Crna Gora
Državna revizorska institucija

DRI broj: 40113/17-031-610/36
Podgorica, 19.10.2017. godine

KONAČNI IZVJEŠTAJ

O

REVIZIJI INFORMACIONOG SISTEMA
FONDA ZA ZDRAVSTVENO OSIGURANJE CRNE GORE

Podgorica, oktobar 2017. godine

SADRŽAJ

I. OPŠTI DIO ... 3
1. PRAVNI OSNOV ZA VRŠENJE REVIZIJE ... 3
2. PREDMET, OBUHVAT I VRSTA REVIZIJE ... 3
3. CILJ REVIZIJE ... 4
4. SUBJEKAT REVIZIJE ... 4
4.1. DJELATNOST FONDA ZA ZDRAVSTVENO OSIGURANJE ... 4
4.2. UNUTRAŠNJA ORGANIZACIJA ... 5
4.2.1. ORGANIZACIJA SEKTORA ZA INFORMACIONE TEHNOLOGIJE I RAZMJENU PODATAKA INTEGRALNOG INFORMACIONOG SISTEMA ZDRAVSTVA (IZIS) ... 6
4.2.2. SISTEMATIZACIJA RADNIH MJESTA ... 8
4.2.3. STANJE IT LJUDSKIH RESURSA ... 8
4.3. INTEGRALNI ZDRAVSTVENI INFORMACIONI SISTEM I INFORMACIONI SISTEM FONDA ZA ZDRAVSTVENO OSIGURANJE ... 9
4.3.1. INFORMATIČKA INFRASTRUKTURA FONDA (LAN MREŽA) ... 16
4.3.2. APLIKATIVNI SOFTVER ... 16
II. UTVRĐENO ČINJENIČNO STANJE ... 19
5.1. IT STRATEGIJA ... 19
5.2. KONTINUITET POSLOVANJA I OPORAVAK OD KATASTROFE ... 21
5.3. MJERE INFORMACIONE BEZBJEDNOSTI ... 23
5.3.1. FIZIČKA ZAŠTITA SERVERA FZO ... 24
5.3.2. BEZBJEDNOST PROSTORIJA ... 24
5.3.3. PROCJENA RIZIKA ... 25
5.3.4. LOGIČKI PRISTUP I UPRAVLJANJE PRIVILEGIJAMA ... 25
5.3.5. SKLADIŠTENJE PODATAKA ... 28
5.3.6. POLITIKA BEZBJEDNOSTI INFORMACIJA ... 29
5.3.7. ORGANIZACIJA IT BEZBJEDNOSTI ... 31
5.3.8. UPRAVLJANJE BEZBJEDNOŠĆU INFORMACIJA U POSLOVIMA SA DAVAOCIMA USLUGA ... 31
III. ZAKLJUČAK ... 33

I. OPŠTI DIO

1. PRAVNI OSNOV ZA VRŠENJE REVIZIJE

Pravni osnov za vršenje revizije informacionog sistema Fonda za zdravstveno osiguranje Crne Gore sadržan je u:

- Ustavu Crne Gore, član 144 ("Sl. list CG" br. 01/07 i 38/13);
- Zakonu o Državnoj revizorskoj instituciji, član 4 („Sl. list RCG“ br. 28/04, 27/06, 78/06 i "Sl. list CG" br. 17/07, 73/10, 40/11 i 31/14);
- Godišnjem planu revizija Državne revizorske institucije, donesenom od strane Senata 14.12.2016. godine, (interno broj 06-23/16) i Izmjenama godišnjeg plana revizija Državne revizorske institucije od 31.07.2017. godine, (interno broj 06-167/17);
- Odluci o vršenju revizije od 03.04.2017. godine (broj 40113/17-031-610).

Revizija je izvršena u skladu sa:

- Poslovnikom Državne revizorske institucije ("Sl. list CG" br. 3/15);
- Međunarodnim standardima za vrhovne revizorske institucije (ISSAI – nivo III) i
- INTOSAI priručnikom za sprovođenje revizije informacionih sistema za vrhovne revizorske institucije[1].

2. PREDMET, OBUHVAT I VRSTA REVIZIJE

Izvršena je revizija informacionog sistema Fonda za zdravstveno osiguranje Crne Gore – oblast informaciona bezbjednost, u dijelu poštovanja mjera informacione bezbjednosti, saglasno Zakonu o informacionoj bezbjednosti ("Službeni list Crne Gore", br. 014/10 od 17.03.2010, 040/16 od 30.06.2016) i Uredbi o mjerama informacione bezbjednosti ("Službeni list Crne Gore", br. 058/10 od 08.10.2010, 055/15 od 30.09.2015). Revizija je izvršena u skladu sa INTOSAI priručnikom za sprovođenje revizije informacionih sistema za vrhovne revizorske institucije.

Predmet revizije je informaciona bezbjednost, a podoblasti su:

1. Fizička zaštita servera FZO
2. Bezbjednost prostorija
3. Procjena rizika
4. Logički pristup i upravljanje privilegijama
5. Skladištenje podataka
6. Politika bezbjednosti informacija
7. Organizacija IT bezbjednosti
8. Upravljanje bezbjednošću informacija u poslovima sa davaocima usluga.

[1] Priručnik je usvojen na XXI INCOSAI kongresu održanom oktobra 2013. godine u Pekingu.

U sklopu predmeta revizije posebno su obrađene oblasti: IT upravljanje i kontinuitet poslovanja.

Vrsta revizije je revizija informacionog sistema po INTOSAI priručniku za vršenje revizije informacionih sistema za vrhovne revizorske institucije.

3. CILJ REVIZIJE

Cilj revizije je bio da se utvrdi da li je obezbijeđena bezbjednost informacionog sistema kroz integritet baze podataka zdravstvenih osiguranika Fonda za zdravstveno osiguranje Crne Gore.

U svrhu ostvarivanja postavljenog cilja revizije bilo je potrebno dati odgovor na glavno revizorsko pitanje: Da li informacioni sistem Fonda za zdravstveno osiguranje Crne Gore u dovoljnoj mjeri obezbjeđuje sigurnost i zaštitu podataka zdravstvenih osiguranika?

4. SUBJEKAT REVIZIJE

4.1. DJELATNOST FONDA ZA ZDRAVSTVENO OSIGURANJE

Fond za zdravstveno osiguranje Crne Gore (u daljem tekstu FZO ili Fond) obezbjeđuje ostvarivanje prava iz obaveznog zdravstvenog osiguranja osiguranim licima pod jednakim uslovima u skladu sa Zakonom o zdravstvenom osiguranju ("Službeni list Crne Gore", br. 06/16, 02/17 i 22/17).

Odgovorno lice je Sead Čirgić direktora Fonda za zdravstveno osiguranje Crne Gore.

Fond obavlja sljedeće poslove[2]:

1) sprovodi zdravstveno osiguranje, u skladu sa Zakonom o zdravstvenom osiguranju;
2) učestvuje u sprovođenju zdravstvene politike u vezi sa obaveznim zdravstvenim osiguranjem;
3) obavlja poslove u vezi sa ostvarivanjem prava osiguranih lica, prati zakonitost ostvarivanja tih prava i pruža potrebnu stručnu pomoć u ostvarivanju prava i zaštiti njihovih interesa;
4) vodi evidenciju o ostvarenim pravima osiguranih lica iz obaveznog zdravstvenog osiguranja;
5) utvrđuje prioritete u finansiranju zdravstvene zaštite iz sredstava obaveznog zdravstvenog osiguranja, u skladu sa zdravstvenom politikom;
6) zaključuje ugovore sa davaocima zdravstvenih usluga;
7) utvrđuje kriterijume za utvrđivanje cijena zdravstvenih usluga koje su obuhvaćene obaveznim zdravstvenim osiguranjem i način plaćanja;

[2] Član 74 Zakona o zdravstvenom osiguranju.

8) obezbjeđuje sprovođenje međunarodnih ugovora o obaveznom zdravstvenom osiguranju;

9) donosi godišnji program zdravstvene zaštite, godišnji plan javnih nabavki za zdravstvene ustanove čiji je osnivač država, usvaja nacrt godišnjeg finansijskog plana i završni račun sa izvještajem o poslovanju, u skladu sa zakonom;

10) vrši kontrolu izvršenja ugovora, cijena zdravstvenih usluga i kontrolu trošenja sredstava od strane davalaca zdravstvenih usluga sadržanih u ugovoru o pružanju zdravstvenih usluga;

11) razmatra stanje u oblasti zdravstvenog osiguranja i predlaže mjere za efikasno funkcionisanje zdravstvenog osiguranja u Crnoj Gori;

12) sprovodi postupak javnih nabavki za potrebe zdravstvenih ustanova čiji je osnivač država, u skladu sa zakonom;

13) vrši i druge poslove u vezi sa sprovođenjem i ostvarivanjem prava iz zdravstvenog osiguranja, u skladu sa Zakonom o zdravstvenom osiguranju, Statutom i drugim aktima Fonda.

Pored poslova utvrđenih zakonom, Statutom je predviđeno da Fond[3] vodi evidenciju svih podataka vezano za sprovođenje zdravstvenog osiguranja putem jedinstvenog informacionog sistema.

Finansiranje obaveznog zdravstvenog osiguranja obezbjeđuje se iz[4]:

1) doprinosa za obavezno zdravstveno osiguranje;
2) Budžeta Crne Gore;
3) sredstava utvrđenih na osnovu međunarodnih konvencija;
4) naknada štete, kamata, dividendi, renti, akciza i koncesija;
5) drugih izvora, u skladu sa zakonom.

Sredstva obaveznog zdravstvenog osiguranja koriste se za:

1) ostvarivanje prava osiguranih lica;
2) troškove sprovođenja obaveznog zdravstvenog osiguranja;
3) druge rashode, u skladu sa zakonom.

4.2. UNUTRAŠNJA ORGANIZACIJA

Poslovi Fonda za zdravstveno osiguranje Crne Gore su Pravilnikom o unutrašnjoj organizaciji i sistematizaciji, organizovani u okviru šest sektora, tri službe, jednog odjeljenja, deset područnih jedinica i trinaest filijala.

1. Sektor za zdravstveno osiguranje i pravne poslove
2. Sektor za zdravstvenu zaštitu
3. Sektor za kontrolu
4. Sektor za ekonomske poslove za zdravstvenu djelatnost

[3] Član 10 Statuta Republičkog fonda za zdravstveno osiguranje ("Sl. list RCG", br. 070/05 od 23.11.2005).
[4] Član 57 Zakona o zdravstvenom osiguranju.

5. Sektor za javne nabavke za potrebe Fonda i javnih zdravstvenih ustanova
6. Sektor za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva
    6.1. Odsjek za upravljanje promjenama
    6.2. Odsjek za razvoj informacionog sistema
    6.3. Odsjek za operativu
7. Odjeljenje za internu reviziju
8. Služba za odnose sa javnošću
9. Služba za opšte i kadrovske poslove
10. Služba za finansije.

4.2.1. Organizacija Sektora za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva (IZIS)

Odgovorno lice je mr Vladimir Raičković, pomoćnik direktora za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva.

U Sektoru za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva obavljaju se poslovi Fonda koji se odnose na: planiranje i organizovanje rada sektora i saradnju sa ostalim organizacionim jedinicama; pripremanje godišnjeg plana aktivnosti iz djelokruga rada sektora; pripremanje godišnjeg izvještaja o radu iz svog djelokruga rada; obezbjeđivanje evidencije i čuvanja podataka putem jedinstvenog informacionog sistema za potrebe ostvarivanja prava iz obaveznog zdravstvenog osiguranja; učestvovanje u pružanju podrške definisanju razvoja i implementaciji jedinstvenog zdravstvenog informacionog sistema; obezbjeđivanje elektronske razmjene podataka između davaoca zdravstvene zaštite i upravljača zbirki podataka odnosno sa ostalim institucijama u državi u skladu sa Zakonom; učestvovanje u izradi programa razvoja informacionog sistema zdravstva u državi; saradnju sa drugim organima i institucijama iz zemlje i inostranstva u oblasti informacionih tehnologija; poslove zaštite i bezbjednosti podataka i sistema; predlaganje i izrađivanje programa permanentnog informatičkog obrazovanja kadrova; usklađivanje razvoja informacionog sistema sa ostalim informacionim sistemima u državi; učešće u razvojnim projektima iz sistema zdravstvenog osiguranja i zdravstvene zaštite; izvršavanje ostalih zadataka iz djelokruga rada sektora i ostalih zadataka po planu rada odnosno po nalogu direktora.

U Odsjeku za upravljanje promjenama obavljaju se poslovi koji se odnose na: upravljanje promjenama u informacionom sistemu u saradnji sa Odsjekom za razvoj informacionog sistema i ostalim sektorima; analizu i predlog promjena poslovnih procesa; analizu i predviđanje moguće optimizacije i poboljšanja informatičkih usluga i podrške; praćenje postavki sistema i davanje smjernica za upravljanje parametrima informacionog sistema u saradnji sa ostalim sektorima Fonda; parametrizaciju poslovnih aplikacija; praćenje razvoja novih dostignuća iz oblasti informacionih

tehnologija i predlaganje primjene odgovarajućih rješenja; učestvovanje u pripremanju parametara za ugovaranje zdravstvenih usluga sa davaocima; proučavanje i saradnju sa stranim sistemima zdravstvene zaštite i zdravstvenog osiguranja; sarađivanje u spoljnim razvojnim projektima; izrada sistemskih analiza i izvještaja (obezbjeđivanje, obrada, posredovanje i čuvanje finansijskih, zdravstvenih i drugih podataka); predlaganje obrazovnih programa za interno obrazovanje sa područja zdravstvene zaštite, zdravstvenog osiguranja i informacionih tehnologija; prikupljanje i uređivanje podataka sa područja zdravstvene zaštite i zdravstvenog osiguranja; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

U Odsjeku za razvoj informacionog sistema obavljaju se poslovi Fonda koji se odnose na: sprovođenje i realizaciju usvojenih koncepcija i projektnih rješenja za razvoj informacionog sistema; usklađivanje procesa, poslova i dokumentacije sa standardima u sektoru; praćenje razvoja novih dostignuća iz oblasti informacionih tehnologija i predlaganje primjene odgovarajućih rješenja; razvijanje informacionog sistema Fonda; administraciju i projektovanje nadogradnje aplikacija u informacionom sistemu Fonda; staranje o postojećim i razvoj novih aplikativnih rješenja i prezentiranje njihove faze razvoja i rezultata; pružanje operativnih parametara pojedincima i poslovnim jedinicama u korišćenju IS; pružanje neposredne pomoći u upotrebi softvera i upravljanju podacima za sve funkcionalne oblasti u organizaciji; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

U Odsjeku za operativu obavljaju se poslovi Fonda koji se odnose na: sprovođenje i realizaciju usvojenih koncepcija i projektnih rješenja za razvoj informacionog sistema; praćenje razvoja novih dostignuća iz oblasti informacionih tehnologija i predlaganje primjene odgovarajućih rješenja; nadzor nad radom računarskog sistema; planiranje i izradu dopunske sistemske programske opreme; upravljanje i administraciju serverskom infrastrukturom; upravljanje i administraciju komunikacionom infrastrukturom; upravljanje storage sistemom; obezbjeđivanje operativnosti baze podataka; usklađivanje razvoja komunikacione infrastrukture u drugim djelovima zdravstvenog informacionog sistema sa već odabranim standardima korišćenim u Fondu; testiranje razvoj i implementaciju nekih aplikativnih rješenja za podršku sistemskim zahjevima procesima i procedurama; razvoj i rješenja u okviru virtualizacione platforme; nadzor modifikacije i proširenja resursa informacionog sistema; rukovođenje prijemom i brigu o smještaju hardvera i njegovom puštanju u funkciju; obezbjeđivanje i brigu o radu na backup-u podataka u cijelom sistemu za koji je odgovoran sektor; administraciju računarskog operativnog sistema; planiranje i održavanje računarske opreme; obezbjeđenje i zaštitu računarske opreme i podataka od uništenja i neovlašćenog pristupa; uvođenje aplikacionih rješenja; organizaciju i pružanje pomoći prilikom ispada računarskog sistema; savjetovanje i pomoć pri korišćenju računarske opreme i računarskih aplikacija; staranje o pravilnoj upotrebi i ispravnosti hardvera; brigu o

nabavci neophodnih rezervnih djelova, alata i softverskih dijagnostičkih alatki; primjenu i projektovanje naprednih informatičkih tehnologija; koncipiranje i realizaciju sistemskih zahtjeva i rješenja; ostale poslove po nalogu direktora i neposrednog rukovodioca koji po sadržaju spadaju u rad odsjeka.

4.2.2. Sistematizacija radnih mjesta

Po Pravilniku o unutrašnjoj organizaciji i sistematizaciji u Fondu za zdravstveno osiguranje Crne Gore, predviđeno je 285 radnih mjesta (izvršilaca).

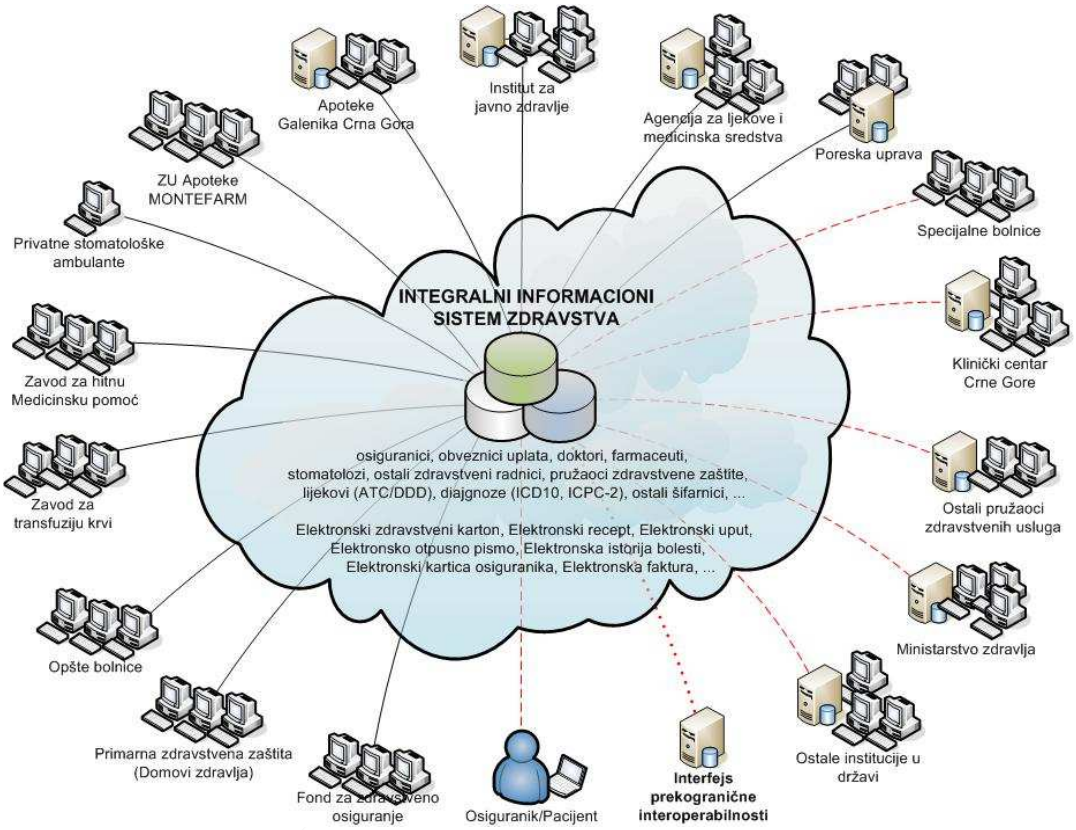
4.2.3. Stanje IT ljudskih resursa

U Sektoru za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva predviđena su 22 radna mjesta od kojih je 16 popunjeno.

Sektor za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva	Predviđeno	Popunjeno
Pomoćnik direktora	1	1
Odsjek za upravljanje promjenama	4	3
Odsjek za razvoj informacionog sistema	7	4
Odsjek za operativu	10	8
UKUPNO	22	16

4.3. INTEGRALNI ZDRAVSTVENI INFORMACIONI SISTEM I INFORMACIONI SISTEM FONDA ZA ZDRAVSTVENO OSIGURANJE

Razvoj Integralnog zdravstvenog informacionog sistema Crne Gore (IZIS) čiji je cilj informatička povezanost subjekata zdravstvenog sistema, otpočet je 2000. godine razvojem Informacionog sistema Fonda za zdravstveno osiguranje. Cjelokupan razvoj počeo razvojem baze osiguranika kao temelja za dalju nadogradnju sistema.



Slika 1: Integralni informacioni sistem zdravstva Crne Gore

Prethodna slika predstavlja Integralni informacioni sistem zdravstva Crne Gore sa svim učesnicima zdravstvenog sistema. Punom linijom su predstavljeni informacioni sistemi koji su integrisani u IZIS u planiranoj mjeri, dok su isprekidanom linijom predstavljeni informacioni sistemi koji su samo djelimično povezani.

Informacije o pacijentu su objedinjene na jednom mjestu bez obzira u kojem se od segmenata sistema osiguranik - pacijent prijavio. Unos podatka u sistem se vrši na mjestu nastanka i dostupan je cijelom sistemu u skladu sa nadležnostima i pravom pristupa.

Integralni informacioni sistem zdravstva Crne Gore obuhvata informacione sisteme sledećih institucija:

1. Fonda za zdravstveno osiguranje
2. ZU Apoteke Crne Gore "Montefarm"
3. Primarne zdravstvene zaštite (PZZ) - domova zdravlja

4. Opštih bolnica (OB)
5. Zavoda za hitnu medicinsku pomoć Crne Gore (ZHMP)
6. Zavoda za transfuziju krvi Crne Gore (ZTK)
7. Privatnih stomatoloških ambulanti koje imaju zaključen ugovor sa Fondom
8. Instituta za javno zdravlje
9. Agencije za ljekove i medicinska sredstva (CALIMS)
10. ZU privatne apoteke koje imaju zaključen ugovor sa Fondom
11. Privatne zdravstvene ustanove i isporučioci medicinsko-tehničkih pomagala koji imaju ugovor sa Fondom
12. Zdravstvenog centra bezbjedonosnih snaga (ZCBS).

Klinički centar Crne Gore (KCCG) još uvijek nije sastavni dio IZIS-a. U dosadašnjem periodu je ostvarena veza između KCCG i FZO u dijelu automatskog ažuriranja baze osiguranika u informacionom sistemu KCCG.

Sektor za informacione tehnologije i razmjenu podataka IZIS-a Fonda za zdravstveno osiguranje pruža tehničku podršku za aplikacije i baze podataka dijela Integralnog informacionog sistema zdravstva Crne Gore koji obuhvata: IS Fonda za zdravstveno osiguranje, IS ZU Apoteke Crne Gore "Montefarm", IS primarne zdravstvene zaštite, IS privatnih stomatoloških ordinacija, IS opštih bolnica, IS Zavoda za hitnu medicinsku pomoć Crne Gore, IS Zavoda za transfuziju krvi Crne Gore i sistema za razmjenu podataka između sistema.

IS Fonda za zdravstveno osiguranje predstavlja osnov Integralnog informacionog sistema zbog činjenice da predstavlja izvor osnovnih podataka o osiguraniku iz kojeg svi ostali subjekti u sistemu dobijaju potrebne podatke i vezu između obveznika uplata doprinosa i pružalaca zdravstvenih usluga. Njegovo funkcionisanje je kritično sa aspekta funkcionisanja cijelog integralnog sistema zdravstva. Zbog te činjenice upravo je Informacioni sistem Fonda za zdravstveno osiguranje direktno povezan sa informacionim sistemima od ključne važnosti u Crnoj Gori: Centralnim registrom osiguranika i obveznika (CROO) koji se nalazi u Poreskoj upravi, Ministarstvom finansija, Agencijom za ljekove i medicinska sredstva Crne Gore, Kliničkim centrom Crne Gore i Centralnim registrom stanovništva koji se nalazi u Ministarstvu unutrašnjih poslova.

Informacioni sistem ZU Apoteke Crne Gore "Montefarm" predstavlja dio Integralnog informacionog sistema zdravstva i pokriva sve radne procese ZU Apoteke Crne Gore "Montefarm". Direktno je povezan na sistem Fonda za zdravstveno osiguranje, a integrisan je i sa sistemom primarne zdravstvene zaštite u dijelu propisivanja i izdavanja lijekova na recept koji se odvija u realnom vremenu. U produkciji je od 01.01.2004. godine.

Informacioni sistem primarne zdravstvene zaštite (domovi zdravlja) predstavlja suštinski dio Integralnog informacionog sistema zdravstva jer se u njemu generišu i čuvaju svi medicinski podaci za svakog od pacijenata

ponaosob. Ovaj sistem je direktno povezan na sistem Fonda za zdravstveno osiguranje, a integrisan je i sa sistemom ZU Apoteke Crne Gore "Montefarm" u dijelu propisivanja i izdavanja lijekova na recept i sa informacionim sistemom opštih bolnica. Razmjena podataka između ovog i pomenutih sistema odvija se u realnom vremenu. U cijelosti je pušten u rad 01.01.2009. godine.

IS privatnih zdravstvenih ustanova – Stomatološke ambulante se za definisane grupe osiguranika ostvaruje se u privatnim stomatološkim ambulantama. Za ove svrhe razvijen je informacioni sistem kojeg sa jedne strane čini serverska infrastruktura koja je smještena u centrali Fonda za zdravstveno osiguranje i sa druge strane 178 stomatoloških ordinacija koje imaju sklopljen ugovor sa Fondom, a čiji se broj mijenja u zavisnosti od javnog poziva. Sistem je povezan na informacioni sistem Fonda za zdravstveno osiguranje i takođe sadrži medicinske podatke za pacijente. U funkciji je od početka 2008. godine.

Informacioni sistem Opštih bolnica predstavlja nadogradnju Integralnog informacionog sistema zdravstva u dijelu medicinskih podataka za svakog od pacijenata ponaosob. Ovaj sistem je direktno povezan na sistem Fonda za zdravstveno osiguranje, i integrisan je sa sistemom primarne zdravstvene zaštite. Razmjena podataka između ovih sistema odvija se u realnom vremenu. U produkciji je 01.01.2010. godine.

Informacioni sistem Zavoda za hitnu medicinsku pomoć Crne Gore u potpunosti je integrisan sa sistemom primarne zdravstvene zaštite i sistemom Fonda za zdravstveno osiguranje. Kao poseban IS u integralnom informacionom sistemu funkcioniše od 01.04.2010. godine.

Klinički centar Crne Gore još uvijek nije integrisan u IZIS. Tenderska procedura za izradu i implementaciju novih programskih modula i nadogradnju postojećih, kojim bi se objedinili Informacioni sistem Kliničkog centra Crne Gore u funkcionalnu cjelinu i koji bi bio sastavni dio Integranog zdravstvenog informacionog sistema, započeta je 10.11.2015. godine objavljivanjem postupka javne nabavke. Međutim, ovaj postupak je obustavljen 11.01.2017. godine Rješenjem br.03/01-346/1.

Centralni registar osiguranika i obveznika (CROO)

Prijava i odjava osiguranika je od 2004. do 2010. godine vršena u Fondu za zdravstveno osiguranje za što je korišten modul Evidencija osiguranika i obveznika uplate doprinosa. Od 01.03.2010. godine sistem Fonda za zdravstveno osiguranje je uključen u projekat objedinjene registracije osiguranika i obveznika uplate doprinosa koji vodi Poreska uprava, a cijeli proces je definisan Protokolom o razmjeni podataka u UCG sistemu. Centralni registar osiguranika i obveznika je od 01.01.2011. godine izvor podataka za bazu osiguranika koju vodi Fond za zdravstveno osiguranje, a Poreska uprava kao izvor podataka odgovorna je za tačnost unosa podataka i jedini je izvor

podataka o svim obveznicima plaćanja poreza i doprinosa za eksterne institucije.

Uspostavljanjem on-line režima podaci iz CROO sistema Poreske uprave se prenose automatski u pomoćnu bazu, a u produkcionu bazu se zatim automatski prenosi definisani set podataka.

Centralni registar stanovništva (CRS)

Povezivanje sa Centralnim registrom stanovništva prvi put je izvršeno u martu 2017. godine. Na ovaj način se iz CRS-a, koji vodi Ministarstvo unutrašnjih poslova, preuzimaju podaci o preminulima, kao i podaci o mjestu prebivališta osiguranika. Sinhronizacija je automatizovana i vrši se petnaestodnevno, a po potrebi se može izvršiti i pojedinačni upit za određeno lice. Takođe je predviđeno vršenje provjere na kraju godine da bi se izbjegla mogućnost da se zbog zakašnjele prijave smrti u CRS-u, koja se evidentira na datum kada je osoba preminula, taj podatak ne prenese u bazu osiguranika Fonda za zdravstveno osiguranje. Za preminula lica se vrši prekid osiguranja čime se oslobađaju kapaciteti za registraciju pacijenata kod izabranih doktora (ID). Sinhronizacija se vrši subotom od 21h i traje oko 6 sati.

U bazi osiguranika na datum 22.03.2017. godine je bilo 760.185 osiguranika. Ažuriranjem podataka baze osiguranika sa podacima iz CRS-a utvrđeno je: za 31.730 matičnih brojeva CRS nema podataka u sistemu, za 728.455 su dobijeni podaci na osnovu matičnog broja, od kojeg broja je 50.330 lica imalo status preminuli, od kojih je: 46.486 imalo status aktivnog osiguranika, 3.841 je bio odjavljen i za 3 lica je bilo prekinuto osiguranje.

Prekid zdravstvenog osiguranja je nastao za 51.933 lica, i to: 50.330 preminulih lica i 1.606 lica koja su osigurana po osnovu nosioca osiguranja, dok je za 3 lica u međuvremenu prekinuto osiguranje.

Aktivnih osiguranika prije ažuriranja preminulih lica sa podacima iz CRS-a je bilo 711.068, a nakon izvršenja procedure u bazi je ostalo 659.135 aktivnih osiguranika (razlika je 51.933 lica).

U konačnom, nakon izvršenja procedure ažuriranja baze osiguranika sa podacima iz CRS-a na dan 25.03.2017. godine prekinuto je osiguranje za 50.327 lica koja su preminula i odjavljeno 5.762 lica koja su bili osigurani po osnovu preminulog nosioca osiguranja, što je ukupno 56.089 lica za koja je prekinuto osiguranje. Takođe, od 50.330 lica sa statusom preminuli, njih 17.383 je imalo izabranog doktora.

Osim ovoga izvršeno je ažuriranje podataka o izbjeglim i interno raseljenim licima sa Kosova, na osnovu podataka dobijenih od MUP – Direktorat za građanska stanja i lične isprave, pa je na dan 13.04.2017. godine prekinuto osiguranje za 11.660 lica. Aktivnih osiguranika prije ažuriranja je bilo 659.649, a nakon ažuriranja 649.138. Razlika je 10.511 lica

koja su imala status aktivnih osiguranika. Odjavljenih lica je bilo 1.149, što je ukupno 11.660 prekinutih osiguranja nakon ažuriranja baze osiguranika.

Saradnja sa partnerima

Izrada Integralnog informacionog sistema zdravstva Crne Gore je počela 2000. godine kada je sklopljen prvi Ugovor o implementaciji poslovnog informacionog sistema sa partnerskom kompanijom, 07.06.2000. godine. Zaključno sa 2017. godinom Fond za zdravstveno osiguranje je sklopio 17 ugovora sa partnerskim kompanijama za izradu softvera.

Tabela predstavlja pregled razvoja IZIS-a kroz ugovore za izradu softverskih modula Integralnog informacionog sistema zdravstva Crne Gore.

R.br.	Ugovori	Ugovorena vrijednost	Datum zaključenja ugovora
1.	Ugovor o implementaciji poslovnog informacionog sistema	DM 11.500,00 + PDV	07.06.2000.g
2.	Ugovor o softveru za kontrolu obveznika uplate doprinosa (OUD)	DM 29.355,00	10.07.2001.g
3.	Ugovor o implementaciji softvera za matične kartone osiguranika i saradnja na formiranju baze OUD	DM 107.500,00 + PDV	29.10.2001.g
4.	Ugovor o implementaciji modula za kadrovsku evidenciju	€3.090,00	25.02.2003.g
5.	Ugovor o softveru za apotekarsko poslovanje i rad veledrogerije	€96.000,00 + PDV	29.05.2003.g
6.	Ugovor o migraciji postojećih aplikacija na on-line rad	€60.000,00 + PDV	07.02.2006.g
7.	Ugovor o softveru za potrebe domova zdravlja Danilovgrad, Tivat i Rožaje	€190.008,00	07.05.2007.g
8.	Ugovor o softveru za primarnu zdravstvenu zaštitu (PZZ) i opstu bolnicu (OB) Pljevlja	€397.800,00	01.08.2008.g
9.	Ugovor o softveru za sekundarnu zdravstvenu zaštitu (SZZ) - opšte bolnice, specijalističke ambulante i stomatološki karton	€237.978,00	20.11.2009.g
10.	Ugovor o softveru za program skrininga	€29.750,00	08.12.2015.g
11.	Ugovor o softveru za grupisanje po dijagnostičko terapijskim grupama (DRG model)	€59.976,00	04.12.2013.g
12.	Ugovor za sofver za privatne apoteke	€17.848,81	23.12.2014.g
13.	Ugovor o softveru za uvođenje dopunskog zdravstvenog osiguranja (DZO)	€28.738,00	27.07.2016.g
14.	Ugovor o izradi WebService-a	€44.982,00	12.01.2016.g
15.	Ugovor o softveru za praćenje realizacije ugovora sa dobavljačima za nabavke medicinskih sredstava	€4.998,00	16.12.2016.g
16.	Ugovor o prilagođavanju softvera opštih bolnica (OB) u 3 specijalne bolnice (SB)	€57.118,81	10.05.2017.g
17.	Ugovor o nadogradnja softvera za privatne apoteke (PA)	€4.938,50	16.06.2017.g
	UKUPNO	**DM 148.355,00 + €1.233.226,62**	

Naredna tabela predstavlja pregled ugovora o održavanju Integralnog informacionog sistema zdravstva Crne Gore, njegovih djelova, kao i ugovora o tehničkoj podršci, koji su se odnosili na 2016. godinu.

R.br.	Ugovori	Ugovorena vrijednost	Datum zaključenja ugovora
1.	Ugovor o održavanju Integralnog informacionog sistema zdravstva	€419.832,00	19.10.2015.g
2.	Ugovor o održavanju za OpenSource tehnologije za IISZ	€27.846,00	11.11.2015.g
3.	Ugovor za održavanje DRG grupera	€12.994,80	26.01.2016.g
4.	Ugovor o održavanju za OpenSource tehnologije za IISZ	€27.846,00	11.11.2016.g
5.	Ugovor o održavanju Integralnog informacionog sistema zdravstva	€437.682,00	20.10.2016.g

Za održavanje IZIS-a za 2016. godinu istovremeno je važilo po tri ugovora, za koje je plaćan mjesečni iznos od ukupno: 38.389,40€ za mjesece januar do oktobar i 39.876,90€ za novembar i decembar 2016. godine.

Numerički prikaz Integralnog zdravstvenog informacionog sistema

Sledeća tabela predstavlja numerički prikaz IZIS-a sa navedenim brojem lokacija, brojem servera, brojem računara i brojem aplikativnih korisnika za svaki njegov segment pojedinačno.

Informacioni sistem		Broj lokacija	Broj računara	Broj aplikativnih korisnika	Serveri		
					Bazni	Aplikativni	Izvještajni
1	IS za potrebe Fonda za zdravstveno osiguranje	21	269	192	2	3	1
2	IS ZU Apoteke Crne Gore "Montefarm"	45	150	314	2	2	1
3	IS primarne zdravstvene zaštite - domovi zdravlja	76	1112	1986	2	2	1
4	IS Zavoda za hitnu medicinsku pomoć	20	32	336			
5	IS opštih bolnica (ISOB)	11	648	1477	2	2	1
6	IS Zavoda za transfuziju krvi	10	57	69			
7	IS privatnih zdravstvenih ustanova – stomatološke ambulante	195	200	379	1	1	
8	IS privatnih apoteka	110	110	0	1	1	
9	IS Instituta za javno zdravlje	1	44	142	2	1	
10	IS CALIMS	1	39	35	2	6	
11	- Sistem za razmjenu podataka - Sistem za testiranje - Sistem za razmjenu poruka				3	8	
U K U P N O		**490**	**2661**	**4930**	**17**	**26**	**4**

Broj aplikativnih korisnika IZIS-a je 4.930 koji na neposredan način pristupaju bazi osiguranika koja je centar Integralnog zdravstvenog informacionog sistema. Broj računara sa kojih se pristupa IZIS je 2.661 sa 490 lokacija. Broj servera u okviru IZIS-a je: 17 baznih, 26 aplikativnih i 4 izvještajna.

1. IS Fonda za zdravstveno osiguranje čine centrala Fonda i 21 područna jedinica, na ukupno 21-oj lokaciji. Ukupan broj računara koji se nalazi u ovom sistemu je 269, definisana su 192 korisnika koji imaju strogo definisana prava pristupa i ovlašćenja za rad nad podacima.

2. IS ZU Apoteke Crne Gore "Montefarm" čini preko 40 apoteka, na 45 lokacija, raspoređenih u svim opštinama u Crnoj Gori od kojih su 38 u on-line režimu rada i veledrogerije sa centralom koja se nalazi u Podgorici. Serverska infrastruktura ovog sistema nalazi se u centralnoj zgradi Fonda za zdravstveno osiguranje. Ukupan broj računara koji se nalazi u ovom sistemu je preko 150, definisano 314 korisnika koji imaju strogo definisana prava pristupa i ovlašćenja za rad nad podacima.

3. IS primarne zdravstvene zaštite pokriva procese u svih 18 domova zdravlja u Crnoj Gori i 3 zdravstvene stanice, na ukupno 76 lokacija. Sistemu

primarne zdravstvene zaštite se pristupa sa 55 lokacija od kojih su 17 centralnih zgrada domova zdravlja po opštinama u Crnoj Gori bez Podgorice, na kojima postoji i do 80 računara. Dom zdravlja Podgorica se sastoji od 15 lokacija na kojima postoji i do 30 računara po lokaciji. Ostale udaljene lokacije su zdravstvene stanice ostalih domova zdravlja u kojima ima do 10 računara. Ukupan broj računara koji se nalazi u ovom sistemu je 1.112, sa 1.986 korisnika koji najveći dio svojih radnih procesa obavljaju na sistemu i imaju strogo definisana prava pristupa i ovlašćenja za rad nad podacima.

4. IS privatnih zdravstvenih ustanova koji se odnosi na stomatološke ambulante obuhvata informatičku podršku za svih 195 stomatološke ordinacije koje su potpisale Ugovor sa Fondom o pružanju zdravstvenih usluga osiguranicima Fonda. Ukupan broj računara koji pristupaju ovom sistemu je preko 200, definisana su 379 korisnika koji imaju strogo definisana prava pristupa i ovlašćenja za rad nad podacima.

5. IS opštih bolnica se sastoji od 7 opštih bolnica u Crnog Gori koje su predmet održavanja: Opšta bolnica Nikšić, Opšta bolnica Cetinje, Opšta bolnica Kotor, Opšta bolnica Bar, Opšta bolnica Pljevlja, Opšta bolnica Bijelo Polje, Opšta bolnica Berane, koje se nalaze na 11 lokacija. U svakoj od bolnica se nalazi od 50 do preko 100 računara. Ukupan broj računara koji se nalazi u ovom sistemu je 648, a broj korisnika sistema je 1.477. Svim korisnicima su sistemom administracije na aplikativnom odnosno baznom softveru strogo definisana prava pristupa i ovlašćenja za rad nad podacima.

6. IS Zavoda za hitnu medicinsku pomoć sastoji se od Centrale koja se nalazi u Podgorici i 19 lokacija po opštinama u Crnoj Gori (smješteni su uglavnom u domovima zdravlja), na 20 lokacija. Aplikacija za Zavod za hitnu medicinsku pomoć se hostuje na serverima primarne zdravstvene zaštite, baza se nalazi na zasebnom serveru, za ZHMP postoji i asterisk server koji služi za snimanje razgovora dispečera. Ukupan broj računara u ovom sistemu je 32, a broj korisnika sistema je 336.

7. IS Zavoda za transfuziju krvi se nalazi na serverima opštih bolnica, sastoji se od centrale u Podgorici i devet centara za transfuziju krvi koji se nalaze u opštim bolnicama, na ukupno 10 lokacija. Broj računara u ovom sistemu je 57, sa 69 korisnika koji mu pristupaju.

Broj zaposlenih u FZO je 196, od kojih 192 u svom radu koriste računar. Broj zaposlenih u Sektoru za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva (koji je zadužen za održavanje cijelog IZIS-a i pojedinih IS zdravstvenih ustanova) je 16. Broj zaposlenih koji imaju korisnički nalog za aplikaciju je 192, a 8 zaposlenih ima administratorski nalog za aplikaciju. Broj računara je 192, a izlaz na internet ima 82 računara.

4.3.1. INFORMATIČKA INFRASTRUKTURA FONDA (LAN MREŽA)

Fond za zdravstveno osiguranje se u smislu računarske mreže sastoji od 22 udaljene lokacije (filijale Fonda) i centralne lokacije u Podgorici gdje je u istoj zgradi smještena i filijala. Na svim lokacijama FZO je realizovana računarska mreža sa utičnim mjestima, centralnim rack ormarom, svičevima i UPS neprekidnim napajanjem.

Centrala Fonda se nalazi zajedno sa filijalom u Podgorici i na toj lokaciji se nalazi server sala sa svim serverima i mrežnom opremom Integralnog zdravstvenog informacionog sistema. Filijale su povezane sa centralom u zvijezda toplogiji što znači da je omogućena samo komunikacija klijenata iz filijala sa centralnom lokacijom. Sigurnosne polise dozvoljavaju samo minimalno potrebnu mrežnu komunikaciju za korišćenje određene poslovne funkcije.

Radi dodatnog odvajanja mrežnog segmenta FZO od ostalih djelova IZIS, kompletna mreža Fonda pripada VLAN-u koji je određen samo za klijente FZO. Svi korisnici sistema se na mrežnom nivou autentifikuju koristeći domenske lozinke i šifru.

Ukupno i okviru Integralnog zdravstvenog informacionog sistema u Crnoj Gori, nalazi se preko 490 lokacija koje razmjenjuju podatke sa centralnom lokacijom u Podgorici. Korisnici svih aplikativnih softvera pristupaju u on-line režimu serverskoj infrastrukturi koja se nalazi u centralnoj zgradi Fonda za zdravstveno osiguranje u Podgorici.

Core sistema predstavlja informacioni sistem za razmjenu podataka preko kojeg se prenose podaci, dokumentacija i vrši elektronska komunikacija među svim podsistemima Integralnog zdravstvenog informacionog sistema. Za razmjenu podataka sa eksternim sistemima (Poreska uprava, MUP, Ministarstvo rada i socijalnog staranja, Ministarstvo finansija, Uprava za kadrove) razvijeni su standardni servisi, uspostavljene potrebne procedure i komunikacioni linkovi.

4.3.2. APLIKATIVNI SOFTVER

Informacioni sistem Fonda za zdravstveno osiguranje pokriva radne procese u centrali Fonda i područnim jedinicama. Za implementaciju softverskog rješenja formirane su baze podataka, a neke od njih su: Baza osiguranika – pacijenata, Baza obveznika uplata doprinosa, Baza ljekara, Baza farmaceuta, Baza stomatologa, Baza ostalog medicinskog osoblja, Baza zdravstvenih ustanova, Baza ljekova po ATC klasifikaciji, Baza dijagnoza MKB 10 i veliki broj šifarnika i parametara. U ovim bazama podataka, koje se nalaze u FZO, nalazi se preko 95% stanovništva Crne Gore, tj. svi oni koji imaju zdravstvenu knjižicu.

U okviru informacionog sistema Fonda za zdravstveno osiguranje razvijeni su sljedeći softverski moduli:

A. Poslovni informacioni sistem (PIS)

Poslovni informacioni sistem obuhvata sve aspekte poslovanja unutar Fonda, kao i integraciju sa poslovnim informacionim sistemima ostalih institucija u zdravstvu u dijelu koji je poslovnim procedurama povezan sa Fondom. Moduli PIS-a u informacionom sistemu Fonda su:

- Upravljanje kadrovima
- Upravljanje finansijama i računovodstvom
- Obračun plata
- Osnovna sredstva
- Administracija
- Modul za integraciju sa poslovnim partnerima.

B. Specifični moduli za poslovne funkcije iz domena rada Fonda

Ovi moduli podržavaju poslovne procese za sve funkcije pri ostvarivanju prava osiguranika po osnovu obaveznog osiguranja.

a. Ostvarivanje prava osiguranika po osnovu obaveznog zdravstvenog osiguranja

- Prijava i odjava osiguranika[5] i obveznika uplate doprinosa (sve poslovne funkcije u tom dijelu);

  Osnovne funkcije modula:
  1. Parametri (šifarski sistem),
  2. Prijem zahtjeva osiguranika i ljekarskih uputa,
  3. Knjiga ljekarske komisije,
  4. Knjiga ostalih ljekarskih komisija
  5. Pravna obrada predmeta,
  6. Obrada faktura po uputima,
  7. Izvještaji.

b. Evidencija, praćenje i kontrola uplata za osiguranike i obveznike uplate doprinosa

  a) Evidencija obveznika uplate doprinosa na osnovu obrasca prijave
  b) Praćenje i kontrola uplata doprinosa,
     i. Praćenje uplate doprinosa,
     ii. Praćenje i kontrola broja osiguranika.

[5] Ove poslovne funkcije su od 1. janura 2011. godine prešle u nadležnost Poreske uprave (osim za neke kategorije).

Ovim modulima su formirani registri (baze) osiguranika i obveznika uplate doprinosa (OUD), koji su osnovni parametri za kompletan informacioni sistem zdravstva. To znači da su sistemi zdravstvenih ustanova povezani sa ovim modulima putem dnevne sinhronizacije podataka.

Na osnovu pristiglih podataka iz Centralnog registra obveznika i osiguranika dnevno se ažuriraju baze podataka Fonda koje se tiču statusa osiguranika i obveznika.

Izvještajima se dobijaju podaci o osiguranicima i obveznicima uplate doprinosa, po različitim kriterijumima, kao i izvještaji za potrebe statističkog posmatranja i analize.

c. Modul za integraciju sa apotekama, praćenje i analizu upotrebe lijekova - sadrži bazu podataka lijekova kao i Pozitivnu listu ljekova, softverski modul za kontrolu upotrebe ljekova, kao i pretragu ljekova (po osiguraniku, ljekaru, ustanovi) i planiranje nabavki ljekova.

d. Modul za integraciju, praćenje i analizu podataka iz primarne zdravstvene zaštite - sadrži neophodne parametre za kontrolu i analizu, automatsko preuzimanje faktura i priloga iz domova zdravlja, kontrolu ispravnosti fakturisanja, praćenje izvršenja plana, te potrebne izvještaje i eksporte podataka za detaljne analize.

e. Modul za integraciju, praćenje i analizu podataka iz stomatoloških ambulanti - obezbjeđuje integraciju stomatološkog dijela informacionog sistema i prihvatanje elektronskih faktura iz svih stomatoloških ordinacija koje imaju ugovor sa Fondom.

f. Modul za integraciju, praćenje i analizu podataka iz sekundarne zdravstvene zaštite (opštih bolnica i ZTK) - omogućava preuzimanje elektronskih faktura i priloga faktura iz opštih bolnica, kontrolu ispravnosti fakturisanja, kontiranje faktura i automatski prenos u finansije.

g. Modul za integraciju, praćenje i analizu podataka iz PZU i isporučioca medicinsko tehničkih pomagala koji imaju ugovor sa Fondom – povezivanjem ovih ustanova od 2016. godine u informacioni sistem Fonda se prenose elektronske fakture sa svim prilozima i evidencijama po pacijentu.

II. UTVRĐENO ČINJENIČNO STANJE

Državna revizorska institucija je na osnovu izvršene Revizije informacionog sistema Fonda za zdravstveno osiguranje Crne Gore – oblast informaciona bezbjednost utvrdila sledeće stanje u ovoj oblasti.

Prilikom vršenja revizije informacionog sistema FZO korištena je: dokumentacija dobijena iz Sektora za informacione tehnologije i razmjenu podataka integralnog informacionog sistema zdravstva, odgovori na pitanja u pisanom obliku i odgovori na upitnike dobijeni od pomoćnika direktora Sektora za informacione tehnologije i razmjenu podataka IZIS, zatim informacije prikupljene putem intervjua sa pomoćnikom direktora, načelnikom Odsjeka za operativu i načelnikom Odsjeka za upravljanje promjenama, informacije objavljene na sajtu Fonda za zdravstveno osiguranje Crne Gore (www.fzocg.me), informacije objavljene na Portalu Vlade Crne Gore (www.gov.me), informacije objavljene na Portalu javnih nabavki (www.portal.ujn.gov.me), informacije prikupljene putem intervjua sa zaposlenima u FZO i podaci dobijeni na bazi ličnog uzorkovanog uvida u aplikativni softver i bazu podataka.

5.1. IT STRATEGIJA

- Zdravstvenu politiku i reformske procese Ministarstvo zdravlja Crne Gore usmjerava kroz Master plan razvoja zdravstva Crne Gore 2015-2020 (od 26.08.2015. godine). Razvoj zdravstvenog informacionog sistema je prepoznat kao ključna i neophodna komponenta uspjeha reformi i boljeg upravljanja i unapređenja zdravstvenog sistema uopšte. Sa početkom Projekta unapređenja sistema zdravstva u Crnoj Gori (od 2004. godine), počele su i paralelne aktivnosti na razvoju zdravstvenog informacionog sistema.

Zdravstveni informacioni sistem integrisano orjentisan i baziran na zajedničkim resursima, uz koordinisano upravljanje i kontrolisanu pokrivenost poslovnih i medicinskih procesa, potencijalno obezbjeđuje ažurne, kvalitetne i korisne podatke i informacije za usmjeravanje strateškog planiranja u sistemu zdravstva, transparentne podatke za upravljanje troškovima u zdravstvu, bolji kvalitet zdravstvene zaštite, upravljanje pacijentom i njegovim zdravstvenim problemima. U cilju boljeg upravljanja za zdravlje i vođenja adekvatne zdravstvene politike, kao i stvaranja preduslova za finansijsku održivost sistema, neophodna su dalja unapređenja i nadogradnje zdravstvenog informacionog sistema.

Značaj e-zdravstva i unapređenje integralnog zdravstvenog informacionog sistema kroz donošenje Strategije razvoja integralnog zdravstvenog informacionog sistema je prepoznat i u Strategiji razvoja informacionog društva Crne Gore do 2020. godine (Ministarstvo za informaciono društvo i telekomunikacije, 21.07.2016. godine).

- Informacioni sistem Fonda za zdravstveno osiguranje Crne Gore je dio Integralnog zdravstvenog informacionog sistema.

U postupku revizije utvrđeno je da je Fond za imao Strateški razvojni plan Republičkog fonda za zdravstveno osiguranje do 2011. godine (21.07.2006. godine), u okviru kojeg je definisan strateški cilj 6 - Razviti integralni informacioni sistem zdravstva uz primjenu savremenih informaciono-komunikacionih tehnologija (IKT) koji podrazumijeva: definisanje i stvaranje uslova i organizacije za primjenu IKT u saradnji sa davaocima zdravstvenih usluga; proširivanje elektronskih i on-line usluga uz korišćenje postojećih baza podataka FZO; uspostavljanje infrastrukture za uključivanje evropskih standarda e-zdravstvene zaštite; definisanje standarda, specificiranje potrebne hardverske i sistemske opreme, specificiranje funkcionalnosti informaciono-komunikacionih rješenja, obezbjeđivanje prostorija i obezbjeđivanje bezbjednosti i tajnosti podataka.

Međutim, projekat Integralni zdravstveni informacioni sistem sadrži: definisanje strategije razvoja, definisanje strukture i obima podataka, definisanje načina komuniciranja u zdravstvenom sistemu, definisanje standarda HW opreme i IKT infrastrukture, postavljanje standarda za sigurnost i bezbjednost i definisanje upravljačke strukture sistema. Početak projekta je bio planiran za 02.10.2006. godine, kraj 08.07.2008. godine, a procjena potrebnih finansija (EUR) je 380.000€.

- U formi predloga je dokument Strategija razvoja Integralnog zdravstvenog informacionog sistema, čiji je nosilac izrade Ministarstvo zdravlja, a iz FZO su bili članovi radne grupe. Ministarstvo zdravlja razmatranje i ažuriranje nacrta teksta Strategije razvoja Integralnog zdravstvenog informacionog sistema planira u narednom periodu u sklopu projekta koje će Ministarstvo zdravlja realizovati u saradnji sa kancelarijom UNDP, a čiji se rok donošenja ne može precizirati.

- IT strategija treba da uspostavi prioritete za duži vremenski period. Finansiranje projekata treba da bude praćeno odgovarajućim IT budžetom. Ovo se odnosi kako na hardver i softver, tako i na stručno zaposlene koji su ili trebaju biti angažovani, dobro obučeni, dobro organizovani i motivisani za efikasan i kvalitetan rad. IT strategija Fonda treba da bude sastavni dio Strategije razvoja Integralnog zdravstvenog informacionog sistema odnosno usaglašena sa istom.

Nalaz 1: Strategija razvoja Integralnog zdravstvenog informacionog sistema nije donijeta, tako da ni Fond za zdravstveno osiguranje nema IT strategiju odnosno akcioni plan kojim bi bili definisani koraci razvoja informacionog sistema Fonda kao dijela IZIS-a.

Rizik 1: Nedonošenje IT strategije Integralnog zdravstvenog informacionog sistema nedoprinosi ispunjavanju ciljeva iz Master plana razvoja zdravstva Crne Gore 2015-2020 i ostvarivanju poslovnih ciljeva Fonda u sistemskom, razvojnom i kadrovskom smislu.

Preporuka 1: Preporučuje se Ministarstvu zdravlja da preduzme dalje aktivnosti na izradi i usvajanju strateškog dokumenta, u okviru kog bi se planirao dalji razvoj Integralnog zdravstvenog informacionog sistema i u sklopu njega informacioni sistem Fonda za zdravstveno osiguranje Crne Gore.

5.2. KONTINUITET POSLOVANJA I OPORAVAK OD KATASTROFE

Kontinuitet poslovanja (eng. Business Continuity) je strateška i taktička sposobnost subjekta revizije da planira i odgovori na incidente i prekide u svom poslovanju, kako bi nastavio sa poslovnim aktivnostima na nivou koji je unaprijed definisan kao prihvatljiv za postizanje ciljeva poslovanja.

Oporavljanje od katastrofe (eng. Disaster Recovery) čine procesi, mjere i procedure koje obezbjeđuju pripremanje oporavka (vraćanja u stanje prije katastrofe) ili eventualni nastavak funkcionisanja ključnih procesa u drugačijim uslovima, što obavezuje subjekat revizije da obezbijedi rezervnu tehnološku infrastrukturu.

Disaster recovery sajt (DRS) je rezervna lokacija koja preuzima funkcionisanje Sistema bez gubljenja podataka i omogućava korisnicima da nesmetano koriste servise informacionih sistema bez zakašnjenja. DRS nije samo lokacija na koju se smještaju rezervne kopije podataka, već lokacija koja ima mogućnost da na svojim serverima i mrežno komunikacionim uređajima čuva podatke u realnom vremenu.

Disaster Recovery centar predstavlja dio procesa upravljanja kontinuitetom poslovanja, koji po definiciji obuhvata identifikovanje i zaštitu kritičnih poslovnih procesa i resursa neophodnih da se održi prihvatljiv nivo poslovanja, štiteći one resurse i primjenjujući one procedure i procese koji će omogućiti opstanak subjekta revizije u slučaju katastrofalnog događaja.

Bivše Ministarstvo za informaciono društvo i telekomunikacije (sada Ministarstvo javne uprave) je na osnovu Strategije implementacije Disaster Recovery-ja (strategija za obezbjeđenje podataka u slučaju katastrofe za potrebe državnih organa i organa uprave u Crnoj Gori), od 23.01.2012. godine, realizovalo projekat izgradnje Disaster Recovery Data centra u Bijelom Polju. Cilj izgradnje je smanjenje rizika od potencijalnih negativnih uticaja u slučaju prirodnih katastrofa, seizmičkih pomjeranja i drugih uticaja koji bi doveli do gubitka podataka smještenih na centralnoj lokaciji u Podgorici. Disaster Recovery Data centar u Bijelom Polju zvanično je pušten u produkcioni rad 20.11.2013. godine.

Nakon završetka prve faze tadašnje Ministarstvo za informaciono društvo i telekomunikacije je na osnovu Zakona o informacionoj bezbjednosti i Uredbe o informacionoj bezbjednosti, koji definišu obaveze svih organizacija da sprovode mjere informacione bezbjednosti, što je u ovom slučaju važno sa aspekta bezbjedne lokacije za odlaganje kopije podataka, naročito imajući u vidu kontinuitet poslovanja, upoznalo sve državne organe, organe državne uprave i sve institucije od državnog značaja sa mogućnošću korišćenja datih resursa na Disaster Recovery lokaciji.

Vlada Crne Gore je na sjednici od 18.12.2014. godine usvojila Informaciju o implementaciji servisa na Disaster recovery lokaciji koju je pripremilo Ministarstvo za informaciono društvo i telekomunikacije, i zadužila organe državne uprave da u informacionim sistemima kojima upravljaju utvrde kritične procese i servise koji podržavaju te sisteme u cilju prenosa i implementacije rezervne kopije na Disaster recovery lokaciji (Zaključak Vlade Crne Gore br: 08-2965/3 od 25.12.2014. godine).

Fond za zdravstveno osiguranje je u 2014. godini započeo aktivnosti migracije i prenosa informacionog sistema[6], ali taj projekat do današnjeg dana nije završen, pa Fond i dalje nema rezervnu lokaciju za oporavak od katastrofe.

U svrhu obezbjeđenja od gubitka podataka svakodnevno se vrši backup baznih, aplikativnih i report servera, takođe, serveri su redudantni i hardverski obezbijeđeni za kontinuitet poslovanja, ali nije vršeno testiranje kontinuiteta poslovanja.

Usled prekida u napajanju električnom energijom, došlo je do incidenta privremenog gašenja Integralnog zdravstvenog informacionog sistema, koji se dogodio 18.06.2016. godine o čemu je sačinjen Izvještaj o uzrocima i posledicama gašenja informacionog sistema – aktivnosti na uspostavljanju produkcije. Nakon prijave sa terena ustanovljen je pad centralnog linka, što je za posledicu imalo da ni jedan servis sistema nije bio dostupan. Prekid je izazvan nenamjernim postupanjem radnika koji su bili angažovani na rekonstrukciji. Nakon određenog vremena (u izvještaju nije precizirano vrijeme), sistem je ponovo uspostavljen.

Nalaz 2: Fond za zdravstveno osiguranje nema uspostavljen plan kontinuiteta poslovanja koji bi imao za cilj uspostavljanje mjera oporavka za prekide u poslovnim aktivnostima, kako bi se kritični poslovni procesi zaštitili od uticaja većih otkaza i da bi se osiguralo njihovo blagovremeno nastavljanje.

Rizik 2: Zbog nepostojanja plana kontinuiteta poslovanja nije utvrđeno ko je zadužen i kako se vrši pokretanje procesa oporavka, što može dovesti do prekida u procesu rada.

[6] Informacija o implementaciji servisa na Disaster recovery lokaciji (Ministarstvo za informaciono društvo i telekomunikacije, 18.12.2014. godine).

Preporuka 2: Preporučuje se Fondu za zdravstveno osiguranje Crne Gore da izradi plan kontinuiteta poslovanja koji će obezbijediti blagovremeno nastavljanje svih kritičnih poslovnih aktivnosti.

Nalaz 3: U Fondu za zdravstveno osiguranje ne postoji plan oporavka od katastrofe. Iako se rezervne kopije podataka čuvaju, u slučaju otkaza postoji mogućnost prekida u procesu rada u dužem vremenskom periodu.

Rizik 3: Neobezbjeđivanjem sekundarne lokacije postoji mogućnost prekida u procesu rada u slučaju većih kvarova na hardveru, na instalaciji ili nekog drugog nepredviđenog događaja zbog kojeg bi došlo do otkaza u radu servera na primarnoj lokaciji, čime bi bili ugroženi poslovni procesi cijelog zdravstvenog sistema Crne Gore.

Preporuka 3: Preporučuje se Fondu za zdravstveno osiguranje Crne Gore da izradi plan oporavka od katastrofe i implementira ga kroz projekat Disaster Recovery, s obzirom da je Disaster Recovery Data centar u Bijelom Polju u funkciji.

5.3. MJERE INFORMACIONE BEZBJEDNOSTI

Mjere informacione bezbjednosti utvrđuju se u skladu sa vrstom podataka, rizicima za njegovu bezbjednost i vrstom zaštite.

Informaciona bezbjednost obuhvata mjere za:
- Fizičku zaštitu
- Zaštitu podataka
- Zaštitu informacionog sistema.

Fizička zaštita obuhvata zaštitu objekata, prostora i uređaja u kojem se nalaze podaci. Mjere informacione bezbjednosti fizičke zaštite su:
1) Uspostavljanje administrativne zone
2) Izrada plana fizičke zaštite
3) Procjena efikasnosti mjera fizičke zaštite
4) Kontrola lica
5) Skladištenje podataka
6) Fizička zaštita informacionih sistema.

Mjere informacione bezbjednosti fizičke zaštite sprovode se radi: sprječavanja neovlašćenog ili nasilnog ulaska lica u objekte i prostorije u kojima se nalaze podaci odnosno uređaji sa podacima, sprječavanja i otkrivanja zloupotreba podataka od strane zaposlenih, otkrivanja i reagovanja na rizike.

Zaštita podataka obuhvata prevenciju i otklanjanje štete od gubitka, otkrivanja ili neovlašćene izmjene podataka. Zaštita podataka odnosi se na:
- Pravila za postupanje sa podacima
- Sadržaj i način vođenja evidencije o izvršenim pristupima podacima
- Nadzor bezbjednosti podataka.

Zaštita informacionog sistema obuhvata zaštitu podataka koji se obrađuju, skladište ili prenose u informacionom sistemu, kao i zaštitu povjerljivosti, cjelovitosti i dostupnosti informacionog sistema u procesu planiranja, projektovanja, izgradnje, upotrebe, održavanja i prestanka rada tog sistema.

5.3.1. FIZIČKA ZAŠTITA SERVERA FZO

Državna revizorska institucija konstatuje da je subjekat revizije preduzeo mjere i u toku vršenja revizije usvojio dokumenta: Fizička bezbjednost (br. 04-2751/1 od 10.04.2017. godine) i Kontrola pristupa informacijama (br. 04-2751/5 od 10.04.2017. godine) koji su politike i procedure Fonda za zdravstveno osiguranje koje se odnose na fizičku bezbjednost.

Dokumentima su između ostalog određene bezbjedonosne zone, ulazak u server salu za lica koja nisu na spisku, kao i iznošenje IT opreme, informacija i softvera van prostorija Fonda.

Istovremeno, subjekt revizije je kao prateća dokumenta donio spisak ovlašćenih lica za pristup server sali i Knjigu evidencije o ulascima u server salu[7].

5.3.2. BEZBJEDNOST PROSTORIJA

Fond za zdravstveno osiguranje nema bezbjedonosni plan IT sistema. Administrativne (bezbjedonosne) zone su uspostavljene dokumentom Fizička bezbjednost (br. 04-2751/1 od 10.04.2017. godine) koji predstavlja plan fizičke zaštite. Fizičko testiranje bezbjednosti nije vršeno. Uspostavljene su mjere zaštite od požara, vlage, hladnoće i toplote na način što se u prostorijama FZO nalaze protiv-požarni aparati, a u server sali su postavljena tri klima uređaja kojima se reguliše toplota, hladnoća i vlažnost. Takođe, na ulazu u server salu se vrši kontrola obezbijeđenog pristupa u okviru koje postoji alarmni sistem sa šifratorom, toplotnim senzorom za mjerenje temperature, senzorom pokreta i senzorom dima. U slučaju da se u server sali pojavi požar-dim automatski se uključuje alarm a takođe se šalje i sms na dva definisana broja mobilnog telefona (načelniku Odsjeka za operativu i službeniku istog Odsjeka). Alarm se takođe aktivira i u slučaju ulaska u server salu bez ukucavanja šifre.

IT sektor po potrebi obavještava nadležne o mogućim incidentima i eventualnim negativnim posledicama po funkcionisanje IZIS-a.

[7] Knjiga evidencije ulazaka u server salu je uvedena 19. juna 2017. godine.

Nalaz 4: Fond za zdravstveno osiguranje nije vršio procjenu efikasnosti mjera fizičke zaštite shodno članu 9 Uredbe o mjerama informacione bezbjednosti.

Rizik 4: Nevršenje procjene efikasnosti mjera fizičke zaštite prostora u kojem se nalaze serveri, mrežna i komunikaciona oprema dovodi do rizika po bezbjednost Integralnog zdravstvenog informacionog sistema.

Preporuka 4: Fond za zdravstveno osiguranje Crne Gore treba da najmanje jednom godišnje, vrši procjenu efikasnosti mjera informacione bezbjednosti fizičke zaštite objekata i prostorija u kojima se nalaze podaci, kao i kad dođe do promjene namjene lokacije ili elemenata u informacionom sistemu, shodno članu 9 Uredbe o mjerama informacione bezbjednosti.

5.3.3. PROCJENA RIZIKA

Nalaz 5: : Fond za zdravstveno osiguranje ne vrši procjenu rizika vezanu za procese pokrivene informacionim tehnologijama. Rizici nisu identifikovani i nisu uspostavljene odgovarajuće strategije ili procedure.

Rizik 5: Postoji mogućnost nastanka negativnih efekata koji bi se reflektovali na funkcionisanje cjelokupnog sistema zdravstva Crne Gore, jer se ne vrši procjena rizika za procese pokrivene informacionim tehnologijama.

Preporuka 5: Potrebno je identifikovati rizike koji su povezani sa informacionim tehnologijama i vršiti redovnu godišnju procjenu rizika i re-procjenu rizika kad god Fond za zdravstveno osiguranje Crne Gore planira da uvede nov informacioni sistem, nadogradnju ili prelazak na noviju verziju.

5.3.4. LOGIČKI PRISTUP I UPRAVLJANJE PRIVILEGIJAMA

Kada je u pitanju logički pristup Fond za zdravstveno osiguranje u svom radu primjenjuje Pravilnik o uslovima, načinu i postupku pristupa podacima u Centru za razmjenu podataka Fonda za zdravstveno osiguranje Crne Gore („Sl. list CG“ br. 70/15 od 16.12.2015. godine) kojim se uređuje pristup podacima i dodjeljuju korisnička prava ovlašćenim licima korisnicima podataka za pristup podacima iz Integralnog zdravstvenog informacionog sistema. Korisnici podataka su davaoci zdravstvene zaštite, upravljači zbirke podataka u oblasti zdravstva i Fond za zdravstveno osiguranje Crne Gore.

Državna revizorska institucija konstatuje da je subjekat revizije preduzeo mjere i u toku vršenja revizije usvojio dokumenta Politika korisničkih šifri (br. 04-2751/4 od 10.04.2017. godine) i Politika udaljenog pristupa (br. 04-2751/3 od 10.04.2017. godine).

Politika korisničkih šifri definiše područje primjene i sadrži uputstva za kreiranje šifri i za zaštitu, a Politika udaljenog pristupa definiše standarde za pristupanje mreži Fonda za zdravstveno osiguranje Crne Gore sa bilo kog mjesta. Procedura za pristup i dodjeljivanje korisničkih prava predstavlja

uputstvo za administraciju sistema kojom se korisnicima sistema dodjeljuju profili i role.

Zahtjev za otvaranje, ažuriranje ili ukidanje korisničkih naloga, korisnici podataka podnose Sektoru za IT i razmjenu podataka IZIS-a. Administratori IZIS za FZO i primarnu zdravstvenu zaštitu su iz Odsjeka za razvoj informacionog sistema, administratori IZIS za sekundarnu zdravstvenu zaštitu i privatne zdravstvene ustanove su iz Odsjeka za upravljanje promjenama i Odsjeka za operativu.

Log fajlovi se evidentiraju u sistemu, ali se ne vrši njihova redovna provjera. Koriste se u svrhu otkrivanja problema ili po pojedinom zahtjevu, što za Fond za zdravstveno osiguranje Crne Gore obavlja partnerska kompanija. Log fajlovi se čuvaju od uspostavljanja svih pojedinačnih sistema, ne postoji stalna kontrola log fajlova, ni od strane lokalnih administratora ni od strane administratora iz partnerske kompanije. Fond nema evidenciju log fajlova koja se može odmah pregledati što potvrđuje da se ne vrši provjera korisničkih naloga i log fajlova.

Zaposleni u Fond za zdravstveno osiguranje Crne Gore nemaju sporazume o povjerljivosti / klauzulu o neobjavljivanju u ugovorima o radu.

Uvidom u proceduru otvaranja korisničkog naloga utvrđeno je sledeće:

- Evidencija o zahtjevima je neuredna.
- Zahtjevi se odnose na otvaranje, ažuriranje i zatvaranje korisničkih naloga.
- Veći dio zahtjeva nije potpisan, zaveden ili ovjeren.
- Zahtjevi se dostavljaju u poslednje vrijeme, administrator ne zna od kada, a prethodno su dostavljani email-om ili faksom što nije pruženo na uvid iako je traženo.
- Za ažuriranje korisničkog naloga (utvrđeno je više različitih korisničkih naloga za istog korisnika, administrator ne zna kada i koje role/profili su dodeljeni i po kojem zahtjevu.
- Nazivi rola u sistemu su internog tipa, pojedini sa imenima zaposlenih, pa se ne može jasno i jednoznačno utvrditi koju funkciju imaju.
- Spisak administratora sistema je 18. jula sadržavao 13 lica – administratora, od kojih je 10 aktivno. Za dva aktivna naloga se nije moglo utvrditi ko ih koristi. Osim zaposlenih iz Fonda na spisku administratora je i saradnik iz partnerske kompanije, dok ostali administratorski nalozi pripadaju zaposlenima u Sektoru za IT i razmjenu podataka u IZIS.
- Ne vrši se provjera ažurnosti korisničkih naloga.

Upoređivnjem spiska korisničkih naloga i evidencije o izvršenim pristupima podacima za avgust 2016. godine, nije se moglo utvrditi, da se prilikom prekida radnog odnosa, korisnički nalog blagovremeno zatvara.

U cilju utvrđivanja da li sistem od korisnika zahtijeva promjenu lozinke pri prvom logovanju, kao i utvrđivanja da li internet browser može zapamtiti korisničku šifru, tražena je demonstracija otvaranja administratorskog korisničkog naloga. Utvrđeno je da korisnik mora svaki put ukucati svoju šifru (web browser je ne pamti) ali da sistem ne zahtijeva od korisnika promjenu šifre pri prvom logovanju. Utvrđeno je da se korisnički (administratorski) nalog može izbrisati iz aplikacije.

Takođe je kroz obavljene intervjue i razgovore sa zaposlenima utvrđeno da pojedine korisničke šifre nisu promjenjene, te je na taj način lako pretpostaviti koja je korisnička šifra zaposlenog. Osim toga, jedan od korisnika sistema je ukazao na praksu da zaposleni za poslovne potrebe međusobno preuzimaju dokumenta što pretpostavlja da jedni drugima znaju šifre za pristup računarima. Takođe, utvrđeno je da korisnici za logovanje na druge sisteme (CROO) koriste nalog i šifru koja nije njihova.

Uvidom u evidenciju zahtjeva u jednom slučaju je utvrđeno da prekidi u radu zaposlenog nisu mogli biti utvrđeni kroz evidenciju zahtjeva za ukidanje korisničkih naloga. Nepostoji zahtjev o ukidanju korisničkog naloga za zaposlenog u periodu prekida zaposlenja u Fondu, iako u evidenciji postoji zahtjev za otvaranje korisničkog naloga od 15.09.2016. godine, nije moglo biti utvrđeno da je u navedenom prekidu zaposlenja korisnički nalog bio zatvoren.

Nalaz 6: Utvrđeno je da se u Fondu za zdravstveno osiguranje Crne Gore neblagovremeno vrši ažuriranje i ukidanje korisničkih naloga.

Rizik 6: Postoji mogućnost neovlašćenog pristupa softveru, kroz neblagovremeno ukidanje korisničkih naloga, naročito kod prekida radnog odnosa.

Preporuka 6: Preporučuje se Fondu za zdravstveno osiguranje da unaprijedi mjere za bezbjednost informacionog sistema kroz procedure i bolju kontrolu logičkog pristupa sistemu i aplikacijama.

Nalaz 7: Revizijom je utvršeno da zaposleni jedni drugima znaju korisnička imena i šifre, kao i da šifre od kreiranja nisu promijenjene, pa ih je lako pretpostaviti, te da zaposleni nisu svjesni odgovornosti koju zahtijeva njihovo radno mjesto.

Rizik 7: Postoji mogućnost zloupotrebe i neovlašćenog pristupa podacima.

Preporuka 7: Preporučuje se Fondu za zdravstveno osiguranje da vrši redovnu edukaciju zaposlenih u smislu obaveze čuvanja i zaštite tajnih podataka kojima po opisu radnog mjesta imaju pristup, kao i da preduzmu mjere na uvođenju lične izjave o prihvatanju odgovornosti za zaposlene.

5.3.5. SKLADIŠTENJE PODATAKA

Procedura skladištenja podataka je opisana u dokumentu Procedura za backup IZIS (br. 04-2751/7 od 10.04.2017. godine). Svakodnevno se u sistemu Fonda za zdravstveno osiguranje odrađuje backup baznih, aplikativnih i report servera IZIS. Fizički backup svih baza IZIS se čuva na storage sistemu, a logički backup baznih servera odrađuje se preko dva Data Protector servera. Precizno je definisano koji sistemi se odrađuju na kojem Data Protector-u.

Ne vrši se sedmično, mjesečno i godišnje skladištenje podataka; ne vrši se čuvanje godišnje uskladištenih podataka; ne vrši se označavanje uskladištenih podataka na propisan način i ne vodi se evidencija informatičkih medija na kojima su podaci uskladišteni, što nije u skladu sa članom 18 stavovi 1, 2, 3, 4, 5, 6, 7 i 8 Uredbe o mjerama informacione bezbjednosti.

U FZO je određena lokacija za odlaganje dnevno uskladištenih podataka, što je u skladu sa članom 19 stav 1 Uredbe o mjerama informacione bezbjednosti. Ne vrši se sedmično, mjesečno i godišnje skladištenje podataka na informatičke medije, pa se samim tim ne mogu odlagati na bezbjednu lokaciju, što nije u skladu sa članom 19 stav 2 Uredbe o mjerama informacione bezbjednosti.

FZO ne vrši šestomjesečnu provjeru upotrebljivosti sigurnosne kopije podataka, što nije u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

FZO nema uspostavljen sistem kriptovane zaštite podataka u prenosu podataka informacionim i telekomunikacionim sistemom, što nije u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

Nalaz 8: Procedura za Backup nije usklađena sa Uredbom o mjerama informacione bezbjednosti (članovi 18, 19 stav 2).

Rizik 8: Nevršenje izrade rezervne kopije podataka u skladu sa Uredbom vezano za skladištenje podataka može dovesti do narušavanja bezbjednosti, povjerljivosti, cjelovitosti i dostupnosti podataka.

Preporuka 8: Fond za zdravstveno osiguranje Crne Gore treba da Proceduru za backup IZIS uskladi sa Uredbom o mjerama informacione bezbjednosti, čl.18 u smislu:

- vrste skladištenja podataka koje se vrše (dnevno, sedmično, mjesečno i godišnje)
- vremena čuvanja godišnje uskladištenih podataka
- označavanja uskladištenih podataka
- vođenja evidencije informatičkih medija na kojima su podaci uskladišteni.

Nalaz 9: FZO ne vrši šestomjesečnu provjeru upotrebljivosti sigurnosne kopije podataka, što nije u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

Rizik 9: Nevršenje provjere rezervne kopije podataka može imati za posledicu nemogućnost obnavljanja rada servera baze podataka.

Preporuka 9: Fond za zdravstveno osiguranje Crne Gore treba da najmanje svakih šest mjeseci vrši provjeru upotrebljivosti sigurnosne kopije podataka, uz provjeru postupka povraćaja baza podataka uskladištenih na informatičkom mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za upotrebu, u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

Nalaz 10: Podaci Integralnog zdravstvenog informacionog sistema se pri prenosu kroz sistem ne kriptuju, što nije u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

Rizik 10: Kada podaci nisu kriptovani postoji rizik pristupa i zloupotrebe od strane neovlašćenih lica.

Preporuka 10: Fond za zdravstveno osiguranje Crne Gore treba da uspostavi sistem kriptovane zaštite podataka u prenosu podataka informacionim i telekomunikacionim sistemom, u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

5.3.6. POLITIKA BEZBJEDNOSTI INFORMACIJA

Što se tiče bezbjednosti informacija Fond nema politiku bezbjednosti informacija, kao ni plan IT bezbjednosti. Jedini dokument je Kontrola pristupa informacijama (br. 04-2751/5 od 10.04.2017. godine), koja je donesena u toku vršenja revizije. Dio ovog dokumenta kojim se definiše administrativni i tehnički pristup informacionom sistemu se primjenjuje na sve računare u sistemu IZIS-a po principu da je definisanim polisama sve zabranjeno sem onog što je eksplicitno dozvoljeno.

Zaposleni u Fondu mogu na računar priključiti eksternu memoriju bez postojanja stvarne poslovne potrebe za tim. Na mrežu FZO nije moguće povezati laptopove ili sopstvene uređaje. Omogućen je VPN pristup za poslovne partnere i pojedine zaposlene u Sektoru za informacione tehnologije i razmjenu podataka IZIS.

Zaštita informacionog sistema se obezbjeđuje nabavkom licenciranog antivirus softvera za sve računare u sistemu IZIS-a za čiju je administraciju zadužen Sektor za IT i razmjenu podataka IZIS (PZZ, SZZ, ZHMP i ZTK).

Samostalni savjetnik II za održavanje sistema iz Odsjeka za operativu, je po opisu poslova definisanim Pravilnikom o unutrašnjoj organizaciji i sistematizaciji radnih mjesta Fonda za zdravstveno osiguranje (broj 01-6748/1, 01-2946, 01-5095 i 01-1784 od 12.12.2013. godine), zadužen da "obezbjeđuje i štiti računarsku opremu i podatke od uništenja i neovlašćenog pristupa". Osim njega svi zaposleni u Odsjeku za operativu se bave uspostavljanjem IT bezbjednosti i kontrolom primjene mjera IT bezbjednosti. Utvrđeno je da se korisnici sistema po potrebi putem e-mail – a obavještavaju o prijetnjama koje su se pojavile.

Međutim, dogodio se incident kada je virus zarazio dva računara u Fondu za zdravstveno osiguranje nad kojima je uspostavljena kontrola podataka i koji je kriptovao sve podatke. Uz podršku trećeg lica kasnije su podaci vraćeni, a jedan od uzroka ovog incidenta je nedovoljna edukacija zaposlenih.

Nalaz 11: FZO nema politiku bezbjednosti informacija i plan IT bezbjednosti.

Rizik 11: Nepostojanje politike bezbjednosti informacija i plana IT bezbjednosti, povećava rizik od unutrašnjih ili spoljašnjih, namjernih ili slučajnih prijetnji po informacije koje se nalaze u sistemu zdravstva.

Preporuka 11: Preporučuje se FZO da izradi politiku bezbjednosti informacija koja treba da sadrži: prava pristupa informacijama, način kontrole njihove primjene, definiše kontrole koje štite od neautorizovanog pristupa informacionim vrijednostima i uputstvo za zaposlene u skladu sa zahtjevima bezbjednosti informacija, kao i plan IT bezbednosti koji uključuje taktičke planove, klasifikaciju podataka, tehnološke standarde, sigurnost i kontrolne politike i upravljanje rizikom.

Nalaz 12: FZO nema uspostavljena bezbjedonosna interna pravila za zaposlene, u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti.

Rizik 12: Nepostojanjem bezbjedonosnih internih pravila za zaposlene postoji rizik od narušavanja informacione bezbjednosti podataka kojima zaposleni imaju pristup.

Preporuka 12: Fond za zdravstveno osiguranje Crne Gore treba da uspostavi bezbjedonosna interna pravila za zaposlene radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti.

5.3.7. ORGANIZACIJA IT BEZBJEDNOSTI

Zaposleni u sistemu zdravstva, korisnici Integralnog informacionog sistema nemaju posebne obuke vezane za informacionu bezbjednost. Pojedine instrukcije putem e-mail – a zaposlenima u vidu upozorenja na prijetnje ili obavještenja o virusima i zaštiti računara povremeno šalje načelnik Odsjeka za operativu. Ne prate se neuspjeli pokušaji logovanja na sistem i ne vrši se provjera log fajlova.

Iako je bilo planirano, zbog opterećenosti obavezama i malog broja raspoloživih zaposlenih, administratori sistema nisu bili u mogućnosti da pohađaju značajnu obuku koja se odnosi na cyber bezbjednost a koju je organizovalo Ministarstvo javne uprave i NATO škola za državne organe.

Nalaz 13: Odsjek za operativu ima sistematizovanih 10 radnih mjesta od kojih je 8 popunjeno, a samo pet službenika radi na poslovima IT bezbjednosti Fonda, PZZ, SZZ, ZHMP i ZTK u čijem sistemu ima ukupno 2.118 računara.

Rizik 13: Nije rijedak slučaj da su samo dva do tri službenika na radnom mjestu, zbog bolovanja i drugih otsustava, što zbog obima posla može dovesti do propusta u radu koji u značajnom mogu ugroziti bezbjednost sistema i podatke koji se nalaze u njemu.

Preporuka 13: Nastaviti aktivnosti na jačanju kadrovskog kapaciteta i potencijala IT stručnjaka u Fondu za zdravstveno osiguranje Crne Gore.

5.3.8. UPRAVLJANJE BEZBJEDNOŠĆU INFORMACIJA U POSLOVIMA SA DAVAOCIMA USLUGA

Fond nema politiku bezbjednosti informacija sa davaocima usluga. Rezervne kopije podataka ne postoje, svi podaci se nalaze u bazama podataka Fonda, ali zaposleni u partnerskoj kompaniji u radu pristupaju produkcionom sistemu i uvijek mogu napraviti kopiju baze podataka.

Sve izvorne kodove i odgovarajuću dokumentaciju o IZIS-u partnerska kompanija je, po tvrdnji pomoćnika direktora, a kako je definisano ugovorima, predala Fondu. Komunikacija između Fonda i partnerske kompanije u vezi sa operativnim radom u toku održavanja sistema definisana je ugovorom i procedurama (Procedura za održavanje serverske infrastrukture, Procedura za napredno održavanje i Procedura za tekuće održavanje softvera). Korisnici IZIS-a potrebe za izmjenama na softveru upućuju zaposlenom u Fondu koji je zadužen za komunikaciju sa davaocem usluga, koji dalje zahtjev prosleđuje partnerskoj kompaniji na izvršenje.

Zaposleni u četiri partnerske kompanije imaju obavezu čuvanja poslovne tajne, što je precizirano u ugovorima.

Jedna od partnerskih kompanija, koja radi na implementaciji i održavanju softvera, ima potpisane generalne sporazume o povjerljivosti sa svojim zaposlenim koji predstavljaju interna dokumenta kompanije i u kojima se klauzula o čuvanju i tajnosti podataka Fonda posebno ne navodi.[8] Međutim, ovi zaposleni prilikom razvoja i održavanja softvera imaju pristup produkcionom sistemu, što omogućava neovlašćeni uvid i izmjenu podataka u bazi osiguranika.

Nalaz 14: FZO nema politiku bezbjednosti informacija sa davaocima usluga.

Rizik 14: Nepostojanje politike bezbjednosti informacija sa davaocima usluga, može dovesti do narušavanja funkcionisanja informacionog sistema.

Preporuka 14: Preporučuje se Fondu za zdravstveno osiguranje da definiše politiku bezbjednosti informacija sa davaocima usluga, radi obezbjeđivanja ispravnog i bezbjednog funkcionisanja informacionog sistema.

Nalaz 15: Fond ne zahtijeva potpisivanje sporazuma o povjerljivosti sa zaposlenima iz partnerskih kompanija.

Rizik 15: Postoji mogućnost da korisnici sistema iz partnerskih kompanija vrše neovlašćeni uvid ili izmjenu podataka u bazi osiguranika.

Preporuka 15: Preporučuje se Fondu za zdravstveno osiguranje da sa korisnicima sistema iz partnerskih kompanija potpisuje izjave o povjerljivosti.

[8] Sporazumi o povjerljivosti sklopljeni između kompanije i njenih 11 zaposlenih od 16.06.2016. godine i sa tri zaposlena od 10.05.2012. godine.

III. ZAKLJUČAK

Na bazi sprovedene revizije i utvrđenog činjeničnog stanja, u skladu sa čl. 45 Poslovnika DRI, nadležni Kolegijum DRI u sastavu: Radule Žurić (član Senata – rukovodilac Kolegijuma) i dr Branislav Radulović (član Senata – član Kolegijuma), na sjednici Kolegijuma DRI održanoj 19.10.2017. godine usvojio je:

KONAČNI IZVJEŠTAJ

o reviziji informacionog sistema Fonda za zdravstveno osiguranje Crne Gore

Odgovornost rukovodstva

Subjekat revizije odgovoran je za dostavljenu dokumentaciju i date činjenice kroz odgovore i intervjue u vezi sa primjenom mjera i standarda informacione bezbjednosti u skladu sa Zakonom o informacionoj bezbjednosti (član 3) i Uredbom o mjerama informacione bezbjednosti.

Odgovornost revizora

Odgovornost Državne revizorske institucije je da, na osnovu izvršene revizije, dâ presjek utvrđenog činjeničnog stanja i zaključak o postupanju subjekta revizije u poštovanju mjera informacione bezbjednosti.

ZAKLJUČAK

Državna revizorska institucija, revizijom informacionog sistema Fonda za zdravstveno osiguranje Crne Gore, revidirala je segment - informaciona bezbjednost.

Državna revizorska institucija, u postupku predmetne revizije, utvrdila je da informacioni sistem Fonda obezbjeđuje ažurnu evidenciju osiguranika i čuvanje podataka, ali da **u dovoljnoj mjeri ne obezbjeđuje** sigurnost istih, utvrđenih mjerama informacione bezbjednosti i standardima iz ove oblasti.

Naime, revizijom je konstatovano da Fond nije blagovremeno usvojio akta u skladu sa Zakonom o informacionoj bezbjednosti, Uredbom o mjerama informacione bezbjednosti i standardima iz ove oblasti, posebno:

- IT strategiju
- Plan kontinuiteta poslovanja
- Plan oporavka od katastrofe
- Procjena rizika
- Politika bezbjednosti informacija
- Plan IT bezbjednosti.

U cilju poboljšanja informacione bezbjednosti, kao i sigurnosti i ažurnost podataka zdravstvenih osiguranika, Državna revizorska institucija izdaje sledeće:

PREPORUKE

Ministarstvu zdravlja:

1. Preporučuje se Ministarstvu zdravlja da preduzme dalje aktivnosti na izradi i usvajanju strateškog dokumenta, u okviru kog bi se planirao dalji razvoj Integralnog zdravstvenog informacionog sistema i u sklopu njega informacioni sistem Fonda za zdravstveno osiguranje Crne Gore.

Fondu za zdravstveno osiguranje Crne Gore:

2. Preporučuje se Fondu za zdravstveno osiguranje Crne Gore da izradi plan kontinuiteta poslovanja koji će obezbijediti blagovremeno nastavljanje svih kritičnih poslovnih aktivnosti.

3. Preporučuje se Fondu za zdravstveno osiguranje Crne Gore da izradi plan oporavka od katastrofe i implementira ga kroz projekat Disaster Recovery, s obzirom da je Disaster Recovery Data centar u Bijelom Polju u funkciji.

4. Fond za zdravstveno osiguranje Crne Gore treba da najmanje jednom godišnje, vrši procjenu efikasnosti mjera informacione bezbjednosti fizičke zaštite objekata i prostorija u kojima se nalaze podaci, kao i kad dođe do promjene namjene lokacije ili elemenata u informacionom sistemu, shodno članu 9 Uredbe o mjerama informacione bezbjednosti.

5. Potrebno je identifikovati rizike koji su povezani sa informacionim tehnologijama i vršiti redovnu godišnju procjenu rizika i re-procjenu rizika kad god Fond za zdravstveno osiguranje Crne Gore planira da uvede nov informacioni sistem, nadogradnju ili prelazak na noviju verziju.

6. Preporučuje se Fondu za zdravstveno osiguranje da unaprijedi mjere za bezbjednost informacionog sistema kroz procedure i bolju kontrolu logičkog pristupa sistemu i aplikacijama.

7. Preporučuje se Fondu za zdravstveno osiguranje da vrši redovnu edukaciju zaposlenih u smislu obaveze čuvanja i zaštite tajnih podataka kojima po opisu radnog mjesta imaju pristup, kao i da preduzmu mjere na uvođenju lične izjave o prihvatanju odgovornosti za zaposlene.

8. Fond za zdravstveno osiguranje Crne Gore treba da Proceduru za backup IZIS uskladi sa Uredbom o mjerama informacione bezbjednosti, čl.18 u smislu:

- vrste skladištenja podataka koje se vrše (dnevno, sedmično, mjesečno i godišnje)
- vremena čuvanja godišnje uskladištenih podataka
- označavanja uskladištenih podataka
- vođenja evidencije informatičkih medija na kojima su podaci uskladišteni.

9. Fond za zdravstveno osiguranje Crne Gore treba da najmanje svakih šest mjeseci vrši provjeru upotrebljivosti sigurnosne kopije podataka, uz provjeru postupka povraćaja baza podataka uskladištenih na informatičkom mediju, tako da vraćeni podaci nakon izvršene provjere budu cjeloviti, povjerljivi i dostupni za upotrebu, u skladu sa članom 20 Uredbe o mjerama informacione bezbjednosti.

10. Fond za zdravstveno osiguranje Crne Gore treba da uspostavi sistem kriptovane zaštite podataka u prenosu podataka informacionim i telekomunikacionim sistemom, u skladu sa članom 22 Uredbe o mjerama informacione bezbjednosti.

11. Preporučuje se FZO da izradi politiku bezbjednosti informacija koja treba da sadrži: prava pristupa informacijama, način kontrole njihove primjene, definiše kontrole koje štite od neautorizovanog pristupa informacionim vrijednostima i uputstvo za zaposlene u skladu sa zahtjevima bezbjednosti informacija, kao i plan IT bezbednosti koji uključuje taktičke planove, klasifikaciju podataka, tehnološke standarde, sigurnost i kontrolne politike i upravljanje rizikom.

12. Fond za zdravstveno osiguranje Crne Gore treba da uspostavi bezbjedonosna interna pravila za zaposlene radi obezbjeđivanja informacione bezbjednosti podataka kojima ta lica imaju pristup, u skladu sa članom 32 Uredbe o mjerama informacione bezbjednosti.

13. Nastaviti aktivnosti na jačanju kadrovskog kapaciteta i potencijala IT stručnjaka u Fondu za zdravstveno osiguranje Crne Gore.

14. Preporučuje se Fondu za zdravstveno osiguranje da definiše politiku bezbjednosti informacija sa davaocima usluga, radi obezbjeđivanja ispravnog i bezbjednog funkcionisanja informacionog sistema.

15. Preporučuje se Fondu za zdravstveno osiguranje da sa korisnicima sistema iz partnerskih kompanija potpisuje izjave o povjerljivosti.

Nadležni Kolegijum DRI utvrdio je da, karakter nalaza u izvršenoj reviziji informacionog sistema Fonda za zdravstveno osiguranje Crne Gore, zahtijeva da subjekt revizije, u roku od 60 dana, dostavi Državnoj revizorskoj instituciji plan aktivnosti za realizaciju preporuka koje se odnose na donošenje akata iz Zakona o informacionoj bezbjednosti, Uredbe o mjerama informacione bezbjednosi i standardima iz ove oblasi.

Fond za zdravstveno osiguranje, kao subjekat revizije, u skladu sa članom 15 Zakona o Državnoj revizorskoj instituciji, dužan je da u roku od 6 mjeseci izvijesti DRI o preduzetim radnjama po datim preporukama.

Podgorica, 19. oktobar 2017. godine

Rukovodilac Kolegijuma DRI

Radule Žurić - član Senata