ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

РЕЗИМЕ ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
„Информациона безбедност у здравственим информационим системима”

18. фебруар 2021. године

Државна ревизорска институција је спровела ревизију сврсисходности „Информациона безбедност у здравственим информационим системима“.

Интегрисани здравствени информациони систем у даљем тексту ИЗИС је сложени информациони систем који чине **здравствено-статистички систем,** информациони системи организација здравственог осигурања и **здравствени информациони системи здравствених установа,** приватне праксе и других правних лица.

У претходним годинама, у процесу вршења ревизије установљено је да **код здравствених установа постоје проблеми везани за информациону безбедност** у више области. Ови проблеми се односе на приступ базама података (поред запослених у здравственим установама, приступ је омогућен и пружаоцима услуга), управљање резервним копијама података, приступ подацима осигураника (поред употребе електронских здравствених књижица, приступ основним подацима је био омогућен и уношењем само једног идентификационог податка (ЈМБГ), континуитет пословања у случају нежељених догађаја, неадекватну организациону ИТ структуру, итд

Циљ ревизије је да се оцени у којој мери су примењене мере у здравственим информационим системима у Републици Србији испуниле неопходне циљеве када је у питању информациона безбедност.

Како су оснивачи здравствених установа **Министарство здравља Републике Србије** и **Покрајински секретаријат за здравство** у даљем тексту Покрајински секретаријат, и у њиховој је надлежности инвестиционо улагање када су у питању информациони системи, и како је **Институт за јавно здравље Србије „Батут“** у даљем тексту Институт „Батут“ руковалац подацима у Интегрисаном здравственом информационом систему, ревизијом су као **субјекти одабрани како би се препоруке могле свеобухватно и системски имплементирати**. Узорковањем је одређен и један број здравствених установа које су нам у току ревизији биле извори информација.

Након спроведене ревизије утврдили смо:

Потребно је да Министарство здравља, Институт „Батут” и Покрајински секретаријат за здравство унапреде мере информационе безбедности што ће допринети већој поузданости здравствених информационих система у Републици Србији.

Наведено заснивамо на закључцима и налазима који су изложени у наставку текста:

1. Постојећи системи ИТ управљања у здравству нису у потпуности омогућили испуњење пословних циљева, тачније пуну имплементацију Интегрисаног

здравственог информационог система, процену ИТ ризика и успостављање адекватне организационе ИТ структуре

Не постоји стратешко планирање ни на републичком нивоу, јер Влада Републике Србије иако јој је то била и законска обавеза није усвојила Стратегију развоја и организације Интегрисаног здравственог информационог система, ни на нивоу сваке здравствене установе, које је неопходно имајући у виду константну потребу одржавања и модернизације информационих система (што подразумева хардвер, софтвер, организацију, едукацију, правила и процедуре итд).

Због непостојања стратешког планирања, Министарство здравља, Покрајински секретаријат и здравствене установе **нису обезбедиле стабилно финансирање здравствених информационих система** самим тим ни развој и одржавање тих система, што може за последицу имати застарелу опрему и недовољан број серверских рачунара, застареле па самим тим и небезбедне оперативне системе, непотребно увећане трошкове за набавку апликативног софтвера, отежану израду финансијских планова када је у питању ИТ и на републичком нивоу и на нивоу сваке установе, недовољан број запослених на ИТ пословима и непостојање неопходних обука.

Организациона ИТ структура није успостављена на начин да је омогућена подела дужности и одговорности, као и испуњење законских обавеза. **нити су усвојена правила и процедуре у вези управљања ИТ операцијама**, што онемогућава или отежава контролу ових послова од стране руководства или континуитет обављања послова у случају замене запослених на ИТ пословима. У здравственим установама у којима су усвојене неке од неопходних процедура у овој области, оне нису довољно детаљне и свеобухватне.

Управљање ИТ ризицима, Министарство здравља и Институт „Батут“, као и здравствене установе које смо обухватили анкетом **нису успоставили** 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. *(Препоруке број 3 и 6)*

ИТ управљање је област која обухвата стратешко планирање, стабилно финансирање које прати акциони план за спровођење стратегије, одговарајућу ИТ организациону структуру, усвојене и примењене процедуре за ИТ послове, и управљање ИТ ризицима. Као што се из напред наведених налаза може закључити, потребно је унапређење у овој области на свим нивоима.

2. Ефективно управљање континуитетом пословања у случају ванредних околности у Интегрисаном здравственом информационом систему није у потпуности успостављено, што за последицу може имати нефункционисање делова система у дужем временском периоду

Институт „Батут“ и Министарство здравља, као и већина анкетираних здравствених установа **нису усвојили ни имплементирали 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. *(Препорука број 3)*

Због недостатка потребне опреме, неадекватне ИТ организационе структуре и непостојања планова и процедура, Институт „Батут“, Министарство здравља и анкетиране здравствене установе **нису успоставиле 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. *(Препорука број 3)*

Управљањем резервним копијама података из здравствених информационих система **се не документује**, зато што здравствене установе нису усвојиле одговарајуће процедуре, што су биле обавезне по закону, што отежава или онемогућава контролу овог процеса. *(Препорука број 3)*

Тестирање планова за континуитет пословања и опоравак од катастрофе Министарство здравља и Институт „Батут“, као и здравствене установе које смо обухватили анкетом и које имају усвојене ове планове, **не врше** 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. *(Препорука број 3)*

План континуитета пословања је шири оквир који дефинише кораке које треба предузети у случају нежељеног догађаја. Иако је чест случај да се посебно усвоји и план опоравка од катастрофе, он може бити и део плана континуитета. У склопу оба плана, управљање резервним копијама је обавезни и главни део тих планова, као и тестирање планова, и у склопу тога враћања података из резервних копија. Већина здравствених установа, као и сбјекти немају усвојене ове планове, а и код здравствених установа које су их усвојиле, они су непотпуни, недовољно детаљни и практично неприменљиви.

3. Здравствене установе нису усвојиле и примениле свеобухватне мере заштите информационих система, а Министарство здравља и Институт „Батут“ нису успоставили управљање информационом безбедношћу Интегрисаног здравственог информационог система и контролу примене мера заштите као приоритет, што је неопходно како би била осигурана поверљивост, доступност и поузданост података о личном здрављу грађана.

Организација ИТ безбедности у интегрисаном здравственом информационом систему **није успостављена на адекватан начин**, иако је то законска обавеза Министарства здравља, Института „Батут“ и здравствених установа, 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 све здравствене установе усвојиле акт о информационој безбедности, нису ни Министарство здравља ни Института „Батут“ ни здравствене установе усвојиле политике и процедуре које се односе на информациону безбедност, није успостављена одговарајућа организациона ИТ структура, нису ни субјекти ревизије ни све здравствене установе одредиле одговорно лице за обавештавање о инцидентима.

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.

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.

Успостављање мера које се односе на информациону безбедност, а обавезно на организацију ИТ безбедности, усвајање и примену процедуре и политике у овој области, јасно уређен процес уговарања услуга када је у питању заштита података, успостављање механизама контроле свих ових послова треба бити приоритет у наредном периоду када је у питању Интегрисани здравствени информациони систем.

Државна ревизорска институција, након спроведене ревизије „Информациона безбедност у здравственим информационим системима“, даје између осталих и следеће **препоруке:**

Министарству здравља: да предузме активности у смислу припреме предлога Стратегије развоја и организације интегрисаног здравственог информационог система и Акционог плана за примену, и иницира њихово усвајање, као и да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије, да предузме активности са циљем ближег уређења услове за функционисање, управљање ризиком и безбедношћу ИЗИС, да предузме активности у смислу уређења свих питања од значаја за успостављање и коришћење података који се воде у електронском медицинском досијеу.

Покрајинском секретаријату за здравство: да приликом припреме финансијских планова осигура стабилно финансирање циљева из Акционог плана за примену Стратегије кроз детаљно планирање средстава за развој, набавку и одржавање информационих система у области здравства.

Институту за јавно здравље Србије „Др Милан Јовановић Батут“: да успостави одговарајуће техничке, организационе и кадровске мере за обраду података у ИЗИС-у, и да успостави механизам за праћење примене тих мера, и да уреди 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.