ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემაში (EHR) პერსონალურ მონაცემთა დაცვა

ანგარიში

ანგარიში შექმნილია ნიდერლანდების საელჩოს მხარდაჭერილი პროექტის ფარგლებში. მის შინაარსზე სრულად პასუხისმგებელია „ინოვაციებისა და რეფორმების ცენტრის“ მკვლევართა ჯგუფი და არ ნიშნავს რომ იგი ასახავს ნიდერლანდების საელჩოს შეხედულებებს.

2020

შესავალი

დღეისათვის ფიზიკურ პირთა პერსონალური მონაცემების მოუწესრიგებელი და უკონტროლო დამუშავებდან მომდინარე საფრთხეების მნიშვნლეობა სცდება ადამიანისთვის მიყენებულ ფსიქოლოგიურ ტკივილსა და დისკომფორტს, რაც შეიძლება გამოიწვიოს ცალკეული პირადი მონაცემების გამჟღავნებამ. პერსონალურ მონაცემთა გადაჭარბებული და უკონტროლო დამუშავება ადამიანის სხვა უფლებებისა და თავისუფლებების შეზღუდვის არსებით რისკებს შეიცავს, რაც დაკავშირებულია ადმიანის ქცევის პროგნოზირებასა და მასზე მანიპულაციის შესაძლებლობასთან, ეს კი თავის მხრივ ასევე საფრთხეს უქმნის თანამედროვე დემოკრატიული წესრიგის არსებობას.

უკანასკნელი ორი ათწლეულის განმავლობაში, ციფრული ტექნოლოგიების განვითარების კვალდაკვალ, სულ უფრო მეტ მნიშვნელობას იძენს ადამიანების და მათი ქცევის შესახებ მონაცემების შეგროვება და დამუშავება. ადამიანის ქცევის შესახებ მონაცემთა ანალიზისა და შესაბამისი პროფილირების საფუძველზე მრავალი მმართველობითი თუ ბიზნეს ამოცანის გადაწყვეტა შეიძლება, თუმცა ამავე დროს იქმნება მომეტებული რისკები ადმიანის პირად ცხოვრებაში და თავისუფლებაში გაუმართლებელი ჩარევისთვის.

შესაბამისად, პერსონალურ მონაცემთა დაცვას, როგორც ადამიანის ერთ-ერთ ფუნდამენტურ უფლებას მზარდი მნიშვნელობა ენიჭება და დემოკრატიული სახელმწიფოები ახლებურ მიდგომებსა და სამართლებრივ მექანიზმებს ავითარებენ მზარდ გამოწვევებზე საპასუხოდ. თანამედროვე სამყაროში არსებულ გამოწვევებთან გასამკლავებლად აღარ არის საკმარისი საკანონმდებლო დონეზე მხოლოდ მონაცემთა დაცვის პრინციპების განსაზღრა და მონაცემთა დაცვის ადეკვატური დონის მისაღწევად სახელმწიფოები უფრო დეტალური, კომპლექსური რეგულაციების შექმნაზე არიან ორინტირებულნი, რომელიც სამართლებრივი პრინციპების და კონცეფციების განსაზღვრასთან ერთად ორგანიზაციული და ტექნოლოგიური გადაწყვეტების სავალდებულოობასაც გულისხმობს.

საქართველოში მრავალი საჯარო თუ კერძო დაწესებულებისთვის პერსონალურ მონაცემთა დაცვის საკითხი ჯერ კიდევ „სიახლედ“ ითვლება, მიუხედავად იმისა, რომ შესაბამისი კანონის ძალაში შესვლიდან 8 წელზე მატი გავიდა. „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი 2012 წლიდან მოქმედებს, თუმცა ამ დროის მანძილზეც საკითხის ცნობადობა და მისი მნიშვნელობის აღქმა მონაცემთა დამმუშავებელთა უმრავლესობისთვის ვერ გასცდა ზოგად შემეცნებით დონეს. საქართველოში ის საჯარო დაწესებულებებიც კი, რომლებიც შეიძლება „სანიმუშოდ“ ითვლებიან მონაცემთა დაცვის სფეროში, ხშირად შორს არიან მონაცემთა დაცვის მაღალი სტანდარტისგან და მხოლოდ კანონის მოთხოვნების ფორმალური დაცვით და ზედაპირზე არსებული პრობლემების მოგვარებით შემოიფარგლებიან.

საქართველოში პერსონალურ მონაცემთა დაცვის საკითხს ზედამხედველობას უწევს დამოუკიდებელი საზედამხედველო ორგანო - სახელმწიფო ინსპექტორის სამსახური. იმის გათვალისწინებით, რომ ინსპექტორის სამსახურის რესურსები შეზღუდულია და ამ შეზღუდული რესურსების მნიშვნელოვანი ნაწილი მიემართება საკითხის ცნობადობის ამაღლებისთვის მიძღვნილ ღონისძიებებზე თუ კონკრეტულ განცხადებება-საჩივრებზე რეაგირებაზე, ზოგჯერ ფოკუსს მიღმა რჩება რიგი კომპლექსური და კრიტიკული საკითხები.

არსებული რეალობისა და იმის გათვალისწინებით, რომ ჩვენს რეალობაში პერსონალურ მონაცემთა დაცვის თემაზე თითქმის არ ისმის ალტერნატიული შეფასებები და საექსპერტო მოსაზრებები, სამოქალაქო მონიტორინგის გზით და შესაბამისი ანგარიშებით გვსურს გამოვკვეთოთ რეალურად არსებული პრობლემური არეები და საზოგადოების ყურადღება მივაპყროთ პერსონალურ მონაცემთა დაცვისა და პირადი ცხოვრების უფლებაში ჩარევის თვალსაზრისით მაღალი რისკების შემცველ სისტემებზე, რომლებიც კომპლექსურ მიდგომასა და მოწესრიგებას საჭიროებს.

1. კონტექსტი

როგორც ადგილობრივი ისე საერთაშირისო კონტექსტის გათვალისწინებით, პერსონალურ მონაცემთა დაცვის საკითხი სულ უფრო აქტუალური ხდება საქართველოშიც, მითუმეტეს, რომ ქვეყანას აღებული აქვს საერთაშორისო ვალდებულებები პერსონალურ მონაცემთა დაცვის საკითხის ევროპული სტადარტების შესაბამისად მოწესრიგებაზე. 2016 წლამდე პერსონალურ მონაცემთა დაცვის საკითხი საქართველოს მთვარობისთვის აქტუალური იყო, ევროკავშირთან სავიზო რეჟიმის ლიბერალიზაციისა და ასოცირების ხელშეკრულების კონტექსტში - საქართველოს მთვარობას ნაკისრი ჰქონდა ვალდებულება გაეუმჯობესებინა პერსონალურ მონაცემთა დაცვის კანონმდებლობა და პრატქიკა. ასევე, აღსანიშნავია, რომ საქართველო მიერთებულია „პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ 108-ე კონვენციას და მის დამატებით ოქმს.

ბოლო წლების განმავლობაში საქართველოში, როგორ სახელმწიფო, ასევე კერძო სექტორში იდგმება ცალკეული ნაბიჯები პერსონალურ მონაცემთა დაცვის საკითხის მოწესრიგებისკენ. თუმცა მიგვაჩნია, რომ გატარებული ღონისძიებები არ არის საკმარისი და არსებული გამოწვევების ადეკვატური. როგორც უკვე აღინიშნა, პერსონალურ მონაცემთა დაცვის საკითხის საკანონმდებლო მოწესრიგებას საქართველოში მხოლოდ 8-9 წლიანი ისტორია აქვს. საჯარო თუ კერძო სექტორში კი მრავალი მიმართულებით რეფორმები ისე გატარდა და მონაცემთა დამუშავების სისტემები ისე განვითარდა რომ პერსონალურ მონაცემთა დაცვის საკითხი საერთოდ არ იყო მხედველობაში მიღებული ან ნაკლები ყურადღება ეთმობოდა. აღნიშნული პრაქტიკა ნაწილობრივ დღემდე გრძელდება, რის შედეგადაც სახეზე გვაქვს

მრავალი საინფორმაციო სისტემა და ინსტრუმენტი, რომელიც დიდი მოცულობით პერსონალურ მონაცემებს ამუშავებს, თუმცა შეუსაბამოა მოქმედ კანონმდებლობასთან, მათი ადაპტირება კი დიდ დანახარჯებთანაა დაკავშირებული, რომლის გაღების საკმარისი მოტივაცია მონაცემთა დამმუშავებელ ორგანიზაციებს არ აქვთ. ამას ნაწილობრივ ისიც განაპირობებს, რომ საქართველოს კანონმდებლობით გათვალისწინებულია ჯარიმების არაადეკვატურად მცირე ოდენობა.

კანონის შემოღებიდან მეცხრე და ინსპექტორის აპარატის დაარსებიდან მეშვიდე წელს პრაქტიკაში ჯერ კიდევ ვხვდებით მონაცემთა დაცვის ძირეული ასპექტების არასწორ გაგებას თუ იგნორირებას. მონაცემთა მსხვილ დამმუშავებელთა ნაწილს, როგორებიცაა მსხვილი ბანკები, სახელმწიფო დასაწესებულებები, სადაზღვევო თუ სატელეკომუნიკაციო კომპანიები და ა.შ. ამდენი ხნის მანძილზე ჯერ კიდევ არ მოუხდენიათ თავიანთი სისტემების ინვენტარიზაცია და რევიზია მონაცემთა დაცვის კანონმდებლობასთან შესაბამისობის დადგენის მიზნით. მეტიც, გასულ წელს ისე დაინერგა ჯანდაცვის ელექტრონული ჩანაწერების (ehr) სისტემა, რომ მონაცემთა დაცვაზე გავლენის სიღრმისეული წინასწარი ანალიზი არ მომხდარა და არ იძებნება ინფორმაცია ამ სისტემაში მონაცემთა დაცვის უზრუნველსაყოფად გატარებული ღონისძიებების - მიღებული ორგანიზაციულ-ტექნიკური ზომების შესახებ.

ასეთ გარემოში უაღრესად მნიშვნელოვანად მიგვაჩია სამოქალაქო საზოგადოების და დამოუკიდებელი ექსპერტების/აქტივისტების როლი, რომლებიც გარედან, ობიექტური დამკვირვებლის თვალით აფასებენ პერსონალური მონაცემების დაცვის თვალსაზრისით ქვეყანაში არსებულ გარემოს და შესაბამისი ცოდნის და გამოცდილების გაზიარებით ხელს უწყობენ სფეროს შემდგომ განვითარებას.

2. კვლევის ამოცანები

ინოვაციებისა და რეფორმების ცენტრმა შეარჩია ისეთი სისტემები, რომლებიც დამუშავებული მონაცემების კატეგორიის, მონაცემთა სუბიექტების სიმრავლისა და ასევე დამუშავების პროცესში გამოყენებული ტექნიკური საშუალებებისა და მათი შესაძლებლობების გათვალისწინებით, პერსონალურ მონაცემთა დაცვის თვალსაზრისით მაღალი რისკის მატარებელს წარმოადგენს.

მნიშვნელოვანია, მსგავს სისტემებში პერსონალურ მონაცემთა დამუშავების საკითხის დეტალური სამართლებრივი რეგლამენტაცია, მონიტორინგის ეფექტიანი და ქმედითი მექანიზმების არსებობა და სისტემის მაქსიმალური გამჭვირვალობა.

იმისათვის, რომ მსგავს მაღალი რისკის შემცველ სისტემებში მინიმუმამდე იქნას დაყვანილი პერსონალურ მონაცემთა უკანონო დამუშავების და მათი არადანიშნულებისამებრ გამოყენების რისკები, აუცილებელია, გატარებული იქნას სამართლებრივი, ორგანიზაციული და ტექნიკური ღონისძიებების ერთობლიობა.

ამგვარი ღონისძიებები შეიძლება იყოს, მათ შორის მონაცემთა დამუშავების საკითხის დეტალური რეგლამენტაცია და გამჭვირვალობის მაღალი ხარისხის უზრუნველყოფა, მონაცემთა დამუშავების პროცესების დოკუმენტირება, ჩანაწერების შენახვის ვადების განსაზღვრა, მონაცემებზე წვდომის კონტროლი, სისტემის დანერგვისას ისეთი პრინციპების უზრუნველყოფა, როგორიცაა მონაცემთა დაცვის სტანდარტების გათვალისწინება ახალი პროდუქტის ან მომსახურების შექმნის პროცესში („Privacy by Design“) და მონაცემთა დაცვა პირველად პარამეტრად („Privacy by Default“), მონაცემთა დამუშავების ზეგავლენის შეფასება (DPIA) და ა.შ.

კვლევის ამოცანას წარმოადგენდა იმის დადგენა, თუ რამდენად არის უზრუნველყოფილი პერსონალურ მონაცემთა დაცვა შერჩეულ სისტემებში და რამდენად სერიოზულად ეკიდებიან საჯარო უწყებები მონაცემთა დაცვის საკითხს მონაცემთა დამუშავების მასშტაბურ, რისკების შემცველ სისტემაში და გატარებულია თუ არა შესაბამისი ორგანიზაციული და ტექნიკური ზომები. უფრო კონკრეტულად კი გვინდოდა პასუხი გაგვეცა შემდეგ კითხვებზე:

- განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების კონკრეტული მიზნები, შესაბამისად, განჭვრეტადია თუ არა მონაცემთა დამუშავების პროცესი მონაცემთა სუბიექტისთვის;
- შეფასებულია თუ არა სისტემაში მონაცემთა დამუშავების ზეგავლენა ან ჩატარდა თუ არა სხვა ტიპის ანალიზი იმის დასადგენად, თუ რა გავლენა აქვს აღნიშნულ სისტემას ფიზიკურ პირთა პერსონალურ მონაცემთა დაცვაზე, რა რისკებს შეიცავს და რამდენად შესაბამისობაშია მოქმედ კანონმდებლობასთან;
- განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების საფუძვლები და ვადები, დაცულია თუ არა მონაცემთა დამუშავების პრინციპები;
- ნათელი და ხელმისაწვდომია თუ არა ინფორმაცია მონაცემთა სუბიექტისათვის, რა მონაცემები შეიძლება დამუშავდეს მის შესახებ ამ სისტემის მეშვეობით;
- რეგულირებულია თუ არა სისტემაში დამუშავებულ მონაცემებზე წვდომის წესები და დონეები;
- რეგულირებული და განჭვრეტადია თუ არა მონაცემთა სუბიექტისთვის სისტემიდან მონაცემების მესამე პირებისათვის გადაცემის საკითხი;
- აქვს თუ არა მონაცემთა დამმუშვებელს მიღებული ადეკვატური ორგანიზაციული და ტექნიკური ზომები სისტემაში მონაცემთა უსაფრთხოების უზრუნველსაყოფად;

კვლევითი ამოცანების შესაბამისად, ინოვაციებისა და რეფორმების ცენტრმა შეიმუშავა კითხვარი და შერჩეული უწყებებიდან გამოითხოვა.

ასევე დამუშავებული იქნა უკვე გამოქვეყნებული/ხელმისაწვდომი ინფორმაცია ნორმატიული აქტებისა და სხვა ინფორმაციის სახით, მათ შორის პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილებები.

3. ძირითადი მიგნებები

შერჩეული სისტემების მონიტორინგის საფუძველზე რამდნეიმე ზოგადი მახასიათებელი გამოიკვეთა. პირველ რიგში, უნდა ითქვას, რომ პერსონალურ მონაცემთა დაცვის მნიშვნელობა მონაცემთა მსხვილი დამმუშავებლების მიერ არასათანადოდაა შეფასებული და გათვალისწინებული. შეფასებული უწყებებისთვის არ ჩანს პერსონალურ მონაცემთა დაცვის საკითხის პრიორიტეტულობა და მისი გათვალისწინება ყოველდღიურ საქმიანობაში, ათასობით მოქალაქის პერსონალურ მონაცემებთან ურთიერთობისას.

მონაცემთა დაცვის საკითხისადმი სისტემური მიდგომა არ არსებობს ისეთ მნიშვნელოვან და მსხვილ დამმუშავებლებშიც, როგორიცაა მაგ. შინაგან საქმეთა სამინისტრო, საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო.

გასათვალისწინებელია, რომ არცერთი შემოწმებული სისტემისათვის, მათ შორის, ისეთი სენსიტიური სისტემებისთვისაც კი, როგორიცაა ჯანმრთელობის შესახებ ჩანაწერების ელექტრონული სისტემა, ჭკვიანი კამერების სისტემა, მშვილებელთა რეესტრი და ა.შ, არ არის შეფასებული მონაცემთა დამუშავების ზეგავლენა და მონაცემთა დამუშავებასთან დაკავშირებული შესაბამისი რისკები.

მონიტორინგის ფარგლებში არცერთ უწყებაში არ აღმოჩნდა მონაცემთა დამუშავების წესების მარეგულირებელი ისეთი დოკუმენტაცია, რომელიც კონკრეტულად უწყებისა თუ სისტემის გათვალისწინებით მოაწესრიგებდა მონაცემთა დამუშავების სპეციფიკურ საკითხებს.

რიგ შემთხვევებში არ არის იდენტიფიცირებული და რეგლამენტირებული მონაცემთა დამუშავების მიზნები და საფუძვლები.

უმეტეს შემთხვევაში პრობლემურია მონაცემთა სუბიექტის უფლების რეალიზების მექანიზმები, რაც გამოიხატება არა იმდენად კონკრეტულ ფაქტებში, როდესაც სუბიექტს შეეზღუდა მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული უფლებები, არამედ სისტემურ სურათში, როდესაც ეფექტიანი მექანიზმების არარსებობა, მონაცემთა წვდომების

არასათანადო აღრიცხვა და ა.შ. ქმნის საფრთხეს მონაცემთა სუბიექტის მოთხოვნა ვერ დაკმაყოფილდეს ან მხოლოდ ნაწილობრივ დაკმაყოფილდეს.

პრობლემურია მონაცემთა შენახვის ვადებთან დაკავშირებული საკითხი, რადგან უმეტესი მონაცემებისა და სისტემებისათვის არ არის განსაზღვრული კონკრეტული, კანონიერ მიზანთან შესაბამისი ვადები. ასევე, არ არსებობს მონაცემთა განდაგურებისა თუ დაარქივების სათანადო წესები.

მონაცემთა დაცვის კანონმდებლობით გათვალისწინებული მონაცემთა უსაფრთხოების უზრუნველსაყოფად მისაღები ორგანიზაციული და ტექნიკური ზომები უწყებების მიერ ძალიან ფრაგმენტულად არის მიღებული. ზოგიერთ უწყებაში გათვალისწინებულია მონაცემთა ბაზებზე წვდომის ავტორიზაცია, ზოგიერთი დამმუშავებელი ახდენს მონაცემთა მიმართ შესრულებული ქმედებების ლოგირებას და ა.შ, თუმცა არცერთ უწყებაში არ აქვს ადგილი სიტუაციის დეტალურ ანალიზს, სათანადო შეფასებას და დამუშავებული მონაცემების ადეკვატური ზომების მიღებას.

4. ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემა (EHR)

4.1 სისტემის აღწერა

2019 წლის 15 იანვარს ამოქმედდა საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის ბრძანება №01-1/ნ, და შეიქმნა „ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემა (EHR)“ და განისაზღვრება მისი წარმოების წესი.

აღნიშნული სისტემის შექმნა გულისხმობს მთელი ქვეყნის მასშტაბით, ყველა სტაციონარული თუ ამბულატორიული სამედიცინო დაწესებულების მიერ ნებისმიერი პაციენტის შესახებ შეგროვებული/დამუშავებული ინფორმაციის (პირის ჯანმრთელობის მდგომარეობის შესახებ პერსონიფიცირებული მონაცემების) შეტანას ერთიან საინფორმაციო სისტემაში, რომლის მფლობელია სამინისტრო. ანუ, ადამიანის ცხოვრების მანძილზე არსებული ავადობისა თუ მკურნალობის ყველა ეპიზოდი თავმოყრილია ერთიან, ცენტრალიზებულ მონაცემთა ბაზაში.

სისტემის მიზანია ხელი შეუწყოს უწყვეტი, ეფექტური, პაციენტზე ორიენტირებული და ხარისხიანი, ინტეგრირებული ჯანმრთელობის დაცვის სისტემის განვითარებას.

2019 წლის ოქტომბრის მდოგმარეობით სისტემაში დარეგისტრირებულია 399 კლინიკა და 5768 ექიმი[1], ხოლო 2020 წლის ივლისის მდგომარეობით სისტემაში უნიკალური პაციენტების რაოდენობა მილიონს აჭარბებს (1,118,036), ხოლო ეპიზოდების რაოდენობა - 2 მილიონს (2,211,755)[2].

4.2. კვლევის ამოცანები

EHR სისტემას აქვს მეტი პოტენციალი ხარისხიანი სამედიცინო ინფორმაციის შესაგროვებლად, ვიდრე სამედიცინო დოკუმენტაციის წარმოების ტრადიციულ ფორმებს. მას პოზიტიურ გავლენის მოხდენა შეუძლია როგორც სამედიცინო მომსახურების ხარისხზე, ისე მთლიანად სექტორის ეფექტიანობაზე. თუმცა, ამავე დროს, EHR სისტემა განაპირობებს პაციენტის შესახებ დიდი მოცულობის, განსაკუთრებული კატეგორიის მონაცემების მაღალ ხელმისაწვდომობას პირთა ფართო წრისთვის.

EHR სისტემა პერსონალური მონაცემების დაცვის თვალსაზრისით წარმოადგენს ერთ-ერთ ყველაზე მგრძნობიარე, მაღალი რისკების შემცველ სფეროს რაც შეიძლება არსებობდეს ბუნებაში, სადაც განსაკუთრებული ყურადღება და ძალისხმევა უნდა იქნას მიმართული პერსონალურ მონაცემთა დაცვის უზრუნველსაყოფად. ეს კი გულისხმობს, რომ მსგავსი სისტემის გაშვებამდე მიღებული უნდა იქნას მთელი რიგი ორგანიზაციული და ტექნიკური

[1] სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 7 თებერვლის გადაწყვეტილება Nგ-1/055/2020 „საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობის და სოციალური დაცვის სამინისტროს შემოწმების დასრულების შესახებ“

[2] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს 2020 წლის 13 ივლისის N01/7968 წერილი

ზომები და სისტემის მფლობელი არ შეიძლება შემოიფარგლოს ნორმატიული აქტის ტექსტში იმის აღიარებით, რომ პერსონალურ მონაცემთა დამუშავება წარმოების კანონის შესაბამისად, მასზე წვდომა შეზღუდულია დამუშავების კანონიერი საფუძვლით და მოქმედებს მონაცემთა ლოგირების სისტემა.

ცივილიზებული სახელმწიფოები, მათ შორის ევროკავშირის წევრი ქვეყნები, სადაც პერსონალურ მონაცემთა დაცვის მაღალი კულტურა არსებობს, მსგავსი სისტემების შექმნისას განსაკუთრებული ყურადღებით ეკიდებიან პერსონალურ მონაცემთა დაცვის საკითხს და შეიძლება ითქვას რომ სისტემის შექმნის დროს, მის ეფექტიანობისა და ტექნიკურ გამართულობასთან ერთად, თანაბარმნიშვნელოვან საზრუნავად მიიჩნევენ პერსონალურ მონაცემთა დაცვას. შესაბამისად, ამ პრიზმაში ხდება სისტემის ყველა კონცეპტუალრი, სამართლებრივ-პროცედურული და ტექნოლოგიური საკითხის განხილვა/გადაწყვეტა.

კვლევის ამოცანას წარმოადგენდა იმის დადგენა, თუ რამდენად არის უზრუნველყოფილი პერსონალურ მონაცემთა დაცვა ელექტრონული ჯანდაცვის სისტემაში - რამდენად სერიოზულად და გულისხმიერად ეკიდება საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტრო პერსონალურ მონაცემთა დაცვის საკითხს მონაცემთა დამუშავების ასეთი მასშტაბურ, რისკების შემცველ სისტემაში და გატარებულია თუ არა შესაბამისი ორგანიზაციული და ტექნიკური ზომები. უფრო კონკრეტულად კი გვინდოდა პასუხი გაგვეცა შემდეგ კითხვებზე:

- განსაზღვრული და დეკლარირებულია თუ არა მონაცემთა დამუშავების საფუძვლები და ვადები, დაცულია თუ არა მონაცემთა დამუშავების პრინციპები;
- რეგულირებულია თუ არა სისტემაში დამუშავებულ მონაცემებზე წვდომის წესები და დონეები;
- რა როლებია გათვალისწინებული სისტემაში დამუშავებულ მონაცემთა წვდომისათვის და რით არის მოწესრიგებული აღნიშნული;
- აქვს თუ არა სამინისტროს მიღებული ადეკვატური ორგანიზაციული და ტექნიკური ზომები სისტემაში მონაცემთა უსაფრთხოების უზრუნველსაყოფად;
- არსებობს თუ არა მონაცემთა დაცვისა და უსაფრთხოებისკენ მიმართული წესებისა და პროცედურების შესრულების აუდიტის პროცედურა და ჩატარებულია თუ არა მსგავსი აუდიტი სისტემის გაშვების შემდგომ
- რა ზომებია მიღებული სისტემის ლოგების მთლიანობისათვის (integrity)?
- სისტემის გაშვების შემდგომ ჩატარდა თუ არა სამედიცინო დაწესებულებების ლოკალური EMR სისტემების აუდიტი
- შეფასებულია თუ არა სისტემაში მონაცემთა დამუშავების ზეგავლენა ან ჩატარდა თუ არა სხვა ტიპის ანალიზი იმის დასადგენად, თუ რა გავლენა აქვს აღნიშნულ სისტემას ფიზიკურ პირთა პერსონალურ მონაცემთა დაცვაზე, რა რისკებს შეიცავს და რამდენად შესაბამისობაშია მოქმედ კანონმდებლობასთან;
- არსებობს თუ არა სამინისტროში და მის კონტროლს დაქვემდებარებულ დაწესებულებებში პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხების მართვის სისტემა (privacy management framework/data protection program) შესაბამისი როლებით, პასუხისმგებელი პირებით და შესაბამისი პოლიტიკებით/პროცედურებით

- სისტემის გაშვების შემდგომ რამდენმა ადამიანმა (როგორც სამინისტროს წარმომადგენელმა, ისე ექიმმა და სისტემაზე წვდომის მქონე პირმა) გაიარა ტრენინგი ან რამე ტიპის გადამზადება პერსონალურ მონაცემთა დაცვის თემებზე

კვლევითი ამოცანების შესაბამისად, ინოვაციებისა და რეფორმების ცენტრმა შეიმუშავა კითხვარი და საქართველოს შინაგან საქმეთა სამინისტროსგან გამოითხოვა საჯარო ინფორმაცია.

ასევე დამუშავებული იქნა უკვე გამოქვეყნებული/ხელმისაწვდომი ინფორმაცია ნორმატიული აქტებისა და სხვა ინფორმაციის სახით, მათ შორის პერსონალურ მონაცემთა დაცვის ინსპექტორის გადაწყვეტილება.

4.3 კვლევის შედეგები

კვლევის ფარგლებში გამოთხოვილი და დამუშავებული ინფორმაციის ანალიზის საფუძველზე გამოიკვეთა შემდეგი სახის პრობლემები:

<u>მონაცემთა დამუშავების საფუძველი</u>

არ არის მკაფიო სისტემაში მონაცემთა დამუშავების საფუძვლები

სისტემაში მუშავდება როგორც ჩვეულებრივი კატეგორიის, ისე განსაკუთრებული კატეგორიის პერსონალური მონაცემები, კერძოდ მონაცემები ადამიანის ჯანმრთელობის მდგომარეობის შესახებ. სამინისტროსაგან მიღებული პასუხისა და ინსპექტორის ხსენებული გადაწყვეტილების თანახმად სისტემაში მონაცემთა დამუშავების საფუძვლად მითითებულია „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-6 მუხლის მე-2 პუნქტის „გ“ ქვეპუნქტი - მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცვის სისტემის მართვისათვის ან ფუნქციონირებისათვის.

სისტემის მომხმარებლები, გარდა კონკრეტული ექიმისა და პაციენტისა ასევე არიან სამინისტროს სახელმწიფო კონტროლს დაქვემდებარებული სსიპ-ები:

- **სოციალური მომსახურების სააგენტო** ჯანდაცვის სახელმწიფო პროგრამების ზედამხედველობის განხორციელების და კანონმდებლობით მისთვის დაკისრებული სხვა მოვალეობების შესრულების მიზნით.

- **ლ. საყვარელიძის სახელობის დაავადებათა კონტროლისა და საზოგადოებრივი ჯანმრთელობის ეროვნული ცენტრი** (შემდგომში – ცენტრი) საზოგადოებრივი ჯანდაცვისა და კანონმდებლობით მისთვის დაკისრებული სხვა მოვალეობების შესრულების მიზნით.

- **სამედიცინო საქმიანობის სახელმწიფო რეგულირების სააგენტო** (შემდგომში – რეგულირების სააგენტო), ჯანდაცვის სახელმწიფო პროგრამების ზედამხედველობისა,

სამედიცინო დახმარების ხარისხის კონტროლის განხორციელების და კანონმდებლობით მისთვის დაკისრებული სხვა მოვალეობების შესრულების მიზნით.

ბრძანების მე-3 მუხლის მე-10 პუნქტი კი ადგენს რომ აღნიშნული დაწესებულებები - „კანონმდებლობით მინიჭებული უფლებამოსილების ფარგლებში, EHR სისტემის ანალიტიკური გვერდის საშუალებით, უზრუნველყოფენ EHR სისტემაში არსებული ინფორმაციის დამუშავებას, მოქმედი კანონმდებლობისა და ამ დანართით განსაზღვრული წესის შესაბამისად. მონაცემებთან წვდომა განხორციელდება სისტემის მფლობელისაგან ავტორიზებული მომხმარებლის უფლების მინიჭების გზით.“

შესაბამის კითხვაზე სამინისტროსაგან მიღებული პასუხის თანახმად „ეს მონაცემები მეტწილად დეპერსონალიზებულ ხასიათს ატარებს. დღეისათვის ანალიტიკური გვერდი დამუშავების პროცესშია, ამიტომ აღნიშნული სამსახურების მიერ მონაცემთა მოთხოვნას ადგილი არ ჰქონია“[3], ასევე „პერსონალურ მონაცემებთან წვდომაზე მოთხოვნა ... განიხილება ინდივიდუალურ რეჟიმში“.[4]

აღნიშნულ უწყებებთან/სსიპ-ებთან დაკავშირებით ჩნდება კითხვა - პერსონალურ მონაცემთა დაცვის შესახებ კანონით გათვალისწინებული რომელი საფუძვლით ამუშავებენ ისინი პაციენტის ჯანმრთელობასთან დაკავშირებულ მონაცემებს, ანუ რა საფუძვლით აქვთ წვდომა EHR სისტემაზე. პერსონალურ მონაცემთა დაცვის შესახებ კანონის მე-6 მუხლი ადგენს განსაკუთრებული კატერგორიის პერსონალურ მონაცემთა დამუშავების საფუძვლების ამომწურავ ჩამონათვალს, რომელთაგან მხოლოდ 2 შეიძლება მოვიაზროთ მონაცემთა დამუშაების საფუძვლად მოცემულ კონტექსტში:

> *ა) მონაცემთა სუბიექტის წერილობითი თანხმობა;*
>
> *გ) მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცის სისტემის მართვისთის ან ფუნქციონირებისთვის;*

ბრძანების ტექსტიდან არ იკითხება რომ EHR სისტემაში პაციენტის შესახებ მონაცემების შეტანისას აუცილებელია მისგან წერილობითი თანხმობის მიღება, ანუ მონაცემთა დამუშავების საფუძველი არ არის სუბიექტის თანხმობა. შესაბამისად, რჩება მხოლოდ მეორე შესაძლო საფუძველი - *„მონაცემები მუშავდება საზოგადოებრივი ჯანმრთელობის დაცვის, ჯანმრთელობის დაცვის ან დაწესებულების (მუშაკის) მიერ ფიზიკური პირის ჯანმრთელობის დაცვის მიზნით, აგრეთვე თუ ეს აუცილებელია ჯანმრთელობის დაცის სისტემის მართვისთვის ან ფუნქციონირებისთვის“*.

სწორედ აქ ჩნდება კითხვა თუ რამდენად მართებულია განსაკუთრებული კატეგორიის მონაცემების დამუშავების საფუძვლად არსებული ნორმის ასეთი ფართო/განვრცობითი

---

[3] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს 2020 წლის 4 ივნისის N01/5923 წერილი

[4] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს 2020 წლის 13 ივლისის N01/7968 წერილი

განმარტება და მისი გამოყენება ზემოაღნიშნულ სამ უწყებასთან მიმართებით, რომლებიც სრულიად განსხვავებულ ფუნქციებს ასრულებენ.

აქვე ისიც უნდა აღინიშნოს, რომ არც ბრძანების ტექსტიდან და არც სამინისტროსაგან მიღებული პასუხიდან კონკრეტულად არ ირკვევა თუ რა სახის წვდომა აქვთ EHR სისტემაზე ზემოაღნიშნულ სსიპ-ებს და რას გულისხმობს მათ მიერ EHR სისტემის ანალიტიკური გვერდის საშუალებით მონაცემთა დამუშავება. გაურკვეველია - აქ საუბარია მხოლოდ დეპერსონიფიცირებულ მონაცემებზე თუ სისტემის ანალიტიკური გვერდის საშუალებით მონაცემთა დამუშავება გულისხმობს, მათ შორის, კონკრეტულ პაციენტთა პერსონალურ/სამედიცინო მონაცემებზე წვდომასაც ან თუ ეს წვდომები დეპერსონიფიცირებულია, რითია უზრუნველყოფილი აღნიშნული.

სისტემის გაუმჭვირვალობა

მონაცემთა სუბიექტისათვის არ არის განჭვრეტადი ის, თუ ვის და რატომ მიუწვდება მის მონაცემებზე ხელი

ბრძანების თანახმად EHR სისტემაში მონაცემები შედის ყველა პაციენტის შესახებ, რის თაობაზეც მას არ ეკითხებიან/მისგან თანხმობას არ ითხოვენ, რაც ნიშნავს რომ სისტემაში მონაცემების შეყვანა სავალდებულოა ყველასთვის. ამავე დროს ბრძანების ტექსტის ანალიზიდან ირკვევა რომ პაციენტს უფლება აქვს სრულად ან ნაწილობრივ დაფაროს EHR სისტემაში მის შესახებ არსებული მონაცემები. თუ პაციენტს უფლება აქვს სრულად და უპირობოდ/უვადოდ დაფაროს მის შესახებ ნებისმიერი მონაცემი, მაშინ რა მნიშვნელობა აქვს EHR სისტემაში მონაცემების შეტანის სავალდებულოობას? ამავე კონტესტში, ბუნდოვანია, თუ რა შედეგებს იწვევს პაციენტის მიერ მონაცემების დაფარვა EHR სისტემის ისეთი მომხმარებლებისთვის, როგორებიცაა სამინისტროს სსიპ-ები. ნიშნავს თუ არა მონაცემების დაფარვა, მათთვის დაფარვასაც, თუ ის მხოლოს ექიმებს უზღუდავს EHR-ში კონკრეტული პაციენტის მონაცემებზე წვდომას.

მონაცემთა თავისთავადი დაცულობა (Privacy by default)

დარღვეულია მონაცემთა თავისთავადი დაცულობის პრინციპი

მონაცემთა დამუშავების პრინციპებიდან ერთ-ერთია მონაცემთა მინიმიზაციის პრინციპი რაც გულისხმობს, რომ მონაცემები მხოლოდ იმ მოცულობით უნდა დამუშავდეს, რაც აუცილებელია მონაცემთა დამუშავების მიზნის მისაღწევად. აღნიშნული პრინციპი განმტკიცებულია მონაცემთა დაცვის კარგი პრაქტიკის მაგალითებითა და მონაცემთა დაცვის ზოგადი ევროპული რეგულაციით (GDPR), რომელმაც ნორმატიულ დონეზე დააწესა მონაცემთა თავისთავადი დაცულობა/მონაცემთა დაცვა პირველად პარამეტრად (Privacy by Design and by Default) და განსაზღვრა, რომ მონაცემთა დამმუშავებელმა უნდა უზრუნველყოს ფიზიკური პირების განუსაზღვრელი რაოდენობისათვის პერსონალური მონაცემების პირველად პარამეტრად ხელმისაწვდომობის შეზღუდვა, ადამიანური ძალის ჩარევის გარეშე.

ამავეს იმეორებს „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს პარლამენტში ინიცირებული კანონის პროექტი.

EHR სისტემის შემთხვევაში კი დარღვეულია სწორედ აღნიშნული პრინციპი, როგორც ნორმატიულ დონეზე, ისე პრაქტიკული განხორციელებადობის თვალსაზრისით:

ბრძანების მე-11 მუხლის მე-8 პუნქტის თანახმად „ექიმის მიერ EHR სისტემაში გადაცემული (შეყვანილი) ეპიზოდის/ვიზიტის მონაცემები ჩვეულებრივ ხილულია (გაზიარებულია) სისტემაში ავტორიზებული ყველა ექიმისთვის, შესაბამისად, ხილულია ამ ეპიზოდის/ვიზიტის შესაბამისი ცხოვრების ანამნეზის შემადგენელი მონაცემებიც“.

ანუ სისტემაში შეტანილი მონაცემები თავისთავად ღიაა სისტემის მომხმარებლებისათვის, მანამ სანამ პაციენტი არ მოისურვებს მის დაფარვას. პაციენტს მონაცემების დაფარვის 2 გზა აქვს - ა) მას შეუძლია მონაცემთა დაფარვა სთხოვოს ექიმს, რისთვისაც პაციენტის ტელეფონის ნომერზე მოსული, სისტემის მიერ გენერირებული კოდი უნდა გადასცეს ექიმს; ბ) პაციენტს შეუძლია თვითონ შევიდეს თავის პირად გვერდზე და დაფაროს მონაცემები სრულად ან მისი ნაწილი;

თუ გავითვალისწინებთ, რომ **სისტემაში მონაცემების შეტანა შესაძლებელია პაციენტის გაწერიდან 14 კალენდარული დღის ვადაში**, გამოდის რომ მონაცემების შეტანის მომენტისათვის პაციენტი სამედიცინო დაწესებულებაში აღარ იმყოფება და ექიმი მას ვერ დაეხმარება მონაცემთა დაფარვაში. თუმცა, პაციენტი სპეციალურად რომ მივიდეს ექიმთან ამ მიზნით ან შემდგომი ვიზიტისას მოითხოვოს აღნიშნული გზით მონაცემების დაფარვა, მაინც პრობლემურია ექიმისთვის ზეპირსიტყვიერად კოდის გადაცემის და მონაცემთა დაფარვის მოთხოვნის საკითხი - ადვილად შეიძლება წარმოიშვას დავა თუ კონკრეტულად რა მოთხოვნით გადასცა კოდი პაციენტმა და შეესაბამება თუ არა ექიმის მოქმედება (მონაცემთა დაფარვის დონე, დასაფარი ეპიზოდები და ა.შ) პაციენტის ნებას;

რაც შეეხება მონაცემთა დაფარვის მეორე გზას (პაციენტი თვითონ შევიდეს თავის პირად გვერდზე და დაფაროს მონაცემები), ეს პრაქტიკული თვალსაზრისით გამოუსადეგარი იქნება პაციენტთა დიდი ნაწილისთვის. მოსალოდნელია რომ უმრავლეს შემთხვევაში მონაცემები სრულად ღია დარჩება და ეს არ იქნება პაციენტის გაცნობიერებული არჩევანი.

მონაცემებზე წვდომა

არ არის მოწესრიგებული მონაცემებზე წვდომის შეზღუდვის საკითხი

სამინისტროსგან მიღებული ინფორმაციის თანახმად, სისტემაში არსებობს შემდეგი როლები: ექიმის, პაციენტისა და მფლობელის მიერ მინიჭებული ავტორიზებული მომხმარებლის როლი (ანალიტიკის გვერდისთვის).

ანალიტიკის გვერდის მიზნებისთვის სისტემაზე წვდომასთან დაკავშირებით, როგორც უკვე ვიმსჯელეთ მონაცემთა დამუშავების საფუძვლების განხილვის ქვეთავში სამინისტროს მმართველობის სფეროში შემავალ სსიპ-ებთან დაკავშირებით, სამინისტრო ამბობს, რომ ანალიტიკური გვერდი დამუშავების პროცესშია.

ამავდროულად, სამინისტროს შემოწმების შესახებ ინსპექტორის გადაწყვეტილებაში ვკითხულობთ, რომ სამინისტროს მხრიდან EHR სისტემაზე წვდომა აქვს ინფორმაციული ტექნოლოგიების დეპარტამენტის დეველოპინგის ჯგუფის 2 თანამშრომელს და ინფორმაციული ტექნოლოგიების დეპარტამენტის უფროსის მოადგილეს, აღნიშნული პირები სარგებლობენ განპიროვნებული მომხმარებლის სახელით და პაროლით. მათი მხრიდან წვდომის მიზანს სამინისტროს წარმომადგენლის განმარტებით, წარმოადგენს სისტემის მონიტორინგი და ადმინისტრირება, ასევე დეველოპინგის პროცესის წარმართვა.

თუმცა არც ბრძანებიდან და არც ინსპექტორის გადაწყვეტილებიდან არ იკითხება მონაცემებზე წვდომისა და სისტემაში განსახორციელებელი ქმედებების ფარგლები. არ ვიცით, აღნიშნულ პირებს წვდომა აქვთ პერსონიფიცირებულ მონაცემებზე თუ არა.

ყოველივე აღნიშნულიდან გამომდინარე, შეიძლება ითქვას, რომ სამინისტროს სისტემაში დამუშავებულ პერსონალურ მონაცემებზე წვდომის საკითხი არ აქვს დოკუმენტირებული და შესაბამისად რეგლამენტირებული.

<u>ლოგირება</u>

არ არის უზრუნველყოფილი ლოგების მთლიანობა

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის თანახმად მონაცემთა დამმუშავებელი ვალდებულია უზრუნველყოს ელექტრონული ფორმით არსებული მონაცემების მიმართ შესრულებული ყველა მოქმედების აღრიცხვა.

ბრძანების მე-8 მუხლის თანახმად „EHR სისტემაში ინფორმაციის დამუშავება ლოგირდება მომხმარებელთა დონეზე. . . . ლოგი შეიცავს მონაცემთა დამუშავების თარიღს, დამუშავებული მონაცემის მაიდენტიფიცირებელ ჩანაწერს, ინფორმაციას მონაცემთა დამუშავების ფორმის შესახებ (დათვალიერება, შეტანა/განახლება, ექსპორტი), ინფორმაციას დამმუშავებლის ვინაობის თაობაზე.“

ამავე მუხლის თანახმად ლოგები ინახება შესაბამისი ქმედების თარიღიდან 3 წლის განმავლობაში, თუ კანონმდებლობით სხვა რამ არ არის დადგენილი. ამავე ვადაზე მიუთითებს სახელმწიფო ინსპექტორი საკუთარ გადაწყვეტილებაში, თუმცა სამინისტროსაგან მიღებულ პასუხში მითთებულია, რომ EHR სისტემაში არსებული ლოგები ინახება 1 წლის განმავლობაში.

ამავე ბრძანების თანახმად, პაციენტს შეუძლია მისი გვერდიდან თვალი ადევნოს ლოგირების მონაცემებს და ამ გზით აკონტროლოს მისი პერსონალური მონაცემების დამუშავების/გამოყენების კანონიერება. აღნიშნული მიდგომა უდავოდ პროგრესული და მისასალმებელია, თუმცა **გაურკვეველია რით არის უზრუნველყოფილი ლოგების მთლიანობა (integrity) და რატომ უნდა ენდობოდეს მას პაციენტი.**

სამინისტროსაგან მიღებულ პასუხში ვკითხულობთ, რომ „მონაცემების მთლიანობის საკითხი და პოლიტიკები განსაზღვრულია შიდა სამსახურეობრივ დოკუმენტში, სადაც შეფასებულია შესაბამისი რისკები და მათი მინიმიზაციის ინსტრუმენტები. დოკუმენტი არ არის საჯარო“.[5]

თუ გავითვალისწინებთ, რომ სისტემის მფლობელია სამინისტრო, რომლიც მის მიერვე შექმნილი ტექნიკური/პროგრამული საშუალებებით ახორციელებს სისტემის წარმოებას, არ არსებობს მყარი გარანტია ლოგების ცვლილებებისა და ცალკეული მოქმედებების მომხმარებლებისაგან წაშლა/დაფარვის უზრუნველსაყოფად.

ამასთან, „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონი ადგენს მონაცემთა დამუშავების სამართლიანობის პრინციპს და მონაცემთა დამმუშავებლის ვალდებულებებს მონაცემთა სუბიექტის ინფორმირების თაობაზე. ყოველივე აღნიშნული გულისხმობს, რომ მონაცემთა დამუშავება მონაცემთა სუბიექტისათვის უნდა იყოს სამართლიანი, განჭვრეტადი, მას უნდა ჰქონდეს სათანადო ინფორმაცია მონაცემთა უსაფრთხოებისათვის მიღებული ზომების შესახებ. რა თქმა უნდა, მონაცემთა დამმუშავებლემა შეიძლება არ გაასაჯაროს სისტემის ტექნიკური დეტალები, კონკრეტული შემუშავებული ალგორითმები და ის კონკრეტული მექანიზმები, რომლითაც უზრუნველყოფს მონაცემთა უსაფრთხოებას, ლოგების მთლიანობას და ა.შ., თუმცა მონაცემთა სუბიექტის ინფორმირებისა და მონაცემთა სამართლიანი დამუშავების პრინციპის შესასრულებლად, მას ევალება გაასაჯაროს ინფორმაცია მიღებული ზომების შესახებ ზოგადად მაინც. მაგალითად, ახსნას ის პრინციპი, რომლის საშუალებითაც მიიღწევა ლოგების მთლიანობა (ასეთი შეიძლება იყოს ლოგების სერვერის ორგანიზაციის გარეთ გატანა და სხვ.) ხოლო თავად აღნიშნულის ფუნქციონირების კონკრეტული დეტალები მოაწესრიგოს არასაჯარო აქტით.

აუდიტი და მონიტორინგი

არ არის განსაზღვრული აუდიტისა და მონიტორინგის სათანადო მექანიზმები

სისტემის გამართული ფუნქციონირებისა და მონაცემთა უსაფრთხოების სათანადო დონის მისაღწევად, ისევე როგორც სისტემის შექმნისას დეკლარირებული უსაფრთხოებისა თუ კანონთან შესაბამისობის უზრუნველსაყოფად, აუცილებელია მონიტორინგის ადეკვატური მექანიზმის არსებობა.

განსახილველი სისტემისათვის მონიტორინგი მექანიზმი ორი მიმართულებით არის საინტერესო:

ა) როდესაც პაციენტს სურს საკუთარი ისტორიის სტატუსის ცვლილება, მასთან იგზავნება მოკლე ტექსტური შეტყობინება ერთჯერადი კოდით, რომლის გამოყენებითაც იცვლება ეპიზოდის სტატუსი. ექიმთან ვიზიტის დროს აღნიშნული ქმედების განხორციელება შესაძლებელია ინფორმირებული თანხმობის (პაციენტის მიერ ხელმოწერილი დოკუმენტი)

[5] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს 2020 წლის 13 ივლისის N01/7968 წერილი

საფუძველზე. ინსპექტორის გადაწყვეტილებაში ვკითხულობთ, რომ აღნიშნული დოკუმენტების შემოწმების მონიტორინგს ახორციელებს სამინისტრო.

ამავე გადაწყვეტილებაში არაფერია ნათქვამი აღნიშნული მონიტორინგის დეტალურ მექანიზმზე. ასეთი მექანიზმი არ არის ნახსენები სამინისტროს არცერთ წერილში. სავარაუდოა, რომ მონიტორინგის კონკრეტული, დეტალური მექანიზმი სამინისტროს არ აქვს დოკუმენტირებული, რამაც შეიძლება ხელი შეუწყოს მანკიერი პრაქტიკის დანერგვას და სამედიცინო დაწესებულებების მიერ გამოთხოვილი თანხმობები ან თანხმობის მიღების პროცედურა ვერ აკმაყოფილებდეს თანხმობის ნამდვილობის კანონისმიერ სტანდარტს.

ბ) ბრძანება ადგენს EMR[6]-ის მიმართ მოთხოვნებს EHR სისტემასთან ინტეგრაციისათვის, ბრძანების მე-12 მუხლის მე-2 პუნქტის თანახმად კი „სამინისტროს უფლება აქვს, გონივრული ეჭვის საფუძველზე, მოითხოვოს EMR სისტემის ამ მუხლში აღნიშნულ მოთხოვნებთან შესაბამისობის შემოწმება.“

სამინისტროსგან მიღებული პასუხის თანახმად მიმდინარე წლის ივნისის თვის მონაცემებით ასეთი აუდიტი არ ჩატარებულა.

გასათვალისწინებელია, რომ EHR სისტემის მომხმარებლები ხდებიან სამედიცინო დაწესებულებები, რომელთა ნაწილი დღემდე არასერიოზულად აღიქვამს პერსონალურ მონაცემთა დაცვის საკითხს და კანონმდებლობის მოთხოვნებთან მხოლოდ ზედაპირულ, ფორმალურ შესაბამისობას სჯერდება. მათ უმრავლესობას არ გააჩნია პეროსნალურ მონაცემთა დაცვისთვის საჭირო მექანიზმები - ორგანიზაციული პოლიტიკები, პროცედურები, ტექნოლოგიური გადაწყვეტები, სასწავლო პროგრამები და ა.შ. შესაბამისად, თანამშრომელთა შორის საკითხისადმი ცნობადობის დონეც დაბალია; ეს მდგომარეობა კიდევ უფრო ზრდის EHR სისტემიდან მომდინარე რისკებს რაც პერსონალური მონაცემების დაცვას უკავშირდება.

შესაბამისად, ძალიან მნიშვნელოვანია სისტემის/ების აუდიტის კონკრეტული და დეტალური მექანიზმების შემუშავება და დანერგვა.

<u>მონაცემთა უსაფრთხოება</u>

არ არის უზრუნველყოფილი მონაცემთა უსაფრთხოების სათანადო დონე

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის თანახმად მონაცემთა დამმუშავებელი ვალდებულია მიიღოს მონაცემთა უსაფრთოხებისათვის სათანადო ორგანიზაციული და ტექნიკური ზომები და აღნიშნული ზომები დამუშავებულ მონაცემებთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

[6] ელექტრონული სამედიცინო ჩანაწერების სისტემა, რომელიც ეკუთვნის სამედიცინო დაწესებულებას.

მონაცემთა უსაფრთხოებასთან დაკავშირებულ კითხვაზე სამინისტროსაგან მიღებული პასუხის თანახმად,[7] აღნიშნული საკითხი წესრიგდება კანონის შესაბამისად, ყველა მომხმარებელს გააჩნია საკუთარი მომხმარებლის სახელი და პაროლი, ასევე, სისტემაში შესასვლელად გამოიყენება ავტორიზაციის ორდონიანი მექანიზმი.

მიუხედავად იმისა, რომ სამინისტროს შემოწმების შესახებ ინსპექტორის შესაბამის გადაწყვეტილებაში[8] გამოთქმული რეკომენდაცია სისტემაში შესასვლელად ავტორიზაციის ორდონიანი მექანიზმის გამოყენების შესახებ სამინისტრომ სრულად გაითვალისწინა, აღნიშნული ვერ იქნება მიჩნეული უსაფრთხოების სათანადო დონის უზრუნველყოფად.. სისტემის მომხმარებლების სიმრავლის, შესაბამისი უნარების ნაკლებობისა და სისტემაში მონაცემთა შეყვანის სპეციფიკის გათვალისწინებით, ასევე, პრაქტიკულად ნანახ რამდენიმე თვალშისაცემ მაგალითზე დაყრდნობით, შეგვიძლია ვთქვათ, რომ გარდა თითოეული მომხმარებლისათვის განპიროვნებული მომხმარებლის სახლისა და პაროლის მინიჭებისა და ავტორიზაციის ორდონიანი მექანიზმის უზრუნველყოფისა, აუცილებელია, სამინისტრომ მიიღოს სათანადო ზომები რათა სისტემის მომხმარებლების მიერ მომხმარებლის სახლისა და პაროლის მესამე პირებისათვის გადაცემა იქნას მკაცრად გაკონტროლებული.

<u>მონაცემთა დამუშავების ზეგავლენის შეფასება</u>

EHR სისტემასთან მიმართებით არ არის ჩატარებული მონაცემთა დამუშავების ზეგავლენის შეფასება

მიუხედავად იმისა, რომ მოქმედი კანონმდებლობა (განსხვავებით საქართველოს პარლამენტში განხილვის ეტაპზე მყოფი პროექტისა) პირდაპირ არ ადგენს მონაცემთა დამუშავების ზეგავლენის შეფასების ვალდებულებას, EHR სისტემის თავისებურების, საუკეთესო ევროპული პრაქტიკისა და საქართველოს ევროპული ინტეგრაციის (მათ შორის ევროპოლთან თანამშრომლობისა და ასოცირების შეთანხმების) გათვალისწინებით მიზანშეწონილია მონაცემთა უსაფრთხოებისთვის და ლეგიტიმური დამუშავებისთვის დამატებითი ზომების მიღება.

„პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონის მე-17 მუხლის თანახმად, მონაცემთა დამმუშავებელი ვალდებულია მიიღოს მონაცემთა უსაფრთხოებისათვის შესაბამისი ორგანიზაციული და ტექნიკური ზომები და ეს ზომები მონაცემთა დამუშავებასთან დაკავშირებული რისკების ადეკვატური უნდა იყოს.

პერსონალურ მონაცემთა დამუშავების ზეგავლენის ანალიზი კი ევროპულ კანონმდებლობით კარგად დანერგილი და ფართოდ გავრცელებული პრაქტიკაა და მნიშვნელოვანია იმდენად, რამდენადაც მონაცემთა დამმუშავებელს აძლევს საშუალებას სისტემურად და

---

[7] საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის სამინისტროს 2020 წლის 4 ივნისის N01/5923 წერილი

[8] სახელმწიფო ინსპექტორის სამსახურის 2020 წლის 7 თებერვლის გადაწყვეტილება Nგ-1/055/2020 „საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობის და სოციალური დაცვის სამინისტროს შემოწმების დასრულების შესახებ“

სიღრმისეულად გაიაზროს მონაცემთა დამუშავების პროცესი, შეაფასოს და გამოავლინოს კანონმდებლობის მოთხოვნებთან შესაბამისობის საკითხი, მონაცემთა სუბიექტის უფლებების რეალიზების შესაძლებლობები, წინასწარ დეტალურად შეაფასოს მოსალოდნელი რისკები და დროულად მიიღოს სათანადო ორგანიზაციული თუ ტექნიკური ზომები.

სამინისტროს ცნობით, განხორციელდა სისტემასთან დაკავშირებული რისკების შეფასების პროცესი და შედეგად სისტემაში დაინერგა რიგი ტექნოლოგიური გადაწყვეტილებები, თუმცა „ეს ყველაფერი არ არის ფორმალიზებული დოკუმენტის დონეზე, რადგან სადღეისოდ სამინისტროს არ ჰყავს ინფორმაციული უსაფრთხოების მენეჯერი“.

მსგავსი მიდგომა ვერ ჩაითვლება გატარებულ რეალურ ზომად და კანონთან თუ კარგ პრაქტიკასთან შესაბამის ღონისძიებად, რადგან შეუძლებელია მონაცემთა დამმუშავებელმა სისტემურად და სიღრმისეულად შეაფასოს მონაცემთა დამუშავების პროცესი, დეტალურად შეაფასოს მოსალოდნელი რისკები და მათი აღრიცხვისა და დოკუმენტირების გარეშე შექმნას მათზე რეაგირების ადეკვატური მექანიზმები, რადგანაც მონაცემთა დაცვა, მათი უსაფრთხოება და არსებულ რისკებზე რეაგირების მექანიზმები - ორგანიზაციულ-ტექნიკური ზომები არ შეიძლება იყოს ერთჯერადი და იმისთვის რომ ისინი იყოს ქმედითი, ეს აუცილებლად განგრძნობით პროცესს გულისხმობს.

შესაბამისად, მსგავსი მოცულობის და მნიშვნელობის სისტემის შექმნის, დანერგვისა და გაშვების დროს, მნიშვნელოვანია წინასწარ იქნას მოძიებული და გამოყოფილი ადეკვატური ფინანსური თუ ადამიანური რესურსი.

<u>ტრენინგები</u>

სისტემის მომხმარებლებს არ გაუვლიათ სპეციალიზებული ტრენინგები

სისტემის განსაკუთრებული სენსიტიური ხასიათიდან და სისტემის მომხმარებელთა სიმრავლიდან გამომდინარე, მნიშვნელოვანია მისმა მომხმარებლებმა კარგად გააცნობიერონ პერსონალურ მონაცემთა დაცვის მნიშვნელობა, მონაცემთა დამუშავების პრინციპები, საკუთარი უფლება-მოვალეობები და მონაცემთა დაცვასთან დაკავშირებული სხვა საკითხები.

სამინისტროსგან მიღებული პასუხის თანახმად 2018 წლიდან 2020 წლის ივნისამდე ექიმებისა და კლინიკის წარმომადგენლებისთვის (დაახლოებით 2000-მდე) ჩატარდა ტრენინგები ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების სისტემის EHR ფუნქციონირების შესახებ, რომლის დროსაც **ასევე** ყურადღება გამახვილებული იქნა პერსონალური მონაცემების დაცვის გადაწყვეტილებებზე არა მარტო აღნიშნული სისტემის ფარგლებში, არამედ ზოგადად ექიმებისა და მენეჯმენტის მხრიდან პაციენტის ნების გამომხატველი დოკუმენტების სწორად გაფორმების საკითხში, პაციენტის ინფორმირებულობის ვალდებულების შესახებ. ტრენინგს ატარებდნენ ინფორმაციული ტექნოლოგიებისა და ანალიტიკის, ასევე, პოლიტიკის დეპარტამენტის თანამშრომლები.

ის, რასაც სამინისტრო მიიჩნევს პერსონალურ მონაცემთა დაცვის საკითხებზე ჩატარებულ ტრენინგად, არც მითითებული/დაფარული საკითხების კუთხით და არც მითითებული

ტრენერების გათვალისწინებით არ შეიძლება მიჩნეული იქნას სისტემის მომხმარებლების რეალურ გადამზადებად და მონაცემთა დაცვის ძირეულ საკითხებზე მათ სრულყოფილ დატრენინგებას.

4.4 ძირითადი მიგნებები[9]

დასკვნის სახით შეიძლება ითქვას, რომ **სამინისტროს, როგორც სისტემის მფლობელს არ აქვს მონაცემთა დაცვის საკითხის მნიშვნელობის სათანადო აღქმა და საკითხის მოწესრიგების მზაობა.** ამას მოწმობს სამინისტროს მიერ გამოთქმული მოსაზრება იმის თაობაზე, რომ მონაცემთა დაცვასთან დაკავშირებული საკითხების მართვის სისტემა სამინსიტროში ფინანსური რესურსების სიმცირის გამო არ არის დანერგილი. ასევე, სამინისტრო მოწერილ პასუხებში აპელირებს კონკრეტული სამედიცინო დაწესებულებების პასხუსიმგებლობაზე მონაცემთა დაცვის საკითხებთან დაკავშირებით, თუმცა იმდენად, რამდენადაც სისტემის მფლობელი არის თავად სამინისტრო, ის არის ვალდებული გაატაროს სათანადო ზომები და უზრუნველყოს მის სისტემაში დამუშავებული მონაცემების უსაფრთხოება.

EHR სისტემასთან დაკავშირებული აქტებისა და ხელმისაწვდომი ინფორმაციის ანალიზის საფუძველზე შეგვიძლია გამოვყოთ შემდეგი ძირითადი მიგნებები:

- **არ ვიცით** რა მონაცემებზე აქვს წვდომა სისტემაში სამინისტროს თანამშრომლებსა და 3 საჯარო უწყებას
- **სისტემა არის გაუმჭვირვალე** სისტემა - პაციენტმა არ იცის თუ ვის რა მონაცემებზე მიუწვდება ხელი და რატომ
- **დარღვეულია** მონაცემთა თავისთავადი დაცულობის პრინციპი - მონაცემები/ეპიზოდები ავტომატურად არის ხილვადი და ხელმისაწვდომი, თუ პაციენტი აქტიური ქმედებით არ შეუცვლის ეპიზოდს სტატუსს
- **არ არის რეგლამენტირებული** მონაცემებზე წვდომის საკითხი და მისი ფარგლები
- **არ ვიცით რა ფორმით არის უზრუნველყოფილი** ლოგების მთლიანობა
- **არ არის გათვალისწინებული** აუდიტისა და მონიტორინგის სათანადო მექანიზმები
- **არ არის უზრუნველყოფილი** მონაცემთა უსაფრთხოების სათანადო დონე
- **არ არის შეფასებული** სისტემაში მონაცემთა დამუშავების ზეგავლენა და რისკები
- სისტემის მომხმარებლებს **არ გაუვლიათ** სპეციალიზებული ტრენინგი და გადამზადება პერსონალურ მონაცემთა დაცვის თვალსაზრისით

[9] EHR სისტემასთან და შემუშავებულ ანგარიშთან დაკავშირებით 2020 წლის 21 აგვისტოს IRC-მ ღია დისკუსია გამართა, რომელშიც ასევე სამინისტროს წარმომადგენლებიც მონაწილეობდნენ. დისკუსიის ფარგლებში სამინისტროს წარმომადგენლები არ დაეთახმნენ IRC-ს პოზიციას რამდენიმე საკითხთან დაკავშირებით, რადგანაც, მათი განცხადებით, ანგარიშში პრობლემად იდენტიფიცირებული რიგი საკითხები სამინისტროს ახლებურად ჰქონდა რეგლამენტირებული ან გეგმავდა ცვლილებებს. შეთანხმების მიუხედავად აღნიშნულის დამადასტურებელი წერილობითი მტკიცებულება IRC-ს არ მიუღია, შესაბამისად, ანგარიში ეყრდნობა ხელმისაწვდომ წყაროებს