KIRURŠKI SANATORIJ
Rožna dolina

PRAVILNIK O POSTOPKIH IN UKREPIH ZA ZAVAROVANJE OSEBNIH PODATKOV in katalog zbirk osebnih podatkov

Upravljavec:

Kirurški sanatorij Rožna dolina, d.o.o.

Rožna dolina cesta IV/45, Ljubljana

Datum sprejetja prvega pravilnika: 20. 12. 2006

Datum sprejetja novega pravilnika: 16. 3. 2015

Na podlagi 24. in 25. člena Zakona o varstvu osebnih podatkov (Uradni list RS, št. 94/07 - UPB; v nadaljevanju: ZVOP-1) izdaja direktorica Kirurškega sanatorija Rožna dolina, d.o.o. Brigita KOLENC, univ. dipl. oec.

P R A V I L N I K
o postopkih in ukrepih za zavarovanje osebnih podatkov v Kirurškem sanatoriju Rožna dolina

I. SPLOŠNE DOLOČBE

1. člen
(področje urejanja)

(1) S tem pravilnikom se določajo organizacijski, tehnični in logično-tehnični postopki ter ukrepi za zavarovanje varovanih osebnih podatkov v Kirurškem sanatoriju Rožna dolina (v nadaljevanju KSRD) z namenom, da se **fizično prepreči slučajno ali namerno nepooblaščeno uničevanje, sprememba ali izguba** varovanih osebnih podatkov, ter **nepooblaščen dostop, obdelava, uporaba ali posredovanje** 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, ki se nanašajo na lastnosti, stanja ali razmerja fizičnih oseb oziroma posameznikov – pacientov in njihovih svojcev, uslužbencev KSRD, zunanjih pogodbenih sodelavcev in poslovnih strank, ne glede na obliko, v kateri so podatki izraženi in ne glede na vrsto nosilca osebnih podatkov, ter glede katerih ni podane pravne podlage za razkritje podatka javnosti (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 (posredno) identificirati posameznika.

(5) V smislu določbe prejšnjega odstavka so primeri osebnih podatkov zlasti:
- identifikacijski podatki o posamezniku,
- podatki o zdravstvenem stanju posameznika, vključno s podatki o načrtovani in izvedeni zdravstveni oskrbi,
- podatki, ki se nanašajo na družinska in sorodstvena razmerja,
- podatki o izobrazbi, zaposlitvi, socialnem in ekonomskem stanju posameznika,

- biometrični podatki (lastna podoba, glas in druge telesne značilnosti),
- podatki o uporabi komunikacijskih sredstev (prometni podatki),
- podatki, ki se nanašajo na rasno poreklo in narodnostno pripadnost,
- podatki o ideoloških, verskih in drugih prepričanjih,
- podatki o navadah posameznika.

(4) Uslužbenci, zunanji sodelavci KSRD ter pogodbeni obdelovalci, ki pri svojem delu obdelujejo osebne podatke, **morajo biti seznanjeni** z ZVOP-1, s področno zakonodajo, ki ureja področje njihovega dela (zlasti z ustreznimi deli Zakona o pacientovih pravicah, Zakona o zdravstvenem varstvu in zdravstvenem zavarovanju, Zakona o zdravstveni dejavnosti, Zakona o zdravniški službi, Pravil obveznega zdravstvenega zavarovanja), z vsebino tega pravilnika ter z drugimi internimi navodili in politikami s področja varovanja informacij in zasebnosti.

(5) KSRD ima sprejeto **Krovno politiko varovanja informacij, z dne 28. 10. 2014, ki se šteje za sestavni del tega pravilnika**.

(6) KSRD ima sprejet **Protokol dela na recepciji Kirurškega sanatorija**. Ta se v delu, ki se nanaša na varstvo osebnih podatkov, **šteje za sestavni del tega pravilnika**.

(7) KSRD ima sprejeta pravila tehničnega varovanja in uporabe alarma, ki so predpisana z okrožnico **»Varovanje objekta, opreme in ljudi v Kirurškem sanatoriju Rožna dolina od 1. 10. 2013 dalje«**, ki se **šteje za sestavni del tega pravilnika**.

2. člen
(pojmovnik)

V tem pravilniku uporabljeni izrazi imajo naslednji pomen:

1. Zbirka osebnih podatkov - je vsak strukturiran (sistematično urejen) niz osebnih podatkov. Kot zbirke osebnih podatkov štejejo zlasti zbirke KSRD, ki so opredeljene v katalogu zbirk osebnih podatkov, ki je PRILOGA A tega pravilnika;
2. Obdelava osebnih podatkov - pomeni kakršnokoli delovanje ali niz delovanj, ki se izvaja v zvezi z osebnimi podatki, ki so pri ročni (npr. klasična papirna zdravstvena dokumentacija) ali avtomatizirani (npr. prenos podatkov prek elektronskih komunikacij) obdelavi del zbirke osebnih podatkov ali so namenjeni vključitvi v zbirko osebnih podatkov. 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 KSRD za potrebe tega pravilnika so:
   - zaposleni v KSRD,
   - zunanji pogodbeni sodelavci, ki imajo pravico opravljati delo v KSRD, vključno s študenti,
   - posamezniki, ki v prostorih KSRD ali izven opravljajo delo za pogodbenega obdelovalca osebnih podatkov za KSRD ter
   - člani nadzornega sveta in družbeniki ali predstavniki družbenikov.
4. Upravljavec osebnih podatkov - je KSRD kot pravna oseba zasebnega prava in izvajalec zdravstvene dejavnosti, ki ima odločilen pravni in fizični vpliv in kontrolo nad obdelavo osebnih podatkov v zbirkah, s katerimi razpolaga;
5. Občutljivi osebni podatki - so podatki o rasnem, narodnem ali narodnostnem poreklu, političnem, verskem ali filozofskem prepričanju, članstvu v sindikatu, zdravstvenem stanju,

spolnem življenju, vpisu ali izbrisu v ali iz kazenske evidence ali prekrškovne evidence ter biometrične značilnosti;

6. 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;
7. 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. CD, DVD, USB ključki, prenosni diski), fotokopije, zvočno in slikovno gradivo, mikrofilmi, naprave za prenos podatkov, ipd.

3. člen
(splošni postopki in ukrepi)

(1) Zavarovanje osebnih podatkov zajema pravne, organizacijske in ustrezne logično-tehnične postopke in ukrepe, s katerimi se:

1. fizično varujejo prostori, kjer se nahajajo osebni podatki, ter strojna in sistemska programska oprema, ki se uporablja pri obdelavi osebnih podatkov;
2. varuje aplikativna programska oprema, s katero se obdelujejo osebni podatki;
3. zagotavlja varnost posredovanja in prenosa osebnih podatkov, vključno s prenosom po telekomunikacijskih sredstvih in omrežjih;
4. onemogoča nepooblaščenim osebam dostop do ročno vodenih zbirk (dokumentacije) in računalniških sistemov, s pomočjo katerih se obdelujejo osebni podatki;
5. zagotavlja učinkovit način zakonitega blokiranja, uničenja, izbrisa ali anonimiziranja osebnih podatkov,
6. omogoča poznejše ugotavljanje, kdaj in kako ter zakaj so bili posamezni osebni podatki obdelani in kdo je to storil, in sicer za obdobje, ko je mogoče zakonsko varstvo pravice posameznika zaradi nedopustnega posredovanja ali obdelave osebnih podatkov (zagotavljanje sledljivosti obdelave).

(2) Postopki in ukrepi za zavarovanje osebnih podatkov morajo biti ustrezni glede na tveganje, ki ga predstavlja obdelava in narava določenih osebnih podatkov, ki se obdelujejo.

4. člen
(register zbirk osebnih podatkov in katalog zbirk osebnih podatkov)

(1) Opis zbirk osebnih podatkov, katerih upravljavec je KSRD, se vodi v katalogu zbirk osebnih podatkov, ki je **PRILOGA A** tega pravilnika, in ki se vodi v skladu z določbami 26. člena ZVOP-1. Podatki iz kataloga zbirk osebnih podatkov ter spremembe se posredujejo Informacijskemu pooblaščencu, pristojnemu tudi za vodenje Registra zbirk osebnih podatkov. Katalog zbirk osebnih podatkov se za vsako novo zbirko osebnih podatkov zagotovi pred vzpostavitvijo zbirke osebnih podatkov. Katalog zbirk osebnih podatkov se dopolnjuje ob vsaki spremembi vrste osebnih podatkov v posamezni zbirki.

(2) KSRD vodi ažuren seznam (**PRILOGA B** tega pravilnika), iz katerega je za vsako zbirko osebnih podatkov razvidno, katera oseba je odgovorna za posamezno zbirko osebnih podatkov ter katere osebe lahko zaradi narave svojega dela obdelujejo osebne podatke, ki se nanašajo na posamezno zbirko osebnih podatkov. V seznam se vpisujejo sledeči podatki:

- naziv zbirke osebnih podatkov ali/in notranja organizacijska enota, ki razpolaga z zbirko

osebnih podatkov,
- identifikacija delovnega mesta osebe (poleg tega lahko tudi njeno osebno ime), ki je odgovorna za posamezno zbirko osebnih podatkov ali sklop zbirk v notranji organizacijski enoti ter
- identifikacija delovnega mesta osebe (poleg tega lahko tudi njeno osebno ime), ki je zaradi narave njenega dela pooblaščena obdelovati osebne podatke iz določene zbirke osebnih podatkov ali sklopa zbirk v notranji organizacijski enoti.

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 KSRD so:
- recepcija,
- sprejemna pisarna,
- ambulante (občasno),
- laboratorij in RTG,
- sestrski pulti in spremljajoči prostori (območje zdravstvenih pisarn oziroma sob),
- bolniške sobe (občasno),
- območje upravnih pisarn, zlasti vodstva,
- pisarna booking službe, klicni center in pisarna pred zahodnim bolniškim oddelkom,
- prehodni hodnik v pritličju,
- arhiv zdravstvene in poslovne dokumentacije (več lokacij),
- območje računalniškega informacijskega sistema in območje komunikacijskega sistema (vodi, strežnik, delovne postaje, druga premična oprema).

(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)**, vključno s pritličnimi ali kletnimi okni,
- **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 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 (npr. v prehodnem hodniku v pritličju) 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 izklopljeni ali fizično oziroma programsko zaklenjeni.

(6) **Politika čiste mize**: Uslužbenci **ne smejo brez stalnega nadzora puščati nosilcev osebnih podatkov** (npr. papirnata zdravstvena dokumentacija, CD-ji, DVD-ji in USB ključi) na mizah, pultih, policah, voziČkih in drugih odlagalnih mestih, ki so neposredno dostopni osebam, ki nimajo pravice do seznanitve. Na primer na pultih in mizah, s katerimi pacienti in drugi redoma prihajajo v stik, zdravstvena dokumentacija kljub prisotnosti uslužbencev **ne sme biti na vpogled pacientom** (razen če gre za njihovo zdravstveno dokumentacijo), obiskovalcem ali drugim nepooblaščenim osebam.

(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 občutljivih 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 zaradi potreb delovnega procesa.

(9) Na **oglasni deski** in podobnih površinah ni dovoljeno objavljati osebnih podatkov, razen osebnih podatkov uslužbencev, če tako določi vodstvo in so izpolnjeni pogoji za javno objavo. V regalih, ki so namenjeni hitremu dostopu do pojasnil za paciente in praznih obrazcev (ambulantni del, sprejemna pisarna) se ne sme shranjevati dokumentov, ki bi vsebovali osebne podatke.

(10) **Seznami ali razporedi pacientov in podobni dokumenti**, ki niso del zdravstvene dokumentacije ne smejo biti nikjer prosto dostopni obiskovalcem (npr. na mizah, pritrjeni na stenah ali omarah).

(11) **Vrata na osebnem vhodu in vrata na servisnem vhodu** ob cesti XV (zahodno od stavbe KSRD) morajo biti stalno zaprta oziroma zaklenjena. Enako velja za dodatna vhodna vrata v stavbo na južnem pročelju (med cesto XV in glavnim južnim vhodom).

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

(13) Hramba zdravstvene dokumentacije (arhivi, ambulantne kartoteke, tekoča dokumentacija hospitaliziranih pacientov itd.) se znotraj posameznih organizacijskih enot **v čim večji meri izvaja centralizirano** (na enem mestu ali na čim manjšem številu mest).

(14) Uslužbenci **ne smejo nosilcev osebnih podatkov odnašati izven prostorov** KSRD, razen kadar gre za zakonito posredovanje dokumentacije drugemu uporabniku ali kadar je to, na podlagi dovoljenja ali vednosti vodstva ali drugih pooblaščenih uslužbencev, nujno potrebno za zagotovitev zdravstvene oskrbe ali za opravo drugih delovnih nalog.

(15) KSRD zagotavlja požarno varnost v skladu s posebnimi predpisi ter v sodelovanju z zunanjim pogodbenikom.

(16) KSRD zagotavlja tehnično varovanje z alarmom s povezavo na zunanjo varnostno službo za potrebe intervencij. **Pravila sistema varovanja in uporabe alarma so predpisana z okrožnico »Varovanje objekta, opreme in ljudi v Kirurškem sanatoriju Rožna dolina od 1. 10. 2013 dalje«**, ki se **šteje za sestavni del tega pravilnika**.

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

Za tehnično etažo (arhiv) ali druge prostore, v katerih je lahko 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**;
- **dostop z dvigalom je za nepooblaščene uporabnike zaklenjen**;
- prostori morajo biti zavarovani pred škodljivim fizičnim delovanjem (izlitje vode, požar, elektromagnetno valovanje ipd.);
- oprema mora biti nameščena v skladu s pogoji, ki so skladni s tehničnimi specifikacijami opreme.

7. člen
(monitorji in zaklepanje računalnika)

(1) V prostorih, ki so namenjeni poslovanju s strankami (npr. recepcija, sprejemna pisarna, sestrski pulti na bolniških oddelkih, laboratorij), morajo biti računalniški **monitorji nameščeni tako, da nepooblaščene osebe nimajo vpogleda vanje**. Izjeme so :

– če se v času prisotnosti tretje osebe obdelujejo le osebni podatki te osebe ali osebni podatki njegovega svojca;
– če zahteve po zdravem in ergonomskem delovnem mestu tega ne dopuščajo;
– če velikost in ureditev prostora tega ne dopušča.

(2) **V recepciji** se za obdelavo osebnih podatkov v internem računalniškem omrežju in programu HIPOKRAT **uporablja le skriti monitor**, usmerjen na zahod in ne monitor, ki je usmerjen na sever.

(3) Vse delovne postaje (računalniki) morajo imeti vklopljeno funkcijo **avtomatskega zaklepanja računalnika**, 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)

(1) Vzdrževanje in popravila strojne računalniške in druge opreme lahko **po navodilih ali z vednostjo vodstva** izvaja le **pooblaščeni uslužbenec** oziroma **zunanji pogodbeni vzdrževalec**, ki ima s KSRD

sklenjeno tudi pogodbo o obdelavi osebnih podatkov po 11. členu ZVOP-1.

9. člen
(zadrževanje drugih oseb v varovanih prostorih)

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

(2) Uslužbenci, ki ne izvajajo strokovnih nalog v zvezi z zbirkami osebnih podatkov, se lahko izven delovnega časa oziroma brez prisotnosti pooblaščenega uslužbenca KSRD 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 preko VPN povezave in z uporabo sistemov za varni dostop (npr. SECURID kartica).

(3) Če službeni notesniki, ki jih uslužbenci iznašajo iz službenih prostorov vsebujejo občutljive osebne podatke pacientov ali drugih oseb, se diske praviloma programsko šifrira. Enako velja za morebitne službene USB ključke in prenosne diske.

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.

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 prisotnost računalniških virusov in zlonamernih kod**. Ob pojavu neželenih pojavov se te čim prej odpravi s pomočjo 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 KSRD 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 KSRD 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 ali pomnilniških medijih zlasti pa priponk v elektronski pošti)**. Tako opremo oziroma dokumente je treba na varen način preveriti, ali obstaja okuženost z zlonamerno programsko opremo.

(4) V informacijskem sistemu KSRD mora biti nameščen:
- **protivirusni program;**
- **požarni zid novejšega tipa;**
- ***anti-spyware* zaščita;**
- ***anti-spam* filter;**
- **sistem poročanja o varnostnih incidentih.**

(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 osebe, zadolžene za delovanje računalniškega informacijskega sistema (pooblaščenega uslužbenca KSRD ali vzdrževalca opreme). Prav tako ne smejo odnašati programske in pomembne stacionarne strojne opreme iz prostorov KSRD brez odobritve ali vednosti osebe, zadolžene za delovanje računalniškega informacijskega sistema.

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. Dostop do *on line* sistema ZZZS se izvaja z opremo ZZZS in v skladu pravili ZZZS.

(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) **Dodeljevanje, uporaba in varovanje gesel (vključno z nadzornimi gesli) je podrobneje določeno v interni »Politiki upravljanja in varovanja gesel«, ki se šteje kot sestavni del tega pravilnika**. Uporaba pravil, določenih v vsakokratno veljavni Politiki upravljanja in varovanja gesel je obvezna.

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

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

16. člen
(varnostne kopije podatkov)

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.

17. člen
(uporaba sistema HIPOKRAT)

(1) Pooblaščeni uslužbenci (upravičeni uporabniki) se v sistem HIPOKRAT **prijavljajo s svojim uporabniškim imenom in geslom**. **Razkrivanje uporabniških imen in gesel sodelavcem ali drugim neupravičenim osebam, ter prijavljanje pod tujim uporabniškim imenom ali geslom je strogo prepovedano**.

(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 oziroma, ki niso potrebni za zdravstveno oskrbo konkretnega pacienta ali niso potrebni za druga nujna opravila v zvezi z zdravstveno oskrbo, je prepovedano in predstavlja prekršek po 91. členu ZVOP-1.**

(4) **Uslužbenci so o odgovornosti iz prejšnjega odstavka opozorjeni s posebnim obvestilom ob**

vstopu v računalniški sistem KSRD, po potrebi tudi ob vstopu v program HIPOKRAT.

(4) Uporabniške pravice iz tretjega odstavka tega člena so določene v **poimenskem seznamu uporabniških pravic za sistem HIPOKRAT**, ki je **PRILOGA C** tega pravilnika. Ob vsaki spremembi uporabniških pravic se PRILOGA C pravilnika ažurira s priložitvijo novega seznama k temu pravilniku.

18. člen
(zagotavljanje sledljivosti v sistemu HIPOKRAT)

(1) **Sistem HIPOKRAT zagotavlja sledljivost** iz 24. člena ZVOP-1, in sicer tako, da omogoča 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. Iskanje se omogoči najmanj po kriteriju določenega pacienta in najmanj s podatki o »pacientu«, »funkciji«, »uporabniku«, »datumu«, »uri« in »akciji«.

(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, log file) se **hranijo 6 let**.

19. člen
(uporaba smernic in posebna pravila za videonadzor)

(1) KSRD se pri uporabi in nadaljnjem razvoju informacijskih rešitev v največji možni meri ravna po »Smernicah za zavarovanje osebnih podatkov informacijskih sistemih bolnišnic« (prva objava 15. 2. 2008) Informacijskega pooblaščenca (dostop je omogočen prek spletne strani www.ip-rs.si).

(2) **Podrobna pravila za zavarovanje videonadzornega sistema so določena v Sklepu o uvedbi videonadzora (2015), ki se šteje kot sestavni del tega pravilnika**.

(3) **O vpogledih in reprodukciji (iznosu) posnetkov iz videonadzornega sistema se vodi posebna evidenca sledljivosti, ki je PRILOGA D tega pravilnika**. Evidenca oziroma zapisi se **hranijo 6 let** od zadnjega vnosa.

IV. UPORABA E-POŠTE IN INTERNETA

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

(1) Računalnik in elektronska pošta se uporabljata 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, lahko na posebej utemeljeno pisno zahtevo vodstva KSRD, v prisotnosti še dveh članov komisije, v izrednih primerih (nenadna odpoved delavca, smrt delavca ali drug izreden dogodek) vpogleda v elektronsko pošto le, če je to neizogibno nujno potrebno za vodenje delovnega procesa. Primarno se vpogleda le v prometne podatke (pošiljatelj/prejemnik, naslov sporočila, velikost in ime priponke, čas), izjemoma pa tudi vsebino domnevno relevantnih e-sporočil. 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 zaposleni ne spoštujejo omejitev iz drugega odstavka tega člena, lahko pooblaščeni uslužbenec, zadolžen za delovanje računalniškega informacijskega sistema, na posebej utemeljeno pisno zahtevo direktorice KSRD 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 KSRD, lahko KSRD zahteva od operaterjev telekomunikacijskih storitev le takrat, kadar pride med KSRD in uslužbencem do kakršnegakoli spora glede višine stroškov porabe konkretnega telefonskega priključka. KSRD nikoli ne sme preverjati identitete oziroma lastništva klicanih ali klicočih številk.

(7) Ob prenehanju delovnega razmerja ali drugega pogodbenega razmerja se uslužbencu ukinejo vse dostopne 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 KSRD pravico, da se vsi za KSRD nepotrebni podatki in nepotrebna elektronska pošta nepovratno uniči.

(8) V primeru iz prejšnjega odstavka, preusmeritev e-pošte na drugega uslužbenca ni dopustna.

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

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 oziroma namesto KSRD opravlja posamezna opravila v zvezi obdelovanjem osebnih podatkov in je tudi registrirana za opravljanje takšne dejavnosti (pogodbeni obdelovalec), se sklene pisna pogodba o pogodbeni obdelavi osebnih podatkov, kot to določa drugi odstavek 11. člena ZVOP-1. V takšni pogodbi morajo biti obvezno predpisani tudi pogoji in ukrepi za zagotovitev varstva osebnih podatkov in njihovega zavarovanja.

(2) Vzorec pogodbe je **PRILOGA I** tega pravilnika.

(3) **Sestavni del vsake pogodbe so naslednje obveznosti pogodbenega obdelovalca (splošni pogoji pogodbene obdelave)**:

a) Pogodbeni obdelovalec opravlja storitve obdelave osebnih podatkov samo v okviru naročnikovih pooblastil ter podatkov ne sme obdelovati ali drugače uporabljati za noben drug namen;
b) Pogodbeni obdelovalec, ki za KSRD opravlja dogovorjene storitve izven prostorov KSRD, mora, ne glede na določbe lastnega pravilnika o zavarovanju osebnih podatkov, upoštevati režim varovanja osebnih podatkov, ki je določen s tem pravilnikom ali pogodbo, če je ta režim strožji;
c) Pogodbeni obdelovalec seznani svoje uslužbence z obveznostmi varovanja osebnih podatkov;
d) Podpogodbena obdelava z drugim obdelovalcem je dopustna z neposredno sklenitvijo pogodbe med KSRD in drugim obdelovalcem, ali na način sklenitve pogodbe v korist tretjega v skladu s pravili obligacijskega prava;
e) Pogodbeni obdelovalec dovoli izvedbo nadzora nad spoštovanjem dogovorjenih in predpisanih pravil varovanja osebnih podatkov;
f) Podobeni obdelovalec po prenehanju pogodbene obdelave posredovane osebne podatke ali dokumente vrne KSRD, jih uniči ali nepovratno anonimizira;
g) Pogodbeni obdelovalec zagotavlja lastno sledljivost obdelave osebnih podatkov v skladu s 5. točko prvega odstavka 24. člena ZVOP-1. Predmet nadzora iz točke c) je lahko tudi dnevnik sledljivosti;
h) Pogodbeni obdelovalec mora v vsakem primeru spoštovati naslednja pravila iz tega pravilnika:
   - 3. člen,
   - drugi, četrti do osmi in smisleno štirinajsti odstavek 5. člena,
   - 6. člen,
   - prvi in tretji odstavek 7. člena,
   - smisleno 8., 9., 10., 11., 13., 14., 15., 16., 24. in 25. člen,
   - tretji odstavek 30. člena.

VI. SPREJEM IN EVIDENTIRANJE VHODNIH DOKUMENTOV

23. člen
(ravnanje z vhodno pošto)

(1) Uslužbenec, ki je zadolžen za sprejem in evidentiranje vhodne pošte, mora izročiti pošiljko z osebnimi podatki neposredno uslužbencu ali organizacijski enoti, na katero je pošiljka naslovljena.

(2) Uslužbenec, ki je zadolžen za sprejem in evidentiranje vhodne pošte, odpira in z namenom evidentiranja ter nadaljnjega posredovanja pregleduje vso vhodno pošto, razen v primeru iz tretjega odstavka tega člena.

(3) 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 vsebuje 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 KSRD, hkrati pa je osebno ime navedeno pred nazivom KSRD,
- 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

24. člen
(splošno o načinu posredovanja)

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

(2) Osebni podatki se pošiljajo v **zaprtih ovojnicah**, praviloma s **priporočeno poštno pošiljko** ali prek kurirske službe. Originalna ali pomembna zdravstvena dokumentacija se obvezno pošilja **priporočeno s povratnico**. **Na ovojnicah so lahko zapisani le podatki, ki so nujni za poštno dostavo pošiljke.**

(3) Če se dokumentacijo z osebnimi podatki, ki jo je zahteval pacient ali njegov svojec pošilja po klasični pošti, se pošiljko vroča osebno (priporočeno in praviloma s povratnico).

(4) Ovojnica, v kateri se posredujejo osebni podatki, mora biti izdelana na takšen način, da **ovojnica ne omogoča**, da bi bila ob normalni svetlobi ali pri osvetlitvi ovojnic z običajno

lučjo **vidna vsebina ovojnice**. Prav tako mora ovojnica zagotoviti, da **odprtja ovojnice in seznanitve z njeno vsebino ni mogoče opraviti brez vidne sledi odpiranja ovojnice**.

(5) O posebnih zahtevah zunanjih uporabnikov za posredovanje osebnih podatkov oziroma zdravstvene dokumentacije (npr. pacientovi svojci, policija, sodišče, zavarovalnice) odloča direktorica ali po njenem pooblastilu druga oseba v vodstvu. Izjema je, če gre za že ustaljeno zakonito posredovanje osebnih podatkov (npr. redno poročanje NIJZ).

25. člen
(posredovanje občutljivih osebnih podatkov prek elektronskih komunikacij)

(1) **Pri prenosu občutljivih osebnih podatkov preko elektronskih komunikacijskih omrežij ali na prenosnih elektronskih medijih** se šteje, da so podatki ustrezno zavarovani, če se posredujejo z uporabo kriptografskih metod in metod za avtentikacijo in avtorizacijo uporabnikov tako, da je zagotovljen varen dostop do podatkov in njihova **nečitljivost oziroma neprepoznavnost med prenosom**.

(2) V skladu s prejšnjim odstavkom, 14. členom ZVOP-1 in splošnimi pravili o varstvu in zavarovanju osebnih podatkov se posredovanje občutljivih osebnih podatkov izvaja tako:

- da je zagotovljeno, da je KSRD po zakonu ali na podlagi privolitve pacienta upravičen podatke posredovati, ter da se osebni podatki sporočajo za zakoniti namen (splošno pravilo, ki izhaja iz pravil o podlagah za obdelavo osebnih podatkov),
- da je zagotovljeno, da je prejemnik (uporabnik) osebnih podatkov na podlagi zakona ali privolitve pacienta upravičen podatke pridobiti (splošno pravilo, ki izhaja iz pravil o podlagah za obdelavo osebnih podatkov ter pravil za zavarovanje osebnih podatkov),
- da je neposredni uporabnik oziroma prejemnik (tj. fizična oseba pri organizaciji) tisti, ki ima pravico do obdelave osebnih podatkov glede na vsebino pravic in obveznosti iz delovnega razmerja ali druge pogodbe oziroma, da je z vidika notranjega poslovanja uporabnika pooblaščen za obdelavo – avtorizacija ali preverjanje pravic posameznika,
- da uporabnik oziroma prejemnik ve, da osebni podatki prihajajo od upravičenega upravljavca, tj. da pošiljatelj (KSRD kot upravljavec) z varnim elektronskim podpisom dokaže, da je tisti, za katerega se izkazuje – avtentikacija ali preverjanje istovetnosti,
- da osebni podatki med prenosom niso čitljivi (prepoznavni) za tretje nepooblaščene osebe (to se zagotavlja s kriptografskimi metodami) in
- da se osebni podatki med prenosom naključno ali namenoma ne spreminjajo ali brišejo (to se zagotavlja tudi z varnim elektronskim podpisom).

(3) Sporočanje informacij o zdravstvenem stanju prek telefona je dopustno samo, če je mogoče nedvomno ugotoviti identiteto uporabnika oziroma osebe, ki je do podatkov upravičena, zlasti tako, da navede **unikatno enolično interno številko**, ki je bila dodeljena pacientu.

(4) Posredovanje informacij o zdravstvenem stanju prek faks naprav je dopustno ob smiselnem upoštevanju določb prvega in drugega odstavka tega člena.

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

(1) Za vsako posredovanje osebnih podatkov mora zunanji uporabnik praviloma vložiti

podpisano pisno vlogo, v kateri mora biti:
- navedena (navedba imena prepisa in ustrezne določbe) ali priložena (npr. privolitev) pravna podlaga, ki uporabnika pooblašča za pridobitev osebnih podatkov,
- navedeno, kateri osebni podatki ali dokumenti se zahtevajo,
- navedeno, zakaj se osebni podatki zahtevajo (namen uporabe),
- navedeno v kakšni obliki se zahtevajo (npr. kopije po pošti),
- naveden polni naziv in naslov uporabnika in
- praviloma navedeno, katere okoliščine opravičujejo uporabo pravne podlage iz prve alineje (npr. obstoj škodnega primera in sklenjeno zavarovanje (številka police in škodnega spisa), če podatke zahteva zavarovalnica za potrebe likvidacije škode).

(2) Če se podatke posreduje na podlagi osebne oziroma ustne zahteve, se o tem napravi pisni zaznamek z vsebino v smislu prejšnjega odstavka. Uporabnik se mora identificirati z ustreznim dokumentom.

(3) Vsako posredovanje osebnih podatkov se zaradi zagotavljanja sledljivosti beleži v **evidenco posredovanj osebnih podatkov** (**PRILOGA E** tega pravilnika), iz katere mora biti razvidno, kateri osebni podatki so bili posredovani, komu, kdaj in na kakšni podlagi, ter druge okoliščine, ki so pomembne za zagotavljanje sledljivosti. To velja ne glede na to, ali se posreduje originalna dokumentacija, kopije ali zgolj posamični podatki. Evidenca se **hrani 6 let**.

Izpolnjevanje zgornje evidence lahko nadomesti:
- v izvorno dokumentacijo vložena vloga uporabnika in vložen odgovor KSRD, s katerim so bili posredovani osebni podatki uporabniku;
- uradni zaznamek (s podatki iz priloge E) na ohranjenem izvirniku posredovanega dokumenta;
- v informacijskem sistemu evidentirana vhodna in izhodna pošta.

(4) **Iznos zdravstvene dokumentacije iz arhiva**, se dokumentira posebej na obrazcu, ki je **PRILOGA F** tega pravilnika. Evidenca se **hrani 6 let.** Izpolnjevanje te evidence, zlasti za iznose za notranje dnevne potrebe, lahko nadomesti drug način zagotavljanja sledljivosti (npr. primeri iz prejšnjega odstavka), če je možno na podlagi podatkov v eni ali več zbirkah oziroma dokumentih, zanesljivo ugotoviti (rekonstruirati za nazaj), kdo, kdaj in kaj (ter po možnosti zakaj) je iznesel iz arhiva.

(5) **Originalna zdravstvena dokumentacija se posreduje izjemoma** (npr. če gre za posredovanje podatkov sodišču in je tako izrecno zahtevano). V času odsotnosti posredovane zdravstvene dokumentacije se te praviloma ne nadomešča s kopijo, če so vsi najnujnejši podatki zabeleženi tudi v programu HIPOKRAT. Če se posredovane dokumentacije ne nadomešča s kopijo, mora biti dokumentacija obvezno poslana najmanj s priporočeno pošiljko, praviloma pa na način priporočeno s povratnico.

(6) O vpogledih v videonadzorni sistem in iznosu posnetkov ali podatkov se vodi posebna evidenca sledljivosti, ki je določena s sklepom o uvedbo videonadzora.

27. člen
(formalne zahteve pri uresničevanju pravic pacienta)

(1) Pregledovanje (vpogled in fotografiranje), prepisovanje in kopiranje zdravstvene

dokumentacije KSRD na pacientovo zahtevo ter na njegove stroške omogoči najkasneje v 5 delovnih dneh.

(2) Pred izvedbo seznanitve je potrebno preveriti identiteto pacienta in sicer tako, da se vpogleda njegovo osebno izkaznico, potni list, orožni list ali vozniško dovoljenje. Kopiranje identifikacijskih listin ni dopustno, dopustno pa je prepisati številko dokumenta.

(3) Pri vsakem pregledovanju oziroma prepisovanju ter posredovanju podatkov iz zdravstvene dokumentacije se naredi **pisni zaznamek v evidenci seznanitev z lastno zdravstveno dokumentacijo** (**PRILOGA G** tega pravilnika), ki se nahaja v dokumentaciji. Iz pisnega zaznamka, ki ga mora podpisati tudi pacient, mora biti razvidna vrsta, datum in ura vpogleda, osebno ime upravičenca, njegov naslov, številka (če obstaja) in vrsta dokumenta, na podlagi katerega je ugotovljena identiteta ter neobvezno namen, zaradi katerega je bil opravljen pregled oziroma prepis.

Pisni zaznamek ni potreben, če gre za posredovanje po pošti, in se v zdravstveno dokumentacijo vloži pacientova zahteva in odgovor KSRD.

(4) Pacientu se pri uresničevanju pravice do seznanitve omogoči vpogled z **izročitvijo originalov v roke le ob stalnem nadzoru uslužbenca**. Enako velja pri uresničevanju pravice do dajanja pripomb na zapise v zdravstveni dokumentaciji. V slednjem primeru lahko pacient sam dopiše pripombe ali jih že napisane vloži v zdravstveno mapo, ali pa jih po nareku pacienta zapiše zdravstveni delavec. Iz zapisa mora biti jasno razvidno, kdo, kdaj in na kateri podlagi (41. člen ZPacP) je dopisal pripombo.

(5) Določbe prejšnjih odstavkov se smiselno uporabljajo tudi pri zahtevah za seznanitev s strani drugih zakonitih uporabnikov.

VIII. PRIDOBIVANJE, POSREDOVANJE IN DRUGA OBDELAVA OSEBNIH PODATKOV NA PODLAGI PRIVOLITVE PACIENTA

28. člen
(obrazec privolitve)

Če se obdelava osebnih podatkov izvaja na podlagi tretjega ali četrtega odstavka 44. člena Zakona o pacientovih pravicah (Ur.l. RS, št. 15/08; ZPacP), se privolitev poda na »obrazcu o privolitvi oziroma prepovedi obdelave osebnih podatkov oziroma sporočanja informacij o zdravstvenem stanju« (obrazec VOP), ki je v prilogi VIII Pravilnika o obrazcih o pisnih izjavah volje pacienta (Uradni list RS, št. 82/08 in 84/08 – popr.).

IX. POSEBNE DOLOČBE GLEDE ROČNO VODENE DOKUMENTACIJE

29. člen
(posebnosti pri obdelavi)

(1) Za varstvene ukrepe glede hrambe in nadaljnje obdelave morebitne digitalizirane zdravstvene

dokumentacije se smiselno uporabljajo določbe tega pravilnika, ki se nanašajo na varstvene ukrepe glede informatiziranih (računalniških) zbirk osebnih podatkov. Če gre pri tem za hrambo prek t.i. informacijskih storitev v oblaku, morajo biti za to izpolnjeni pogoji za zakonitost, kot to izhaja iz smernic Informacijskega pooblaščenca.

(2) Zdravstvena mapa (bolnišnični oziroma ambulantni karton) se vsak dan po zaključku dnevne obravnave praviloma in v najkrajšem možnem času vloži na stalno mesto hrambe.

(3) **Temperaturni listi ali druga zdravstvena dokumentacija se niti začasno ne hrani na bolniških posteljah ali na podoben način v bolniških sobah**.

(4) **Sledljivost notranje obdelave zdravstvene dokumentacije (npr. premeščanju zdravstvene dokumentacije med enotami) se zagotavlja prek rednih podatkov, ki so na voljo v sistemu HIPOKRAT**.

(6) Po izteku rokov za hrambo se zdravstvena dokumentacija **uniči** ali **anonimizira** ali **preda pacientu** (če gre za manj pomembno dokumentacijo s kratkimi roki hrambe) ali **preda pristojnemu arhivu**, če gre za odbrano arhivsko gradivo oziroma so za arhivsko hrambo izpolnjeni pogoji.

(7) Dokumentacija, ki nastane v pritožbenih postopkih oziroma postopkih reševanja sporov ter dokumentacija, ki nastane v okviru internih strokovnih nadzorov in drugih oblik nadzorov, se hrani **ločeno od zdravstvene dokumentacije** (izven zdravstvene mape) posameznega pacienta. Lokacija hrambe je v vodstvu KSRD.

X. IZBRIS OSEBNIH PODATKOV

30. člen
(način izbrisa podatkov)

(1) Za brisanje podatkov iz računalniških medijev se uporabi takšna metoda brisanja, da je nemogoča restavracija vseh ali dela 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 fizični obliki se uničijo na način, s katerim se zagotovi, da postane osebni podatek nerazpoznaven in neobnovljiv** (npr. rezalnik papirja).

(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 izpolnjena zdravniška potrdila, neustrezne nalepke za paciente) mora biti popolnoma oziroma nepovratno uničena (rezalnik, trganje) še isti dan ali najkasneje naslednji dan (če se uničuje v prostorih vodstva).

(5) Pri prenosu elektronskih nosilcev osebnih podatkov (npr. starih diskov) ali večjega števila nosilcev v papirni obliki (npr. uničevanje celotnih zdravstvenih map) 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 direktorica KSRD, in ki o uničenju sestavi tudi ustrezen zapisnik ali zaznamek. Uničevanje lahko namesto KSRD izvaja zunanji izvajalec, ki mora uničenje dokumentirati (kaj, kdaj in kako je bilo uničeno ter kdo je odgovorna oseba). Uničenje mora biti nepovratno.

XI. ODGOVORNOST ZA IZVAJANJE VARNOSTNIH UKREPOV IN POSTOPKOV

31. člen
(odgovorne osebe)

Za izvajanje in nadzorovanje postopkov in ukrepov za zavarovanje osebnih podatkov so odgovorni vsi uslužbenci, vključno z zunanjimi pogodbenimi izvajalci.

32. člen
(izjava o varovanju osebnih podatkov)

(1) Vsak, ki obdeluje osebne podatke, je dolžan izvajati v tem pravilniku predpisane postopke in ukrepe za zavarovanje podatkov, ter kot poklicno tajnost varovati podatke, za katere je zvedel oziroma bil z njimi seznanjen pri opravljanju svojega dela.

(2) Pred nastopom dela na delovno mesto, kjer se obdelujejo osebni podatki, mora uslužbenec ali druga oseba, ki opravlja delo ali uslugo v KSRD podpisati posebno **izjavo** (**PRILOGA H** tega pravilnika), ki jo opozarja in zavezuje k varovanju osebnih podatkov.

33. 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 materialno.

(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) KSRD mora v skladu 46. členom ZPacP vsak ugotovljen ali sporočen primer nedovoljenega sporočanja ali druge nedovoljene obdelave osebnih podatkov o pacientu, ne glede na voljo pacienta, posebej raziskati in ugotoviti morebitno odgovornost zdravstvenih delavcev, zdravstvenih sodelavcev ali drugih oseb ter primer pisno dokumentirati. O tem mora obvestiti pacienta, pristojnega zastopnika pacientovih pravic in Informacijskega pooblaščenca.

XII. KONČNE DOLOČBE

34. člen
(publiciteta)

(1) Ta pravilnik prejmejo oziroma se hrani:

- v prostorih vodstva (v elektronski in fizični obliki),
- v sprejemni pisarni, recepciji in študentski sobi,
- v obeh bolnišničnih oddelkih,
- pri vodjih posameznih organizacijskih enot,
- pri glavni medicinski sestri,
- pri vodji administracije,
- v skupnih mapah računalniškega omrežja in
- po potrebi v drugih primernih prostorih.

(2) Ta pravilnik je dostopen tudi pogodbenim obdelovalcem osebnih podatkov.

(3) Ta pravilnik predstavlja nasproti tretjim neupravičenim osebam poslovno skrivnost KSRD (39. člen ZGD-1).

35. člen
(razveljavitev, vakacijski rok in objava)

(1) Z dnem uveljavitve tega pravilnika preneha veljati Pravilnik o zavarovanju osebnih podatkov, z dne 20. 12. 2006.

(2) Ta pravilnik prične veljati v osmih dneh po sprejemu in njegovi objavi v skladu s prvim odstavkom 34. člena tega pravilnika.

Datum: 16. 3. 2015

Brigita KOLENC, univ. dipl. oec.
D I R E K T O R I C A