2. Даном ступања на снагу катастра непокретности за дио катастарске општине Приједор 1, град Приједор, стављају се ван снаге и престају да важе:

1) катастар земљишта за катастарске парцеле означене као к.ч. бр. 5506, 5507/2 и 5507/5, уписане у ПЛ број: 4170, катастарска општина Приједор 1,

2) земљишна књига за парцеле старог премјера означене као к.ч. бр. 1274/6 и 1274/7, уписане у зк. уложак број: 6489, катастарска општина СП Приједор.

3. Налаже се Подручној јединици Приједор да даном ступања на снагу катастра непокретности за дио катастарске општине Приједор 1, град Приједор, поступи у складу са тачком 2. овог рјешења.

4. Катастар непокретности за непокретности поближе описане у тачки 1. овог рјешења ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Српске".

Број: 21.04/951-1006/18
26. јула 2023. године Директор,
Бањалука Мр **Драган Станковић**, с.р.

Фонд здравственог осигурања Републике Српске

На основу члана 98. став 11. и члана 101. тачка 3) Закона о обавезном здравственом осигурању ("Службени гласник Републике Српске", бр. 93/22 и 132/22), уз Мишљење Министарства за научнотехнолошки развој, високо образовање и информационо друштво, број: 19.02/020-1155/23, од 15. маја 2023. године, и Сагласност министра здравља и социјалне заштите, број: 11/08-505-106/23, од 20. јуна 2023. године, Управни одбор Фонда здравственог осигурања Републике Српске, на 11. редовној сједници, одржаној 13. јула 2023. године, д о н о с и

ПРАВИЛНИК

О ЈЕДИНСТВЕНИМ МЕТОДОЛОШКИМ ПРИНЦИПИМА И СТАНДАРДИМА ЗА ФУНКЦИОНИСАЊЕ ИНТЕГРИСАНОГ ЗДРАВСТВЕНОГ ИНФОРМАЦИОНОГ СИСТЕМА

ГЛАВА I

ОСНОВНЕ ОДРЕДБЕ

Члан 1.

Овим правилником прописују се јединствени методолошки принципи и стандарди за функционисање Интегрисаног здравственог информационог система (у даљем тексту: ИЗИС), управљање ризиком и безбједношћу ИЗИС-а, интеграција постојећих информационих система базирана на размјени података веб-сервисима, садржај, изглед и коришћење подсистема за пословне функције учесника у процесу пружања здравствене заштите, односно за установе у којима се обезбјеђују подаци за здравствено осигурање или се пружа здравствена заштита обезбијеђена кроз уговоре о пружању здравствене заштите са Фондом здравственог осигурања Републике Српске (у даљем тексту: Фонд), изглед и садржај електронске картице здравственог радника.

Члан 2.

Поједини изрази који се употребљавају у овом правилнику имају сљедеће значење:

1) Примарни дата центар - сервер сала у пословној згради Фонда у Бањој Луци за управљање подацима који су прикупљени кроз ИЗИС,

2) SSO (енгл. Single sign-on) - процес аутентификације сесије корисника који дозвољава да се само једним уношењем приступних параметара изврши пријављивање и приступ у више апликација,

3) двофакторска аутентификација - начин аутентификације који, поред постојања безбједносне лозинке или кôда, подразумијева и постојање физичког медија као предуслова за аутентификацију,

4) Site to Site - начин повезивања двије (или више) различитих мрежа путем једног тунела,

5) DMZ (енгл. Demilitarized zone) - физичка или логичка подмрежа која одваја локалну мрежу (LAN) од других непоузданих мрежа,

6) IPSec (енгл. Internet Protocol Security) - протокол за успостављање безбједне конекције између информационих система на бази интернет протокола,

7) VPN (енгл. Virtual private network) - начин повезивања код којег виртуелна приватна мрежа проширује приватну мрежу преко јавне мреже као што је интернет, те омогућава размјену података на начин као да су рачунарски и комуникациони уређаји директно повезани са приватном мрежом,

8) хардвер - физичка компонента информационог система,

9) софтвер - сваки оперативни систем, програм, корисничка и сервисна апликација,

10) криптографска заштита - систем заштите података и информационих система који осигурава безбједан пренос података кроз рачунарску и телекомуникациону мрежу,

11) информатички медиј - сваки медиј на којем је могуће преносити или складиштити податке у електронском облику,

12) безбједно складиште - сеф, каса или други простор за складиштење података опремљен уређајем који спречава неовлашћени приступ ускладиштеним подацима,

13) ризик - потенцијални узрок који може нанијети штету податку или информационом систему у којем се користе подаци,

14) безбједна локација - мјесто за чување података складиштених на информатичком медију у радним просторијама или изван радних просторија субјекта, опремљено техничким уређајима којима се спречава неовлашћени приступ уређајима и подацима,

15) административна зона - простор или просторија у објекту у којем се чувају подаци и уређаји на којима су смјештени подаци и који захтијева одговарајућу физичку заштиту,

16) криптована заштита података - примјена програмских рјешења или уређаја за заштиту података који осигуравају повјерљивост, цјеловитост и доступност података,

17) безбједни податак - податак који у складу са прописаним безбједносним мјерама није доступан неовлашћеним лицима у процесу управљања тим податком (обрада, измјена, пренос, складиштење, тј. архивирање, копирање, брисање, уништавање),

18) политика безбједности информационог система - скуп правила, смјерница и поступака који дефинишу на који начин информациони систем учинити безбједним, укључујући безбједност технологије, као и информација које информациони систем садржи,

19) дигитално представљање - начин употребе електронске картице са циљем добијања права на рад са апликацијама које су инсталиране на серверима Фонда,

20) дигитални цертификат - скуп података у електронском облику који представља електронски идентитет у разним електронским интеракцијама,

21) интегрисано електронско коло - коло које се састоји од процесора и меморије, неодвојиво је од пластичне подлоге и у себи садржи податке о власнику картице,

22) ПИН кôд - број познат само власнику електронске картице и користи се приликом приступа садржају контактног меморијског модула који се налази на картици (дигитално представљање),

23) администратор - лице запослено у здравственој установи које је овлашћено за спровођење правила безбједности дефинисаних од стране Фонда,

24) суперадминистратор - овлашћено стручно лице Фонда које унутар рада Дата центра управља системом,

25) администратор са пренесеним правима администрације - овлашћено лице које врши администрацију на нивоу основних организационих јединица (дома здравља, клиничког центра, болнице и сл.),

26) аутентификација - процес утврђивања идентитета корисника који приступа систему на основу приступних параметара,

27) ауторизација - права корисника на систему након успјешне аутентификације,

28) ОИБ - Одјељење за информациону безбједност унутар Ресора за информационо друштво у оквиру Министарства за научнотехнолошки развој, високо образовање и информационо друштво, које врши непосредан надзор и контролу над спровођењем информационе безбједности.

ГЛАВА II

ЈЕДИНСТВЕНИ МЕТОДОЛОШКИ ПРИНЦИПИ И СТАНДАРДИ ЗА ФУНКЦИОНИСАЊЕ ИНТЕГРИСАНОГ ЗДРАВСТВЕНОГ ИНФОРМАЦИОНОГ СИСТЕМА

Члан 3.

ИЗИС представља централни електронски систем у коме се чувају и обрађују: сви медицински и здравствени подаци пацијената, подаци здравствених радника и сарадника, подаци здравствених установа, здравствене интервенције и услуге извршене у здравственим установама, подаци електронских упутница и електронских рецепата, подаци о заказивању за специјалистичке прегледе, дијагностичке процедуре и хируршке интервенције.

Члан 4.

ИЗИС се темељи на информационо-комуникационим технологијама, односно на расположивости комуникација и информација у систему здравствене заштите, с циљем повезивања у јединствени информациони систем различитих учесника, локација, активности и процеса здравствене заштите.

Члан 5.

(1) ИЗИС обезбјеђује јединство података у здравству и јединствену информационо-комуникацијску инфраструктуру за управљање збиркама података и пренос података.

(2) ИЗИС омогућава унос, прикупљање, складиштење и размјену података који се односе на здравствени систем у Републици Српској.

(3) Подаци се чувају и одржавају у централној бази података.

(4) Извор података су здравствене установе, а здравствени радници и здравствени сарадници прикупљају податке.

(5) Интеграција здравствене установе са ИЗИС-ом и прикупљање података је могућа на два начина:

1) користећи апликације Централног апликативног система,

2) користећи сервисе Централног интеграционог система.

(6) Централни апликативни систем састоји се од одређеног броја апликација које у склопу рада појединих подсистема омогућавају прикупљање података.

(7) Апликације Централног апликативног система ИЗИС-а намијењене су јавним здравственим установама које немају адекватне или имају неадекватне постојеће информационе системе.

(8) За установе које задржавају сопствени информациони систем у употреби Фонд пружа могућност интеграције путем веб-сервиса (Централни интеграциони систем ИЗИС-а).

Члан 6.

(1) Администрацију, управљање и развој ИЗИС-а врши Фонд, који представља централно мјесто за размјену медицинских података и обављања кључних улога као што су генерисање, похрањивање и размјена медицинских података између свих установа које користе ИЗИС.

(2) Задаци Фонда при администрацији и управљању ИЗИС-ом су:

1) управљање Дата центром - примарном и секундарном локацијом,

2) обезбјеђивање поузданости и доступности цјелокупног система,

3) обезбјеђивање функционалности, капацитета и перформанси система неопходних за пружање адекватне подршке пословним процесима здравствених установа,

4) централизовано управљање апликацијама, регистрима и шифарницима,

5) контрола приступа, поступања и коришћења медицинских података,

6) обезбјеђивање сервиса за размјену медицинских и осталих података,

7) пружање неопходне стручне помоћи корисницима ИЗИС-а.

ГЛАВА III

УПРАВЉАЊЕ РИЗИКОМ И БЕЗБЈЕДНОШЋУ ИНТЕГРИСАНОГ ЗДРАВСТВЕНОГ ИНФОРМАЦИОНОГ СИСТЕМА

1. Управљање ризиком

Члан 7.

(1) Безбједносни ризик представља могућност реализације неког нежељеног догађаја који може негативно утицати на повјерљивост, интегритет и расположивост информационих ресурса ИЗИС-а (хардвер, софтвер, људски ресурси, подаци и сл.).

(2) Управљање ризиком дефинише се као процес идентификације оних фактора који могу негативно утицати на повјерљивост, интегритет и расположивост рачунарских ресурса и њихова анализа у смислу вриједности појединих ресурса и трошкова њихове заштите.

(3) Процес управљања безбједносним ризицима састоји се и спроводи у три фазе:

1) процјена ризика,

2) умањивање ризика,

3) испитивање и анализа.

(4) Директор Фонда рјешењем именује лице задужено за процес управљања безбједносним ризицима и дефинише овлашћења и одговорности.

Члан 8.

(1) Лице одговорно за управљање ризиком процес процјене ризика спроводи идентификацијом и класификацијом ресурса, идентификацијом пријетњи, идентификацијом рањивости, анализом постојећих контрола, анализом вјероватноће појаве нежељених догађаја и могућих посљедица и одређивањем ризика, након чега даје препоруке за умањивање ризика.

(2) Након завршеног процеса процјене ризика према ставу 1. овог члана, лице одговорно за управљање ризиком директору Фонда доставља извјештај.

Члан 9.

(1) Опције за управљање ризиком су:

1) умањивање ризика - подразумијева спровођење одговарајућих безбједносних контрола са циљем умањивања идентификованог ризика,

2) трансфер ризика - ризик и трошкови у случају његове реализације пребацују се некој другој организацији,

3) прихватање ризика - поступак којим се ризик прихвата као такав без спровођења било каквих безбједносних контрола, након што кост-бенефит анализе (енгл. cost/benefit analisis, CBA, анализа предности и трошкова) покажу да је већи трошак улагати у заштиту ресурса него што представља његов губитак.

(2) Спровођењем одговарајућих безбједносних контрола и механизама, прихватљивих са финансијског и техничког становишта, безбједносни ризик своди се на прихватљив ниво.

(3) Ризик који остаје након спровођења безбједносних контрола назива се резидуалним ризиком и он подразумијева све оне пријетње и рањивости за које се сматра да не захтијевају додатни третман за умањивање постојећег ризика.

(4) Присутност резидуалног ризика посљедица је спроведених кост-бенефит анализа којима је установљено да су трошкови заштите већи од трошкова у случају његове реализације.

(5) Директор Фонда, на основу изнесених резултата према извјештају из члана 8. овог правилника, одлучује о томе који ће се ризик умањивати и на који начин, а који ће се прихватити онаквим какав јесте, те стручна служба Фонда спроводи одговарајуће безбједносне контроле.

Члан 10.

(1) Ризик се уклања по приоритету који се одређује на основу степена безбједности података који могу бити погођени и на основу кост-бенефит анализе.

(2) Прво се спроводе рјешења која су финансијски најприхватљивија, а резултат који показују су што квалитетније, поуздане безбједносне контроле са минималним утицајем на мисију и пословне процесе.

(3) Умањивању ризика приступа се методолошки и поступак се спроводи у седам фаза:

1) одређивање приоритетних акција,

2) евалуација препоручених безбједносних контрола,

3) анализа добијеног и уложеног,

4) одабир безбједносних контрола,

5) подјела одговорности,

6) израда плана за спровођење безбједносних контрола,

7) спровођење контрола.

(4) Испитивање и анализа, односно процјена ризика спроводи се једном годишње.

2. Управљање безбједношћу

Члан 11.

(1) Стручни надзор и контрола спровођења информационе безбједности врше се у складу са прописима којима се уређује област информационе безбједности.

(2) Фонд спроводи интерну ревизију безбједносних аспеката информационог система.

Члан 12.

(1) Административне зоне се класификују на јавне административне зоне и безбједне административне зоне.

(2) Јавним административним зонама се класификују административне зоне у којима се налазе или су у њиховој непосредној близини само јавни подаци.

(3) Безбједним административним зонама се класификују административне зоне које нису јавне и могу према степену безбједности података, опреме или ресурса који се у тој зони налази имати сљедеће степене безбједности:

1) први степен безбједности - ако садржи најмање један податак, опрему или ресурс првог степена безбједности,

2) други степен безбједности - ако садржи најмање један податак, опрему или ресурс другог степена безбједности,

3) трећи степен безбједности - ако садржи најмање један податак, опрему или ресурс трећег степена безбједности.

(4) Простор у коме се налазе сервери, мрежна или комуникациона опрема информационог система организује се као безбједна административна зона, а степен безбједности тих зона одређују податак, опрема или ресурс који се у тој зони налази.

Члан 13.

(1) Мјере информационе безбједности физичке заштите Фонд спроводи ради спречавања неовлашћеног или насилног уласка лица у објекте и просторије у којима се налазе подаци, односно уређаји са подацима, спречавања и откривања злоупотреба података од стране запослених, као и откривања и реаговања на ризике.

(2) Најмање једном годишње Фонд процјењује ефикасност мјера информационе безбједности физичке заштите објеката и просторија у којима се налазе подаци, као и у случају промјене намјене локације или елемената у информационом систему.

(3) Фонд обезбјеђује контролу лица на улазима и излазима из објекта или простора у којима се налазе подаци и о томе се води евиденција ради спречавања неовлашћеног изношења података или спречавања уношења недозвољених предмета којима се може угрозити безбједност података.

(4) Сви меморијски медији који служе за смјештај резервних копија података смјештени су на безбједној локацији ван објекта/просторије у којој се налазе оригинали тих података.

(5) Просторије у којима се смјештају меморијски медији са резервним копијама података су степена безбједности који одговара степену безбједности података који се на медијима налазе и задовољавају спецификације произвођача медија за њихово безбједно складиштење.

Члан 14.

(1) Подаци у ИЗИС-у могу имати један од сљедећих степена безбједности:

1) први степен безбједности - одређује се ради спречавања настанка непоправљиве штете по интересе субјекта,

2) други степен безбједности - одређује се ради спречавања настанка изузетно штетне посљедице по интересе субјекта,

3) трећи степен безбједности - одређује се ради спречавања настанка штете по интересе субјеката,

4) четврти степен безбједности - одређује се ради спречавања настанка штете за рад, односно обављање задатака и послова субјекта који их је одредио,

5) пети степен безбједности (у даљем тексту: јавни подаци) - подаци за које се сматра да не могу узроковати настанак било какве штете за субјекат који их је одредио.

(2) Лични подаци корисника ИЗИС-а се квалификују као подаци трећег степена безбједности.

Члан 15.

(1) Корисницима ИЗИС-а додјељују се само оне привилегије неопходне за приступ подацима који су неопходни за обављање њиховог посла, а са циљем ограничавања штете која може настати усљед безбједносних инцидената, грешака или неауторизоване употребе података и ресурса информационог система.

(2) Фонд дефинише списак права приступа (улога) у систему и даје препоруке у вези са приступом и обрадом података пацијента.

(3) Надлежни администратор здравствене установе корисницима система омогућава права приступа подацима.

(4) Обавезно је раздвајање дужности надлежних администратора и корисника информационог система који раде са подацима одређеног степена безбједности.

(5) Сви витални дијелови информационог система ИЗИС-а (физички и виртуелни сервери, комуникациона опрема, апликативни сервери, системи за управљање базама података и др.) имају задужене администраторе који су

одговорни за поузданост и расположивост информационог система.

(6) Фонд обезбјеђује да запослена лица Фонда и здравствених установа која имају одобрен приступ личним подацима корисника здравствене заштите у ИЗИС-у потпишу изјаву да су упозната са обавезама и одговорностима у вези са законитим приступањем личним подацима и чувањем тајности личних података садржаних у ИЗИС-у.

(7) Изјава из става 6. овог члана потписује се на обрасцу који се налази у Прилогу 1 овог правилника и чини његов саставни дио.

Члан 16.

(1) Копирање безбједних података врши се на начин који осигурава да неће доћи до неовлашћеног копирања безбједних података или нарушавања интегритета података који се копирају.

(2) Уништавање безбједних података на медијима за складиштење података чији је животни вијек истекао или који ће се даље користити у друге сврхе обавља се одговарајућим рачунарским програмима, уређајима и софтверским алатима.

(3) Сви информациони системи који се користе за пренос и размјену безбједних података су осигурани средствима која обезбјеђују адекватну криптографску заштиту.

Члан 17.

(1) Фонд спроводи Политику безбједности ИЗИС-а којом се прописују: политика класификације информација и података, политика управљања ризицима, политика контроле приступа, e-mail политика, политика енкрипције, политика приступа интернету, политика креденцијала за аутентификацију, политика физичке безбједности, политика удаљеног приступа, безбједносна политика сервера, безбједносна политика мрежних уређаја, безбједносна политика опреме и DMZ, VPN политика, екстранет политика, политика бежичне комуникације, политика радних станица, политика провјере рањивости, политика одговора на безбједносне инциденте, безбједносна политика мобилних уређаја и антивирус политика.

(2) Политика безбједности ИЗИС-а из става 1. овог члана објављује се на интернет страници Фонда.

Члан 18.

(1) Апликативни софтвер и сервиси имају уграђене контроле исправности, потпуности и конзистентности података који се уносе, мијењају, обрађују и генеришу.

(2) У складу са процјеном ризика израђују се апликативни и системски записи ради откривања неовлашћених приступа и радњи у информационом систему, идентификације проблема, реконструисања догађаја и утврђивања одговорности.

(3) Апликативни и системски записи из става 2. овог члана чувају се најмање двије године.

Члан 19.

Систем управљања приступом ресурсима информационог система обухвата дефинисање одговарајућих управљачких, логичких и физичких контрола, управљање корисничким правима приступа који обухвата процесе евидентирања, ауторизације, идентификације и аутентификације, надзора права приступа и управљање удаљеним приступима.

Члан 20.

(1) Базе података се складиште на преносиве информатичке медије најмање једном дневно, седмично, мјесечно и годишње за потребе обнове базе података, о чему се води посебна евиденција, а овлашћени администратор свакодневно провјерава исправност дневних безбједносних копија.

(2) Процес управљања безбједносним копијама (енгл. backup) укључује процедуре израде безбједносних копија, њиховог складиштења, тестирања рестаурације података са безбједносних копија података, као и адекватан транспорт и предају безбједносних копија, да би се обезбиједила расположивост података у случају потребе, омогућио опоравак, односно поновно успостављање критичних (виталних) пословних процеса у захтијеваном времену.

(3) Процес управљања безбједносним инцидентима обухвата процедуре за пријављивање, класификацију, праћење и извјештавање о безбједносним инцидентима и дефинисање одговорности и процедура које омогућавају брз и ефикасан одговор у случају нарушавања безбједности информационог система.

Члан 21.

(1) Корисници ИЗИС-а одговарају за све активности извршене на рачунарској опреми на радном мјесту употребом њихових креденцијала за приступ информационом систему (корисничко име и лозинка, дигитални цертификат на паметној картици и др.).

(2) Корисници ИЗИС-а креденцијале за приступ информационом систему чувају у тајности, мијењају их према дефинисаној Политици безбједности ИЗИС-а из члана 17. овог правилника, траже њихову промјену од надлежног администратора уколико постоји сумња да је њихова тајност нарушена и користе за потребе за које су им и издати.

ГЛАВА IV

ИНТЕГРАЦИЈА ПОСТОЈЕЋИХ ИНФОРМАЦИОНИХ СИСТЕМА БАЗИРАНА НА РАЗМЈЕНИ ПОДАТАКА ПУТЕМ ВЕБ-СЕРВИСА

Члан 22.

(1) Уколико здравствена установа или друго правно лице посједује и задржава сопствени информациони систем у употреби, тај систем се интегрише са ИЗИС-ом.

(2) Ради успостављања и очувања интегралности ИЗИС-а, здравствена установа и друго правно лице, уз стручну подршку Фонда, обезбјеђују да постојећи и други системи за прикупљање, чување и обраду података из става 1. овог члана, као и систем извјештавања, буду компатибилни.

(3) Здравствена установа или друго правно лице из става 1. овог члана одржавају сопствени информациони систем.

Члан 23.

Предмет приступа, преноса и размјене података из постојећих информационих система који се са ИЗИС-ом размјењују путем веб-сервиса су подаци из основне и помоћне медицинске документације који се воде у здравственим установама.

Члан 24.

(1) Интеграција са ИЗИС-ом, те приступ подацима из евиденција наведеним у члану 23. овог правилника путем Централног интеграционог система ИЗИС-а врши се на основу захтјева за интеграцију са ИЗИС-ом који здравствена установа или друго правно лице подноси Фонду.

(2) На основу захтјева из става 1. овог члана, Фонд врши евидентирање установе у Јединствени регистар здравствених установа ИЗИС-а и евидентирање здравствених радника у Јединствени регистар здравствених радника како би се добио јединствени идентификатор установе за размјену података, односно јединствени идентификатор здравственог радника на основу којег се здравствени радник исправно идентификује на нивоу ИЗИС-а.

(3) Интеграција са ИЗИС-ом обухвата комуникационо увезивање локација здравствене установе, опремање читачима картица и тестирање и верификацију размјене података путем веб-сервиса према HL7 стандарду, након чега се између Фонда и здравствене установе закључује споразум уз размјену докумената који потврђују прихватање процедура и података о комуникационим параметрима за интеграцију са ИЗИС-ом.

ГЛАВА V

САДРЖАЈ, ИЗГЛЕД И КОРИШЋЕЊЕ ПОДСИСТЕМА

Члан 25.

(1) За функционисање ИЗИС-а развијају се и користе одговарајући системи, подсистеми и сервиси за пословне функције свих учесника у процесу пружања здравствене заштите, односно за све установе у којима се обезбјеђују подаци за здравствено осигурање или се пружа здравствена заштита обезбијеђена кроз уговоре о пружању здравствене заштите са Фондом.

(2) ИЗИС чине информациони системи здравствених установа, Фонда и других правних лица која у свом пословању сарађују са системом здравствене заштите и са Фондом успостављају сарадњу по овом питању.

(3) Подсистеми који се развијају и користе у складу са ставом 1. овог члана су:

1) Централни апликативни систем ИЗИС-а са подсистемима:

1. подсистем примарне здравствене заштите,

2. подсистем специјалистичко-консултативне заштите (примарни и ванболнички),

3. болничко-клинички подсистем;

2) Централни интеграциони систем са подсистемима:

1. подсистем електронског здравственог картона - подсистем за електронску размјену здравствених података,

2. подсистем електронских упутница - еУпутница,

3. подсистем електронских рецепата - еРецепт,

4. подсистем за електронску размјену немедицинских података уз формирање јединствених регистара;

3) подсистем за приступ медицинским подацима од стране пацијента;

4) подсистем за администрацију ИЗИС-а, који чине:

1. подсистем управљања ресурсима и шифарницима,

2. подсистем управљања и подршке корисницима здравствене заштите;

5) подсистем за извјештаје и пословну интелигенцију (енгл. Business Intelligence, BI);

6) подсистем за лабораторијску и радиолошку дијагностику;

7) подсистем за електронску здравствену картицу и идентификациону електронску картицу здравственог радника;

8) остали подсистеми.

1. Функционисање Централног апликативног система

Члан 26.

Централни апликативни систем ИЗИС-а састоји се од апликација:

1) примарне здравствене заштите,

2) специјалистичко-консултативне здравствене заштите (примарни и ванболнички),

3) болничко-клиничког подсистема,

4) подсистема за администрацију.

Члан 27.

Фонд обезбјеђује функционисање и техничку администрацију апликативних сервера, те даљи развој и унапређење апликација Централног апликативног система ИЗИС-а.

Члан 28.

(1) Омогућавање приступа здравствених установа апликацијама врши Фонд на основу писменог захтјева здравствене установе.

(2) Омогућавање приступа састоји се од комуникационог увезивања, те креирања приступних параметара надлежног администратора.

(3) Даље управљање приступом корисника здравствене установе појединим апликацијама врши надлежни администратор здравствене установе уз дефинисање и додјељивање права над појединим апликацијама.

(4) Приступ корисника апликацијама могућ је на два начина:

1) преко корисничког имена и лозинке и

2) користећи идентификациону електронску картицу здравственог радника (у даљем тексту: електронска картица).

(5) Обје врсте приступа засноване су на SSO приступу (енгл. Single sign-on).

Члан 29.

(1) Корисници Централног апликативног система ИЗИС-а су овлашћена лица која у склопу обављања својих редовних активности, а у складу са пословним процесима, користе једну или више апликација наведеног подсистема.

(2) Управљање корисницима Централног апликативног система ИЗИС-а врши се кроз подсистем за управљање ресурсима и шифарницима.

(3) Управљање корисницима врши се од стране овлашћених лица - администратора који имају додијељено право приступа, те администраторске привилегије унутар наведеног подсистема.

(4) Нивои администрације су:

1) администрација на нивоу цјелокупног система - суперадминистратори,

2) администрација на нивоу основне организационе јединице - администратори са пренесеним правима администрације.

Члан 30.

(1) Процес управљања корисницима Централног апликативног система ИЗИС-а подразумијева:

1) дефинисање, креирање и управљање приступним параметрима,

2) дефинисање, креирање и управљање апликацијама, те правима на појединим апликацијама,

3) креирање захтјева за електронске картице и

4) управљање електронским картицама.

(2) Основну организациону структуру формира Фонд у складу са структуром организационих јединица у систему здравствених установа.

(3) Свака од основних организационих јединица именује администратора којем се додјељују одређена права унутар организационих јединица за које је надлежан, те у оквиру те јединице је могуће даље управљање и формирање организационе структуре, у складу са потребама.

Члан 31.

(1) Фонд додјељује право приступа администраторима на нивоу основне организационе јединице на основу попуњеног захтјева основне организационе јединице која уз захтјев доставља и попуњен Безбједносно-технички образац, који се налази у Прилогу 2 овог правилника и чини његов саставни дио (у даљем тексту: БТ образац).

(2) Приликом пријаве и дефинисања права приступа корисника, администратор у здравственој установи креира налог на основу попуњеног и овјереног БТ обрасца из става 1. овог члана у који се уноси: име, презиме и ЈМБ корисника, списак апликација које је потребно додијелити кориснику и списак рола (улога) по појединим апликацијама које је неопходно додијелити кориснику.

(3) Фонд у електронској и писаној форми чува податке о БТ обрасцима за администраторе из здравствених установа, а администратор здравствене установе у електронској и писаној форми чува податке о БТ обрасцима корисника.

Члан 32.

(1) Аутентификација корисника подразумијева процес утврђивања идентитета корисника који приступа систему на основу приступних параметара.

(2) Одређивање аутентификацијских параметара и даље управљање корисницима Централног апликативног система ИЗИС-а врши надлежни администратор.

(3) Приликом креирања корисничког имена користе се почетна слова имена и презимена корисника плус прве четири цифре матичног броја, а латинична слова Č, Ć, Š, Đ, Ž и Dž мијењају се редом са C, C, S, DJ, Z и DZ.

(4) У случају да корисничко име већ постоји, користи се сљедеће слово у низу из имена.

(5) Уколико лице има више имена и презимена, користе се почетна слова свих имена и презимена.

(6) Промјеном имена или презимена корисника, након креирања налога, не врши се креирање новог, већ се задржава постојеће корисничко име.

(7) Иницијалну лозинку одређује администратор, а коју корисник мијења након првог пријављивања на систем.

(8) Након одређивања приступних параметара, ти подаци се достављају кориснику у запечаћеној коверти.

(9) Када корисник прелази из једне у другу организациону јединицу врши се одјава у једној организационој јединици, те активирање корисничких параметара у другој организационој јединици уз праћење историје кретања корисника кроз систем.

(10) Одјавом корисника врши се деактивирање (закључавање) корисничког имена у систему, уз аутоматско поништавање картице здравственог радника.

Члан 33.

(1) Управљање ауторизацијом подразумијева додјељивање одговарајућих улога (рола) корисницима у систему.

(2) Креирање иницијалног списка апликација и улога (рола по апликацијама) и даље управљање апликацијама и ролама по појединим апликацијама Централног апликативног система ИЗИС-а врше администратори Фонда, док ауторизацију корисника (додјељивање дефинисаних рола) врши надлежни администратор здравствене установе на основу достављеног БТ обрасца из члана 31. овог правилника.

(3) Кориснику се додјељују одговарајућа права на појединим апликацијама која омогућавају приступ појединим формама унутар апликације и даљи рад на тим формама.

(4) Права на податке, те даља размјена података између подсистема Централног апликативног система ИЗИС-а врши се на основу надлежности корисника и здравствене установе.

2. Функционисање Централног интеграционог система

Члан 34.

Централни интеграциони систем ИЗИС-а састоји се од сљедећих подсистема:

1) подсистем електронског здравственог картона (подсистем за електронску размјену здравствених података),

2) подсистем електронских упутница,

3) подсистем електронских рецепата,

4) подсистем за електронску размјену немедицинских података.

Члан 35.

(1) Омогућавање приступа систему од стране здравствених установа које задржавају сопствени информациони систем у употреби врши Фонд на основу захтјева установе, у писаној форми.

(2) Омогућавање приступа састоји се од комункационог увезивања, евидентирања здравствене установе у Јединственом регистру здравствених установа, одређујући при томе јединствени идентификатор здравствене установе на нивоу система.

(3) Евидентирање установе у регистру обављају администратори Фонда.

(4) За идентификацију здравствене установе при размјени података користи се јединствени идентификатор.

Члан 36.

(1) Размјена података између Фонда и здравствене установе врши се преко подсистема електронског здравственог картона.

(2) Све здравствене установе које користе локалне здравствене информационе системе преносе информације у ИЗИС путем Централног подсистема за електронску размјену здравствених информација коришћењем HL7 стандарда (CDA R2).

(3) Подсистем електронског здравственог картона подржава спремање и обраду сљедећих клиничких докумената:

1) извјештај о прегледу на примарном нивоу,

2) извјештај о ванболничком/амбулантном лијечењу,

3) извјештај о хоспитализацији,

4) упутницу,

5) рецепт.

(4) Подсистем електронског здравственог картона подржава преузимање сажетка медицинских података пацијента из електронског здравственог картона у реалном времену (енгл. On-demand option).

(5) Подсистем електронског здравственог картона подржава претрагу и преузимање појединачних докумената регистрованих у Регистру докумената (енгл. Document Registry).

(6) Подсистем електронског здравственог картона омогућава увид у појединачна документа из Регистра докумената (енгл. Document Repository).

Члан 37.

(1) Корисници подсистема за електронску размјену медицинских/здравствених података су све установе које приступају систему, задржавајући сопствени информациони систем у употреби (размјена података између два независна информациона система).

(2) Омогућавање приступа систему врши Фонд на основу достављеног захтјева од стране установе која се интегрише и састоји се од:

1) комуникационог увезивања,

2) дефинисања приступних параметара.

(3) Приликом дефинисања приступних параметара врши се унос организационе јединице у систем уз одређивање јединственог идентификатора на нивоу система који се користи при даљој размјени података.

Члан 38.

(1) Приступ подацима од стране пацијента врши се путем подсистема за приступ медицинским подацима од стране пацијента.

(2) Подсистем за приступ медицинским подацима пацијента омогућава:

1) веб базиран приступ порталу и приступ кроз мобилну апликацију,

2) приступ свим веб-страницама кроз јединствено пријављивање на систем (SSO - Single Sign On),

3) слање информација осигураницима путем имејл-порука,

4) приступ носиоцу осигурања својим члановима уже породице (дјеца и супружници), те претрагу и преглед свих медицинских података за своје чланове породице,

5) портал са веб базираним интерфејсом, компатибилан са тренутно најзаступљенијим веб-претраживачима: Internet Explorer, Google Chrome, Mozilla Firefox и Safari.

(3) Пацијенту је омогућен приступ подсистему из става 1. овог члана пријавом на тај подсистем.

(4) Пријавом се одређују параметри неопходни за приступ подсистему из става 1. овог члана, а ти приступни параметри достављају се на имејл-адресу пацијента.

ГЛАВА VI

ИЗГЛЕД И САДРЖАЈ ЕЛЕКТРОНСКЕ КАРТИЦЕ ЗДРАВСТВЕНОГ РАДНИКА

Члан 39.

(1) Фонд доставља електронску картицу јавној здравственој установи која има одобрен приступ Централном апликативном систему ИЗИС-а.

(2) Електронска картица омогућава приступ Централном апликативном систему ИЗИС-а и уручује се здравственом раднику и здравственом сараднику запосленом у здравственој установи из става 1. овог члана (у даљем тексту: корисници електронске картице), у складу са њиховим овлашћењима за обављање одређених послова.

(3) Израда и издавање електронске картице врши се примјеном лиценцираног софтверског програма у власништву Фонда.

(4) У периоду израде, дистрибуције и уручења електронске картице приступ систему се врши на основу креираног корисничког имена и лозинке.

(5) Приликом креирања корисничког имена и лозинке врши се аутоматско подношење захтјева за електронску картицу.

Члан 40.

(1) Електронска картица је идентификациони документ димензија 85,6 mm · 53,98 mm, дебљине 0,76 mm или 0,96 mm (по ISO стандарду ISO/IEC 7810, 7816/1 и 7816/2), израђена од пластике и садржи:

1) назив здравствене установе у којој је корисник електронске картице запослен,

2) идентификациони број корисника електронске картице,

3) идентификациони број електронске картице,

4) име и презиме корисника електронске картице са фотографијом,

5) ознаку да се ради о електронској картици,

6) интегрисано електронско коло са уписаним дигиталним цертификатима за доказивање идентитета.

(2) Технологија израде чипа електронске картице је Smart контактни микропроцесорски чип CPU.

(3) Интегрисано електронско коло има минимално сљедеће карактеристике: Chip CC certification EAL 5+, ROM memory 80 KB, EEPROM memory 400 KB, Internal clock 66 MHz, External clock up to 10 MHz, Voltage range 1.62 V - 5.5 V, Temperature range -25 ºC to +85 ºC, Technology CMOS 0.13 microns, Memory rewrite > 500 K r/w cycles, Data retention > 10 years, Crypto processor (1408 bit), Onboard key generation, True Random Number Generator и CPU RISC 32 bit.

(4) Рок важења електронске картице је неограничен.

Члан 41.

(1) Здравствена установа својим интерним актима уређује правила за додјелу права корисницима електронске картице, начин одређивања корисника и начин вођења евиденције издатих картица и одговара за додјелу права за доставу података и приступ Централном апликативном систему и Подсистему за администрацију ИЗИС-а.

(2) Администратор здравствене установе или друго лице које овласти здравствена установа води регистар корисника електронске картице.

(3) Здравствена установа приликом одређивања новог администратора спроводи прописану процедуру издавања електронске картице.

Члан 42.

(1) Администратор здравствене установе на основу налога, у писаној форми, руководиоца електронским путем кроз Подсистем за администрацију ИЗИС-а доставља Фонду захтјев за израду електронске картице за овлашћене кориснике електронске картице.

(2) Фонд обезбјеђује набавку и израду електронске картице и доставља их здравственој установи која је уручује кориснику здравствене картице.

(3) Активирање електронске картице врши надлежни администратор.

(4) Здравствена установа води евиденцију својих запослених лица која имају право да приступају подацима или достављају податке у евиденције.

(5) Обим права приступа апликацијама корисника електронских картица утврђује здравствена установа према својим организационим и техничким могућностима.

Члан 43.

(1) Уручење електронске картице врши се у здравственој установи уз коришћење апликације за рад са електронским картицама.

(2) Уручење електронске картице врши се лично, предајом електронске картице у затвореној коверти која у себи садржи и кôд за потврду преузимања картице, ПИН кôд, упутство о обавезама и начину коришћења картице и непотписану Изјаву о преузимању идентификационе електронске картице здравственог радника (у даљем тексту: Изјава).

(3) Образац Изјаве из става 2. овог члана налази се у Прилогу 3 овог правилника и чини његов саставни дио.

Члан 44.

(1) Лице којем је додијељена електронска картица, прије активирања картице потписује Изјаву из члана 43. став 2. овог правилника, а копија те изјаве чува се у досијеу корисника електронске картице из те здравствене установе.

(2) Потписивањем Изјаве из члана 43. став 2. овог правилника корисник електронске картице потврђује своју сагласност на прописане услове и начин коришћења електронске картице, као и да је упознат са садржајем прописа за коришћење електронске картице.

(3) На основу потписане Изјаве из члана 43. став 2. овог правилника, администратор здравствене установе уноси кôд за потврду преузимања електронске картице, те се електронска картица сматра активираном.

(4) Корисник електронске картице од момента активирања стиче могућност коришћења те картице.

(5) Активирањем електронске картице поништава се раније издата електронска картица за исто корисничко име, врши се аутоматско активирање нове електронске картице и врши се активирање корисника у подсистему за управљање корисницима.

(6) Електронску картицу није могуће замијенити, а оштећена или изгубљена картица поништава се и враћа Фонду, након тога се подноси захтјев за издавање нове електронске картице.

(7) У случају промјене личних података корисника електронске картице, подноси се захтјев за издавање нове картице.

(8) Поништавање електронске картице врши се кроз апликацију за управљање корисницима подсистема за администрацију ИЗИС-а на иницијативу здравствене установе која је поднијела захтјев за издавање електронске картице и врши се од момента подношења пријаве којом се тражи поништавање.

(9) Деблокада електронске картице подразумијева промјену ПИН кôда на захтјев корисника електронске картице у случају када се због нетачног уноса ПИН кôда електронска картица закључа, а деблокаду обавља надлежни администратор здравствене установе кроз апликацију за управљање корисницима подсистема за администрацију ИЗИС-а на основу поднесеног писменог захтјева корисника електронске картице.

Члан 45.

Корисник електронске картице одговоран је за правилну употребу и овлашћено коришћење електронске картице, на начин да чува картицу од оштећења и да без одлагања администратору пријављује оштећење, нестанак или губитак електронске картице, а оштећену електронску картицу без одлагања предаје здравственој установи и у случају престанка радног односа без одлагања враћа електронску картицу здравственој установи.

Члан 46.

Здравствена установа на чији захтјев се издаје електронска картица спроводи сва правила прописана за систем приступа евиденцијама и заштиту података, обезбјеђује да свака промјена радног мјеста или радног статуса корисника електронске картице буде спроведена кроз подсистем за управљање корисницима, а преко администратора обезбјеђује поништавање нестале или изгубљене електронске картице, Фонду доставља оштећену или на други начин неупотребљиву картицу, води евиденцију писмених захтјева за деблокаду ПИН кôда електронске картице и упознаје кориснике електронске картице о њиховим правима и обавезама.

Члан 47.

Фонд, у електронској форми, води Регистар о издатим електронским картицама, који садржи податке о идентификационом броју и статусу електронске картице, називу здравствене установе којој је издата електронска картица, имену и презимену корисника електронске картице, насталим промјенама у вези са издатом електронском картицом и поништавању електронске картице.

ГЛАВА VII

ПРЕЛАЗНА И ЗАВРШНА ОДРЕДБА

Члан 48.

Електронска картица која је израђена и уручена здравственом раднику или здравственом сараднику у складу са Правилником о изгледу и садржају идентификационе електронске картице здравственог радника ("Службени гласник Републике Српске", број 99/19) задржава се у употреби и након истека рока важења који је одштампан на електронској картици, све док здравствени радник или здравствени сарадник има додијељена овлашћења за обављање одређених послова.

Члан 49.

Овај правилник ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Српске".

Број: 02/002-3054-6/23
13. јула 2023. године
Бања Лука

В.д. замјеника
предсједника Управног одбора,
Драгослав Топић, с.р.

ПРИЛОГ 1

ОБРАЗАЦ ИЗЈАВЕ О ПОВЈЕРЉИВОСТИ ЗА АДМИНИСТРАТОРЕ СИСТЕМА

_____
(име и презиме запосленог)

_____
(организациона јединица)

_____
(радно мјесто)

ИЗЈАВА

О ЧУВАЊУ ПОСЛОВНЕ ТАЈНЕ, ПРИСТУПУ РАЧУНАРСКИМ СИСТЕМИМА, ПРАВИМА ИНТЕЛЕКТУАЛНОГ ВЛАСНИШТВА, ОБАВЕЗИ ПОВРАТА ИНФОРМАЦИЈА И ПРАВУ НАДЗОРА

Ја,_____, под материјалном и кривичном одговорношћу, изјављујем:

- да ћу чувати тајност личних података и придржавати се утврђеног начина обезбјеђивања личних података, у складу са обавезом према прописима којима се уређује област заштите личних података,

- да ћу чувати као професионалну тајну све што сазнам о свим подацима који се налазе у Интегрисаном здравственом информационом систему Републике Српске (у даљем тексту: ИЗИС РС) или у Пословном информационом систему Фонда здравственог осигурања Републике Српске (у даљем тексту: ПИС ФЗОРС),

- да нећу оштетити, измијенити, избрисати, уништити или учинити неупотребљивим аутоматски обрађене податке или софтверске апликације који се налазе у ИЗИС РС или у ПИС ФЗОРС,

- да нећу неовлашћено приступати претраживању рачунарских база података или неовлашћено приступити аутоматски обрађеним подацима или рачунарским програмима који се налазе у ИЗИС РС или у ПИС ФЗОРС,

- да нећу неовлашћено употријебити податке које могу добити из базе података или софтверских апликација који се налазе у ИЗИС или у ПИС ФЗОРС,

- да ћу у свом раду поштовати и спроводити одредбе Правилника о јединственим методолошким принципима и стандардима за функционисање Интегрисаног здравственог информационог система и

- да ћу у свом раду поштовати и спроводити одредбе Правилника о мјерама информационе безбједности у Фонду здравственог осигурања Републике Српске.

У_____ Потпис:

Датум:_____ _____

ОБРАЗАЦ ИЗЈАВЕ О ПОВЈЕРЉИВОСТИ ЗА КОРИСНИКА АПЛИКАЦИЈА

_____
(име и презиме запосленог)

_____
(организациона јединица)

_____
(радно мјесто)

ИЗЈАВА

О ЧУВАЊУ ПОСЛОВНЕ ТАЈНЕ, ПРИСТУПУ РАЧУНАРСКИМ СИСТЕМИМА, ПРАВИМА ИНТЕЛЕКТУАЛНОГ ВЛАСНИШТВА, ОБАВЕЗИ ПОВРАТА ИНФОРМАЦИЈА И ПРАВУ НАДЗОРА

Ја, _____, под материјалном и кривичном одговорношћу, изјављујем:

- да ћу чувати тајност личних података и придржавати се утврђеног начина обезбјеђивања личних података, у складу са обавезом одређеном прописима којима се уређује област заштите личних података,

- да ћу чувати као професионалну тајну све што сазнам о свим подацима који се налазе у Интегрисаном здравственом информационом систему Републике Српске (у даљем тексту: ИЗИС РС) или у Пословном информационом систему Фонда здравственог осигурања Републике Српске (у даљем тексту: ПИС ФЗОРС),

- да нећу неовлашћено употријебити податке које могу добити из базе података или софтверских апликација који се налазе у ИЗИС или у ПИС ФЗОРС,

- да ћу у свом раду поштовати и спроводити одредбе Правилника о јединственим методолошким принципима и стандардима за функционисање Интегрисаног здравственог информационог система и

- да ћу у свом раду поштовати и спроводити одредбе Правилника о мјерама информационе безбједности у Фонду здравственог осигурања Републике Српске.

У_____ Потпис:

Датум:_____ _____

ПРИЛОГ 2

БЕЗБЈЕДНОСНО-ТЕХНИЧКИ ОБРАЗАЦ
(БТ ОБРАЗАЦ)

Датум:

Име и презиме корисника:

ЈМБ корисника:

Организациона јединица:

☐ Пријава корисника ☐ Одјава корисника ☐ Промјена права

АПЛИКАЦИЈА	ПРАВА
☐ Апликација 1	☐ Рола 1 ☐ Рола 2 ☐ Рола 3
☐ Апликација 2	☐ Рола 1 ☐ Рола 2 ☐ Рола 3
☐ Апликација 3	☐ Рола 1 ☐ Рола 2 ☐ Рола 3

М. П. Потпис овлашћеног лица

_____

ПРИЛОГ 3

ОБРАЗАЦ ИЗЈАВЕ О ПРЕУЗИМАЊУ ИДЕНТИФИКАЦИОНЕ
ЕЛЕКТРОНСКЕ КАРТИЦЕ ЗДРАВСТВЕНОГ РАДНИКА

_____
(име и презиме запосленог)

_____
(радно мјесто)

Ја, _____, запослен/-а у _____

преузимам идентификациону електронску картицу здравственог радника, а прије активирања електронске картице, под пуном материјалном и кривичном одговорношћу, дајем сљедећу

ИЗЈАВУ

О ПРЕУЗИМАЊУ ИДЕНТИФИКАЦИОНЕ
ЕЛЕКТРОНСКЕ КАРТИЦЕ ЗДРАВСТВЕНОГ РАДНИКА

1. Идентификациону електронску картицу здравственог радника користићу искључиво у складу са одредбама Правилника о јединственим методолошким принципима и стандардима за функционисање Интегрисаног здравственог информационог система;

2. У вези са заштитом података који су ми коришћењем картице доступни, директно ћу се придржавати прописа којима се уређује област заштите личних података са чијим одредбама сам упознат/-а, укључујући и казнене одредбе;

3. Упознат/-а сам са одредбама Закона о обавезном здравственом осигурању, те са одредбама свих прописа на основу којих вршим приступ подацима или обраду података;

4. Упознат/-а сам са обавезом правилне употребе која обухвата чување картице од оштећења, обавезу да без одлагања администратору пријавим оштећење, нестанак или губитак електронске картице, обавезу да оштећену електронску картицу без одлагања предам здравственој установи, као и обавезу да електронску картицу вратим здравственој установи у случају престанка радног односа.

У _____ Потпис:

Датум: _____ _____

На основу члана 26. став 5. и члана 101. тачка 3) Закона о обавезном здравственом осигурању ("Службени гласник Републике Српске", бр. 93/22 и 132/22), уз Сагласност министра здравља и социјалне заштите, број: 11/06-505-63-3/23, од 19. јуна 2023. године, Управни одбор Фонда здравственог осигурања Републике Српске, на 11. редовној сједници, одржаној 13. јула 2023. године, д о н о с и

ПРАВИЛНИК

О ИЗМЈЕНАМА ПРАВИЛНИКА О ПОСТУПКУ УТВРЂИВАЊА СВОЈСТВА ОСИГУРАНОГ ЛИЦА, ВОЂЕЊУ ПОДАТАКА У МАТИЧНОЈ ЕВИДЕНЦИЈИ И ИЗГЛЕДУ, САДРЖАЈУ И ПОСТУПКУ ИЗДАВАЊА И УПОТРЕБЕ ЕЛЕКТРОНСКЕ ЗДРАВСТВЕНЕ КАРТИЦЕ

Члан 1.

У Правилнику о поступку утврђивања својства осигураног лица, вођењу података у матичној евиденцији и изгледу, садржају и поступку издавања и употребе електронске здравствене картице ("Службени гласник Републике Српске", број 48/23) у члану 8. у ставу 2. Прилог 1 замјењује се новим Прилогом 1, који чини саставни дио овог правилника.

Члан 2.

У члану 25. став 4. мијења се и гласи:

"(4) Здравствена картица на предњој страни садржи сљедеће податке:

1) име и презиме осигураника / осигураног лица,

2) идентификациони број осигураника / осигураног лица у систему обавезног здравственог осигурања,

3) датум рођења осигураника / осигураног лица,

4) идентификациони број картице".

Члан 3.

У члану 27. у ставу 1. Прилог 2 замјењује се новим Прилогом 2, који чини саставни дио овог правилника.

У ставу 3. Прилог 3 замјењује се новим Прилогом 3, који чини саставни дио овог правилника.

Став 6. мијења се и гласи:

"(6) Фонд води електронски регистар о издатим картицама, који омогућава праћење картице по статусима и садржи податке: о организационој јединици која је издала картицу; о идентификационом броју картице; о кориснику картице и о поништавању картице".

Члан 4.

У члану 29. у ставу 1. Прилог 4 замјењује се новим Прилогом 4, који чини саставни дио овог правилника.

Члан 5.

Овај правилник ступа на снагу осмог дана од дана објављивања у "Службеном гласнику Републике Српске".

Број: 02/002-3054-8/23
13. јула 2023. године
Бања Лука

В.д. замјеника предсједника
Управног одбора,
Драгослав Топић, с.р.

ПРИЛОГ 1

ФОНД ЗДРАВСТВЕНОГ ОСИГУРАЊА РЕПУБЛИКЕ СРПСКЕ	ОБРАЗАЦ ПР-1
ПОСЛОВНИЦА/ЕКСПОЗИТУРА	
ВРСТА ОБРАСЦА: □ ПРИЈАВА □ ОДЈАВА □ ПРОМЈЕНА ПРИЈАВЕ	ЗА ОСИГУРАНО ЛИЦЕ – ЧЛАНА: □ УЖЕ ПОРОДИЦЕ □ ШИРЕ ПОРОДИЦЕ □ ПОРОДИЧНОГ ДОМАЋИНСТВА

ПОДАЦИ О ОСИГУРАНИКУ (НОСИОЦУ ОСИГУРАЊА)

Презиме и име	Општина пребивалишта □□□
ЈМВ (или ЈИБ за странце) □□□□□□□□□□□□□	Општина пријаве на осигурање □□□

ПОДАЦИ О ОСИГУРАНОМ ЛИЦУ

1.	Презиме и име	Сродство са осигураником
	ЈМБ □□□□□□□□□□□□□	Пол М Ж
	Адреса пребивалишта/боравка	
2.	Презиме и име	Сродство са осигураником
	ЈМБ □□□□□□□□□□□□□	Пол М Ж
	Адреса пребивалишта/боравка	
3.	Презиме и име	Сродство са осигураником
	ЈМБ □□□□□□□□□□□□□	Пол М Ж
	Адреса пребивалишта/боравка	