ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

РЕЗИМЕ
ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
„Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у Републичком фонду за здравствено осигурање”

8. фебруар 2024. године

У току 2023. године, ДРИ је у спровела ревизију сврсисходности пословања на тему „Ефективност информационог система Матична евиденција и остваривање права (МЕОП) у РФЗО”.

Због чега је ДРИ спровела ову ревизију?

Обавезно здравствено осигурање обезбеђује се и спроводи у РФЗО и веома је значајно за све грађане. За спровођење обавезног здравственог осигурања најзначајнију улогу има информациони систем Матична евиденција и остваривање права (МЕОП). МЕОП чине подаци о: осигураницима, члановима породице осигураника, обвезницима плаћања доприноса и коришћењу права из обавезног здравственог осигурања.

У претходним годинама, уочени су проблеми у функционисању информационих система РФЗО у више области:

1) стратегијски приступ

Без усвојене стратегије развоја информационих технологија, која треба бити саставни део стратешког планирања за период од три до пет година, информационе технологије не могу у одговарајућој мери допринети остваривању и развоју пословних циљева организације, ни у системском (хардвер и софтвер) ни у кадровском (структура и знање) смислу.

2) поузданост информационих система

Проблеми који су се односили на информациону безбедност, обухватају питања:

- физичког и логичког приступа систему од стране запослених у РФЗО;
- приступа системима и базама података од стране пружаоца услуга одржавања ИС МЕОП;
- управљања лог фајловима и инцидентима (базе података садрже осетљиве податке о личности о сваком осигуранику).

3) начин пријаве осигураника и приступ картону осигураника

Здравствена исправа представља документ којим осигурано лице остварује своја права на здравствено осигурање. Процес замене папирне исправе здравственом картицом започео је 2015. године. Иако је преузето око 7 милиона електронских здравствених картица, подацима осигураника се може приступити и без њих, често и само на основу ЈМБГ, што у пракси значи чак и без присуства или чак и знања осигураника.

Такође, у ревизији сврсисходности пословања „Информациона безбедност у здравственим информационим системима“ , утврђено је да се картону осигураника може приступити без електронске здравствене књижице, већ само употребом ЈМБГ осигураника.

4) синхронизација података са здравственим установама

ЗУ користе различите здравствене информационе системе, као што су „Heliant Health“, „NexTZU“, „ZipSoft“ и друге. То има за последицу да се подаци уносе и обрађују у појединачним информационим системима ЗУ и потом преносе у матичну евиденцију.
Базе података у информационим системима ЗУ садрже поред личних података осигураника, податке о болестима, терапијама, евиденцији лечења осигураника, издатим лековима и друго, што представља осетљиве личне податке и изискује примену одређених мера заштите.

Кључном поруком, након спроведене ревизије утврдили смо да **је неопходно да Републички фонд за здравствено осигурање унапреди ИТ управљање, обезбеди виши ниво информационе безбедности и обезбеди континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.**

У наставку су дати закључци и одређени налази до којих смо дошли у поступку ревизије:

Закључак 1: РФЗО није у потпуности успоставио ефективно ИТ управљање због недостатка кадровских капацитета, непрепознавања могућих ИТ ризика и проблема са управљањем подацима из матичне евиденције осигураника.

- РФЗО није донео ИТ стратегију за период 2022-2024. године.
- ИТ управљање није успостављено на адекватан начин због непрепознавања свих ИТ ризика и недовољних кадровских капацитета.
- РФЗО није успоставио правила управљања подацима из матичне евиденције осигураника, којима би онемогућио приступ личним подацима осигураника и без њиховог физичког присуства.

Закључак 2: РФЗО није у потпуности успоставио управљање информационом безбедношћу ИС МЕОП јер није попунио радна места у Сектору за информациону безбедност и заштиту података и не прати и не контролише додељена права приступа ИС МЕОП, што може довести до неовлашћеног приступа подацима осигураника и остварeним правима у здравственој заштити.

- РФЗО није у потпуности успоставио логички приступ ИС МЕОП који обезбеђује поузданост информационог система (контролу права приступа).
- РФЗО није попунио радна места у Сектору за информациону безбедност и заштиту података.
- РФЗО није у потпуности успоставио процес праћења и контроле приступа ИС МЕОП од стране ЗУ и запослених у РФЗО.

Закључак 3: РФЗО није у потпуности успоставио ефективан механизам сарадње, односно није у потпуности уредио правилима и процедурама однос са пружаоцем услуге одржавања ИС МЕОП и мере којима обезбеђује континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

- РФЗО није успоставио (уредио) однос са пружаоцем услуга одржавања ИС МЕОП у делу дефинисања нивоа доступности и врсте информација, средстава којима могу приступити пружаоци услуга, начина приступа информацијама и средствима и надзора над приступом.
- РФЗО је обезбедио заштиту осетљивих података о осигураницима тако да врши псеудонимизацију података базе МЕОП.
- РФЗО није предвидео мере које обезбеђују континуитет пословања у случају прекида сарадње са пружаоцем услуге одржавања ИС МЕОП.

За све утврђене несврсисходности Републичком фонду за здравствено осигурање (субјекту ревизије) су дате одговарајуће препоруке, како би се отклонили узроци проблема.