РЕПУБЛИКА СРБИЈА
ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ

МИНИСТАРСТВО ЗДРАВЉА РЕПУБЛИКЕ СРБИЈЕ

по ревизији сврсисходности пословања „Информациона безбедност у здравственим информационим системима“

Број: 400-734/2020-03/34
Београд, 2. јул 2021. године

Садржај

I УВОД

Државна ревизорска институција издала је Извештај о ревизији сврсисходности пословања „Информациона безбедност у здравственим информационим системима“ број: 400-734/2020-03/20 од 10. фебруара 2021. године.

С обзиром да све откривене несврсисходности нису биле отклоњене у току ревизије, Институција је од субјекта ревизије, Министарства здравља Републике Србије, захтевала достављање одазивног извештаја.

Субјект ревизије у остављеном року од 90 дана није доставио одазивни извештај. Узимајући у обзир ванредне околности због пандемије вируса COVID-19 и примене мера[1] заштите јавног здравља, ограниченог кретања, броја људи у просторијама, као и друга ограничења, достављен је потписан и оверен извештај од стране одговорног лица 18.јуна 2021. године.

У одазивном извештају су приказане мере исправљања утврђених несврсисходности. У послеревизионом поступку смо прегледали одазивни извештај и оценили његову веродостојност и оценили да ли су мере исправљања задовољавајуће.

У овом извештају:

- приказујемо несврсисходности које су обелодањене у извештају о ревизији за које је захтевано предузимање мера исправљања,
- резимирамо предузете мере исправљања и
- дајемо мишљење о томе да ли су мере за исправљање стања, исказане у одазивном извештају, задовољавајуће.

[1] Уредба о мерама за спречавање и сузбијање заразне болести COVID-19 „Службени гласник РС“, бр. 151/2020-3, 152/2020-4, 153/2020-46, 156/2020-6, 158/2020-3, 1/2021-3, 17/2021-3, 19/2021-18, 22/2021-3, 29/2021-3, 34/2021-3, 48/2021-4.

II НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

1. Не постоји стратешко планирање развоја и одржавања Интегрисаног здравственог информационог система

Опис несврсисходности

Законом о здравственој заштити прописано је да Стратегију развоја и организације интегрисаног здравственог информационог система, доноси Влада.

Влада Републике Србије није донела Стратегију развоја и организације Интегрисаног здравственог информационог система, што је довело до неправовременог и несвеобухватног развоја и одржавања здравствених информационих система.

Исказане мере исправљања (препорука 1)

Одговорним лицима Министарства здравља Републике Србије препоручено је да предузму активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену, које ће између осталог обухватити и прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства, и иницира усвајање Стратегије и Акционог плана за њену примену, као и

У одазивном извештају Министарства здравља Републике Србије наводи се да је формирано координационо тело за дигитализацију у здравственом систему Републике Србије ("Сл. гласник РС", бр. 3/2021). Координационо тело разматра питања, даје предлоге и усмерава рад државних органа у домену дигитализације здравственог система у Републици Србији, са циљем постизања квалитетније и ефикасније здравствене заштите у државном и приватном сектору здравства, као и стварања повољних услова за иновације, истраживање и развој у државном н приватном сектору.

Задаци координационог тела се између осталог управо односе на израду програма дигитализације здравства са Акционим планом, као и подршка стварању регулаторних услова за системски развој и унапређење здравственог система.

Координационо тело је дужно да достави извештај Влади сваких шест месеци, а по потреби чешће.

Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу.** Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања. Отклањање утврђене несврсисходности је у току.

2. Није обезбеђено стабилно финансирање здравствених информационих система

Опис несврсисходности

Министарство здравља због непостојања стратешког планирања није успоставило стабилно финансирање ИЗИС-а, што за последицу има отежан процес развоја и одржавања здравствених информационих система, застареле рачунаре и сервере,

застареле па самим тим и небезбедне оперативне системе, непостојање обука за запослене и недовољан број ИТ стручњака

Имајући у виду да је дигитализација један од приоритета Владе Републике Србије, као и област здравства, усвајањем Стратегије којој ће претходити одговарајуће анализе, створили би се услови да се сва ова питања и проблеми везани за финансирање системски уреде. Неопходно је да будући финансијски планови прате остварење циљева из Акционог плана за примену Стратегије.

Исказане мере исправљања (препорука 2)

Одговорним лицима Министарства здравља Републике Србије препоручено је да приликом припреме финансијских планова осигурају стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства

У одазивном извештају Министарства здравља Републике Србије наводи се да је Министарство здравља огласило набавку хардвера и софтвера за здравствене установе (56 установа) и ИЈЗС „Др Милан Јовановић Батут“ (SPN Reference No. RS-SSHP-8338YF-G-RFB-20-1.1.19) објављен је 28. јануара 2021. у дневном листу „Политика“, на web сајту Министарства здравља https://www.zdravlje.gov.rs/tekst/353728/spn-reference-no-rs-sshp-8338yf-g-rfb-20-1119-.php и на web сајту UNDB online.

Набавка је у току. Уговор ће бити реализован до краја 2021.

Како се још наводи у одазивном извештају, након усвајања стратегије, финансијски захтеви ће бити прилагођени Акционом плану за спровођење Стратегије.

Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу.** Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања. Отклањање утврђене несврсисходности је у току.

3. Нису усвојене и примењене све мере информационе безбедности, које укључују ИТ управљање, управљање ИТ ризицима, континуитет пословања у ванредним околностима и организацију и управљање ИТ безбедношћу

Опис несврсисходности

Министарство здравља није усвојило процедуре за управљање ИТ пословима, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима

Министарство здравља није успоставило управљање ИТ ризицима, иако је ово и законска обавеза, пре свега због непознавања ове проблематике, недовољно искуства и обученог ИТ кадра, а што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити, или великих нефинансијских губитака (података на пример) због неблаговременог предузимања мера. Поуздан, али истовремено и ефикасан систем се не може постићи без успостављеног процеса управљања ризицима. На пример, могуће је све елементе система дуплирати, и тако постићи скоро 100% поуздан систем. Али због цене

дуплирања, такав систем се не може сматрати ефикасним, јер се можда исти циљ (поузданост) може постићи и са мање улагања. Министарство здравља није успоставило управљање ИТ ризицима.

Термин „континуитет пословања у ванредним околностима“ у ширем смислу подразумева више подобласти: континуитет пословања, чување резервних копија и опоравак система у случају ванредних околности (у терминологији другачије речено – опоравак од катастрофе (disaster recovery - DR), као и процес тестирања планова за континуитет пословања и опоравак од катастрофе. Законом о информационој безбедности уређени су критеријуми мере заштите од безбедносних ризика у информационо-комуникационим системима (ИКТ). Мерама заштите ИКТ система се између осталог обезбеђује континуитет обављања посла у ванредним околностима. Министарство здравља није успоставило управљање континуитетом пословања у ванредним околностима.

Министарство здравља није усвојило ни имплементирало правила и процедуре за континуитет пословања иако је то и законска обавеза, што може за последицу имати нефункционисање система у неодређено дугом временском периоду, па самим тим и отежано пружање услуга здравственим осигураницима.

Због недостатка потребне опреме, неадекватне ИТ организационе структуре и непостојања планова и процедура, Министарство здравља нису успоставило континуитет пословања у ванредним околностима – тј. опоравак од катастрофе, иако им је то била законска обавеза, што за последицу може имати нефункционисање информационог система у дужем временском периоду.

Тестирање планова за континуитет пословања и опоравак од катастрофе Министарство здравља не врши зато што немају довољно ресурса за то - пре свега запослених са довољно знања и искуства, иако је верификација тих планова обавеза свих оператора ИКТ система од посебног значаја, а што за последицу може имати нефункционални систем у току и након ванредне ситуације у дужем временском периоду.

Закон о информационој безбедности (цео закон) и пратеће уредбе, као и Закон о здравственој документацији и евиденцијама у области здравства (посебно чланови 44-51) прописују мере које се односе на информациону безбедност а које се односе на организацију ИТ безбедности, питања приступа систему и управљања подацима. Наведене мере Министарство здравља није применило.

Организација ИТ безбедности у интегрисаном здравственом информационом систему није успостављена на адекватан начин, иако је то законска обавеза Министарства здравља, што за последицу има већи степен рањивости овог система па самим тим и осетљивих података здравствених осигураника. Нису организоване/спроведене обуке запослених на овим пословима, нису усвојиле политике и процедуре које се односе на информациону безбедност, није успостављена одговарајућа организациона ИТ структура, није одређено одговорно лице за обавештавање о инцидентима.

Није успостављен процес одобравања и укидања приступа продукционом систему на задовољавајући начин, због тога што нису усвојене процедуре које уређују овај процес и није успостављена контрола тог процеса, иако је то законска обавеза, што за последицу може имати угрожену безбедност података здравствених осигураника.

Начин пријаве осигураника у систем није успостављен на једнообразан и максимално безбедан начин у свим здравственим установама, па постоји могућност да се од стране корисника система оствари увид у личне податке осигураника и у случајевима када он није присутан, идентификован на други начин или када то уопште није потребно. Не

постоје успостављене и примењене процедуре које уређују безбедност свих излазних података, што за последицу може имати нарушавање поверљивости података.

Исказане мере исправљања (препорука 3)

Одговорним лицима Министарства здравља Републике Србије препоручено је да предузму активности у смислу припреме и доношења подзаконског акта којим ће ближе уредити услове за функционисање, управљање ризиком и безбедношћу интегрисаног здравственог информационог система, укључујући континуитет пословања у ванредним околностима, начин пријаве осигураника и заштиту излазних података, уз прибављање мишљења Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства.

У одазивном извештају Министарства здравља Републике Србије наводи се да је формирано координационо тело за дигитализацију у здравственом систему Републике Србије ("Сл. гласник РС", бр. 3/2021). Координационо тело разматра питања, даје предлоге и усмерава рад државних органа у домену дигитализације здравственог система у Републици Србији, са циљем постизања квалитетније и ефикасније здравствене заштите у државном и приватном сектору здравства, као и стварања повољних услова за иновације, истраживање и развој у државном н приватном сектору.

Задаци координационог тела се између осталог управо односе на стварање регулаторних услова за системски развој и унапређење здравственог система путем дигитализације процеса рада и управљања, за примену технолошких решења у процесу пружања здравствене заштите, као и за иновације, истраживање и развој у државном и приватном сектору, затим на предлагање и координација приоритизације пројеката из домена дигитализације здравства, као и на координацију и праћење спровођења приоритетних мера.

Једна од подгрупа координационог тела је задужена за анализу правног оквира за дигитализацију у здравству.

Координационо тело је дужно да достави извештај Влади сваких шест месеци, а по потреби чешће.

Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања. Отклањање утврђене несврсисходности је у току.

4. Није успостављен механизам заштите података када су у питању пружаоци услуга

Опис несврсисходности

Министарство здравља није успоставило механизам контроле заштите података здравствених осигураника од стране пружаоца услуга апликативног софтвера „Мој доктор“. Закон о информационој безбедности, у члану 7. уређује мере заштите ИКТ система од посебног значаја и то на следећи начин: “Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система. Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга

другим лицима. Мере заштите ИКТ система се, између осталог, односе на: заштиту средстава оператора ИКТ система која су доступна пружаоцима услуга (став 3, тачка 25) и одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (став 3, тачка 26)“. Такође, ова питања уређују и Закон о заштити права пацијената и Закон о заштити података о личности. Није уређен однос са пружаоцима услуга када је у питању заштита података у здравственим информационим системима, нити је и поред тога што у већини уговора са пружаоцима услуга постоји део који се односи на поверљивост података, успостављен механизам за контролу да ли пружалац услуга ту обавезу поштује, што за последицу може имати одавање осетљивих података здравствених осигураника.

Исказане мере исправљања (препорука 4)

Одговорним лицима Министарства здравља Републике Србије препоручено је предузму активности у смислу припреме и одређивања ближе садржине података, укључујући и податке о личности, који се воде у електронском медицинском досијеу, начин и поступак преузимања података, као и друга питања од значаја за успостављање и коришћење података, уз прибављено мишљење Института за јавно здравље Србије „Др Милан Јовановић Батут“ и других организација и установа у области здравства

У одазивном извештају Министарства здравља Републике Србије наводи се да је формирано координационо тело за дигитализацију у здравственом систему Републике Србије ("Сл. гласник РС", бр. 3/2021). Координационо тело разматра питања, даје предлоге и усмерава рад државних органа у домену дигитализације здравственог система у Републици Србији, са циљем постизања квалитетније и ефикасније здравствене заштите у државном и приватном сектору здравства, као и стварања повољних услова за иновације, истраживање и развој у државном н приватном сектору.

Министарство здравља је у одазивном извештају навело да је започет рад на изради измене Закона о здравственој документацији и изради подзаконског акта.

Координационо тело је дужно да достави извештај Влади сваких шест месеци, а по потреби чешће.

Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања. Отклањање утврђене несврсисходности је у току.

III МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА

Прегледали смо одазивни извештај, који је поднео субјект ревизије. Оценили смо да је одазивни извештај, који је потписало и печатом оверило одговорно лице субјекта ревизије, веродостојан.

Вредновање мера исправљања смо оценили на основу њиховог описа и достављене документације. Сматрамо да смо добили довољне и одговарајуће доказе да можемо изрећи мишљење да ли су мере исправљања задовољавајуће.

Оцењујемо, да су мере исправљања, описане у одазивном извештају који је поднео субјект ревизије **задовољавајуће**.

Напомена:

У складу са одредбама члана 37. Закона о Државној ревизорској институцији, а након истека рокова исказаним у одазивном извештају, потребно је да обавештавате Државну ревизорску институцију о предузетим мерама и активностима о отклањању откривених несврсисходности према роковима из одазивног извештаја и доставите одговарајуће доказе.

По истеку три године Државна ревизорска институција ће утврђивати ефекте остварене након спровођења препорука и отклањања откривених несврсисходности.

У ове ефекте укључиће се и ефекти које будете ви исказали предузетим мерама и активностима из одазивног извештаја.

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
02. јул 2021. године