РЕПУБЛИКА СРБИЈА
ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ

ИНСТИТУТ ЗА ЈАВНО ЗДРАВЉЕ СРБИЈЕ „ДР МИЛАН ЈОВАНОВИЋ БАТУТ“

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

Број: 400-734/2020-03/38
Београд, 02. 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, Института за јавно здравље Србије „Батут“, 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 20.маја 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. Није успостављено управљање ИТ ризицима у информационим системима ИЗИС-а

Опис несврсисходности

Управљање ИТ ризицима Институт за јавно здравље „Батут“, руковалац подацима у **ИЗИС-у,** није успоставио иако је ово и законска обавеза, пре свега због непознавања ове проблематике, недовољно обученог ИТ кадра без искуства у овој области, а што за последицу може имати стварање непотребно великих трошкова у случају настанка нежељеног догађаја, а који се могао спречити или велике нефинансијске губитке (на пример података) због неблаговременог предузимања мера.

Исказане мере исправљања (препорука 6)

Одговорним лицима Института за јавно здравље Србије „Батут“ препоручено је да успостави одговарајуће техничке, организационе и кадровске мере за обраду података у ИЗИС-у, и да успостави механизам за праћење примене тих мера

У одазивном извештају Института за јавно здравље Србије „Батут“ наводи се да је у сарадњи са Владом Републике Србије и Министартвом здравља формирано координационо тело за дигитализлацију у здравственом систему Републике Србије ("Сл. гласник РС", бр. 3/2021). Координационо тело као и да су формиране одговарајуће радне групе (1. за регулативу, 2. за програм и акциони план, 3. за електронски здравствени досије), и да је започет рад на изради предлога стратешких докумената и законских и подзаконских аката. како је такође наведено, израда ових докумената и аката за циљ има боље и јасније уређење услова и стандарда (техничких, организационних, кадровских) за функционисање ИЗИС-а и безбедност информационих система и заштиту података, успостављање евалуационих и контролних механизама и тела (сертификација ИС) за праћење процееса обраде података на свим нивоима (ИС у здравственим установама и централне базе на републичком нивоу).

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 успостављен механизам заштите података када су у питању пружаоци услуга

Опис несврсисходности

Институт за јавно здравље Србије „Др Милан Јовановић Батут“, као руковалац подацима у ИЗИС-у, и поред тога што у уговорима здравствених установа са пружаоцима услуга (а сви ти системи су део ИЗИС-а) постоји део који се односи на поверљивост података, није успоставио механизам за контролу да ли пружалац услуга ту обавезу поштује, због недостатака кадровских капацитета, недоумица у вези

законске регулативе и недовољно стручног знања, што за последицу може имати одавање осетљивих података здравствених осигураника. 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 7)

Одговорним лицима Института за јавно здравље „Батут" Србије препоручено је да уреде процес обраде података од стране пружаоца услуга у здравственим информационим системима на законом прописан начин, што подразумева обавезну примену мера заштите података, и може укључити процес сертификације и издавања посебног или општег писменог овлашћења другим обрађивачима

У одазивном извештају Института за јавно здравље Србије „Батут" наводи се да је у сарадњи са Министарством здравља и Владом Републике Србије започет рад на изради измене закона о здравственој документацији и евиденцијама у области здравства и изради подзаконских аката којима би се јасније уредили услови за функционисање, управљање ризиком и безбедношћу ИЗИС-а, јединствени методолошки принципи и стандарди, и други услови од значаја за функционисање.

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