaj, trajanje ipd.),
- kateri podatki, dokumenti, zbirke ali oprema so predmet incidenta,
- katere kategorije posameznikov in koliko posameznikov je prizadetih,
- kje in kdaj je bil zapažen incident,
- kdo je bil prisoten,
- kakšne so posledice (negativni ali možni negativni učinki) in kakšen vpliv ima incident na poslovanje zavoda oziroma zaupnost, celovitost ali razpoložljivost podatkov,
- ukrepanje uslužbencev.

(4) Pooblaščena oseba beleži vse podatke o prijavljenih in obravnavanih incidentih na enem mestu vsaj v e-obliki (**EVIDENCA INCIDENTOV, kot PRILOGA H tega pravilnika – ta vsebuje podatke iz prejšnjega odstavka ter podatke o aktivnostih in odločitvah v zvezi z incidentom ter sprejetih popravnih ukrepih**) in izvajati aktivnosti odprave oziroma zmanjšanja posledic incidentov. Vsi incidenti, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov (podatki v elektronski obliki, papirni dokumenti itd.), morajo biti takoj sporočeni direktorju. Vsi incidenti, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo strojne ali programske opreme oziroma izpad delovanja računalniškega informacijskega sistema zavoda, ki vpliva na razpoložljivost podatkov, morajo biti v istem delovnem dnevu oziroma prvi delovni dan po incidentu sporočeni direktorju. Vsi lažji ali skorajšnji incidenti, ki bi lahko bili posledica kršenja zakonodaje ali neupoštevanja določil varnostnih politik, morajo biti direktorju sporočeni zbirno najkasneje v enem mesecu.

(5) **To poglavje velja tudi za evidentiranje in uradno obveščanje o kršitvah varstva osebnih podatkov po členu 33 in 34 Splošne uredbe EU**. Končno odločitev o uradnem obveščanju o kršitvi Informacijskega pooblaščenca ali posameznikov sprejme direktor. Poročanje Informacijskemu pooblaščencu se izvaja skladno z navodili, ki so objavljena na spletni strani Informacijskega pooblaščenca.

35. člen
(splošna pravila o ravnanju ob incidentih)

(1) V primeru incidentov, ki lahko povzročijo oziroma so povzročili izgubo, uničenje ali zlorabo osebnih podatkov, je treba takoj poskrbeti za izvajanje ukrepov za zaščito podatkov. Preostale podatke se mora primerno zaščititi z ustreznimi varnostnimi ukrepi. Revizijske sledi dostopov do izgubljenih, uničenih ali zlorabljenih podatkov se mora preveriti, da se ugotovi, kdo in kdaj je povzročil izgubo, uničenje ali zlorabo podatkov.

(2) V primeru incidentov, ki lahko povzročijo oziroma so povzročili namerno ali nenamerno poškodovanje ali zlorabo računalniškega informacijskega sistema, krajo opreme oziroma izpad delovanja računalniškega informacijskega sistema, je treba poskrbeti za primerno zaščito računalniških informacijskih sredstev (prenos sredstev na varno mesto, omejitev dostopa) oziroma ponovno vzpostavitev delovanja računalniškega informacijskega sistema. Primarne aktivnosti so namenjene vzpostavitvi komunikacijskih povezav in delovanju opreme.

(3) V primeru incidentov, ki predstavljajo direktno kršitev zakonodaje, mora vodstvo takoj obvestiti ustrezne državne institucije (npr. policija, Informacijski pooblaščenec) in v skladu z njihovimi navodili podati vse podatke oziroma predati sredstva, ki so bila uporabljena pri izvajanju prekrška oziroma kaznivega dejanja.

(4) V primeru incidentov, ki bi lahko bili posledica oziroma so posledica neupoštevanje določil varnostnih politik, je treba zagotoviti primerno zaščito podatkov in računalniškega informacijskega sistema ter zabeležiti vse značilnosti incidenta.

(5) V postopku je treba izločiti in fizično zaščititi ter varno shraniti dokaze, ki so na voljo v zvezi z incidentom (npr. videonadzorni posnetek, revizijske sledi, poročilo pregleda IS) oziroma posledice incidenta dokumentirati na drug način (npr. fotografiranje, skeniranje).

36. člen
(naknadna ravnanja)

(1) Po zaključenem reševanju incidenta mora pooblaščena oseba oceniti posledice incidenta in ukrepe, ki so bili izvedeni na podlagi incidenta. Oceni se vrsta incidenta, število prizadetih uporabnikov, količina in stopnja zaupnosti izgubljenih, uničenih ali zlorabljenih podatkov, čas trajanja in pogostost pojavljanja. Na tej podlagi se izvede ali dopolni evidentiranje kršitev po petem odstavku 34. člena tega pravilnika in po potrebi poroča direktorju.

(2) Pooblaščena oseba ima pravico, da ugotavlja, kdo je bil udeležen v posameznem incidentu, v ta namen pa ima pravico do vpogleda v vse zbirke podatkov, revizijske sledi, programske rešitve, podatke nadzornih mehanizmov, prometne podatke, podatke na računalniški opremi ipd. Uslužbenci so dolžni sodelovati s pooblaščeno osebo.

XII. DRUGE IN KONČNE DOLOČBE

37. člen
(privolitev pacienta in informiranje o obdelavi)

(1) Če želi pacient podati pisno privolitev glede razkrivanja njegovih osebnih podatkov in zdravstvene dokumentacije svojcem ali tretjim osebam, se mu lahko ponudi v izpolnitev izjava kot **PRILOGA I**. Izpolnjena izjava se vloži v zdravstveni karton. Izjava je preklicljiva. Izjava se uporablja le za razkrivanje informacij tistim uporabnikom, ki nimajo zakonske podlage za seznanitev.

(2) Na podlagi člena 13 in 14 Splošne uredbe (EU) o varstvu podatkov se paciente prek spletne strani (kategorija varstvo osebnih podatkov) in v tiskani obliki, ki je na voljo po organizacijskih enotah, vključno v sprejemni pisarni, obvešča z osnovnimi informacijami o obdelavi osebnih podatkov, ki so **PRILOGA J** tega pravilnika.

38. člen
(publiciteta)

(1) Ta pravilnik se hrani oziroma **mora biti na voljo uslužbencem**:
- v prostorih uprave v elektronski in fizični obliki,
- pri vodjih posameznih organizacijskih enot,
- v zunanjih enotah zavoda,
- v elektronski obliki v skupnih mapah (intranet) ali na način posredovanja pravilnika vsem zaposlenim prek e-pošte in
- po potrebi v drugih primernih prostorih (npr. fizična oglasna deska).

(2) Ta pravilnik je prosto dostopen tudi pogodbenim obdelovalcem osebnih podatkov oziroma je priloga pogodb o obdelavi osebnih podatkov.

(3) Ta pravilnik se proaktivno **ne objavi na spletni strani** zavoda iz varnostnih razlogov. Uslužbenci zavoda so dolžni varovati njegovo vsebino nasproti tretjim nepooblaščenim osebam. Pacientom se na zahtevo oziroma na predlog zdravstvenega delavca posreduje priloga I za potrebe uveljavljanja pravic.
Na spletni strani (kategorija varstvo osebnih podatkov) se objavita le prilogi A in J.

(3) Sestavni del tega pravilnika so priloge od A do J ter oba sklepa o uvedbi videonadzora.

39. člen
(razmerje do internih politik)

(1) Med interne akte zavoda spadajo tudi naslednje sprejete **splošne politike**:
- Politika fizične zaščite in dostopa (2018);
- Politika nadzora dostopa do aplikacij, informacij in sistemov (2018);
- Politika nadzora dostopa do omrežja (2018);
- Politika revizijskih sledi (2018);
- Politika upravljanja in varovanja gesel (2018);
- Politika varnostnega kopiranja podatkov (2018);
- Politika zagotavljanja kakovosti infrastrukture (2018);
- Politika zaščite pred zlonamerno programsko opremo (2018).

(2) Pri izvajanju ukrepov za varnost osebnih podatkov **imajo prednost določbe tega pravilnika**. Za posamezna vprašanja, ki **v pravilniku niso urejena ali niso urejena tako podrobno, se uporabljajo politike iz prejšnjega odstavka.**

(3) Določbe tega pravilnika se smiselno uporabljajo tudi za poslovne skrivnosti in morebitne druge interne podatke, ki jih določi zavod.

40. člen
(sodelovanje sindikatov, razveljavitev, vakacijski rok)

(1) Reprezentativni sindikati v zavodu so pozvani k podaji mnenja k pravilniku. Pridobljena mnenja se hranijo kot posebna priloga pravilnika.

(2) Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o varovanju osebnih in drugih zaupnih podatkov ter dokumentarnega gradiva, št. 142-03/ZM z dne 30. 5. 2003.

(3) Ta pravilnik prične veljati v osmih dneh po sprejemu in njegovi objavi v skladu s prvim odstavkom 38. člena tega pravilnika.

Številka: 03-138/2020
Različica: 1.0.
Datum: 27.11.2020

Dražen Levojević, univ. dipl. prav.
DIREKTOR