ინოვაციებისა და რეფორმების ცენტრი
INNOVATIONS AND REFORMS CENTER

ელექტრონული ჯანდაცვის სისტემა

EHR

დოკუმენტი მომზადდა პროექტის "მონაცემთა სუბიექტებისა და სხვა აქტორების გაძლიერება პირადი ცხოვრების ხელშეუხებლობის უფლების რეალიზაციისთვის" ფარგლებში, ნიდერლანდების საელჩოს მხარდაჭერით. დოკუმენტში მოცემული მოსაზრებები წარმოადგენს მხოლოდ ინოვაციებისა და რეფორმების ცენტრის პოზიციას და ის შეიძლება არ ასახავდეს ნიდერლანდების საელჩოს შეხედულებებს.

საქართველო, თბილისი, 0160, ს. ცინცაძის ქ. #12 ტელ: (+995 32) 255 2001/02
12 S. Tsintsadze Str. 0160 Tbilisi, Georgia Tel: (+995 32) 2552001/02
www.irc.ge E-mail: info@irc.ge

ინოვაციებისა და რეფორმების ცენტრი
INNOVATIONS AND REFORMS CENTER

2019 წლის 15 იანვარს ამოქმედდა საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის ბრძანება №01-1/ნ, რომლის თანახმადაც იქმნება „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 მფლობელი იქნება სამინისტრო. ანუ, თუ ტრადიციულად, ჯანმრთელობასთან (ავადობასა და მკურნალობასთან) დაკავშირებული დოკუმენტაცია ხელმისაწვდომი იყო ფრაგმენტულად, მხოლოდ ცალკეული სამედიცინო დაწესებულებისა და პერსონალისთვის, ახალი სისტემის ამოქმედების შემდეგ მთელი სამედიცინო ისტორია - ადამიანის ცხოვრების მანძილზე არსებული ავადობისა თუ მკურნალობის ყველა ეპიზოდი თავმოყრილი იქნება ერთიან, ცენტრალიზებულ მონაცემთა ბაზაში.

ბრძანებით დადგენილი მოთხოვნები 2019 წლის განმავლობაში ეტაპობრივად შედის ძალაში სხვადასხვა სამედიცინო დაწესებულებების მიმართ და წლის ბოლოსთვის სრულად ამოქმედდება, კერძოდ:

> *„2020 წლის 1 იანვრიდან ყველა სტაციონარული და ამბულატორიული სამედიცინო დაწესებულება (გარდა ამბულატორიულად/დღის სტაციონარის პირობებში განსახორციელებელი, მაღალი რისკის შემცველი დერმატოკოსმეტოლოგიური სამედიცინო საქმიანობის/მომსახურების მიმწოდებლებისა) ვალდებულია, ყველა იდენტიფიცირებული პაციენტის ჯანმრთელობის მდგომარეობის შესახებ ინფორმაცია გადასცეს ჯანმრთელობის შესახებ ელექტრონული ჩანაწერების (EHR) სისტემაში . . .“*

ბრძანებაში ვკითხულობთ, რომ EHR სისტემის მიზანია

საქართველო, თბილისი, 0160, ს. ცინცაძის ქ. #12 ტელ: (+995 32) 255 2001/02
12 S. Tsintsadze Str. 0160 Tbilisi, Georgia Tel: (+995 32) 2552001/02
www.irc.ge E-mail: info@irc.ge

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

EHR სისტემა, მთელ მსოფლიოში, მთავრობების მიერ მართლაც განიხილება როგორც კარგი საშუალება იმისათვის რომ:

- პაციენტს გაეწიოს უკეთესი სამედიცინო მომსახურება, ვინაიდან მის შესახებ ხელმისაწვდომი ხდება უფრო მეტი და ხარისხიანი ინფორმაცია;
- სამედიცინო მომსახურების სფეროში გაიზარდოს ხარჯეფექტურობა და მოხდეს შესაბამისი ბიუჯეტების დეფიციტის ზრდის პრევენცია;
- არსებობდეს საჭირო მონაცემები სამედიცინო მომსახურების სფეროში ხარისხის კონტროლისთვის, სრულყოფილი სტატისტიკისა და ჯანდაცვის სექტორში სწორი დაგეგმვისთვის.

ჩვენ, რა თქმა უნდა, ვიზიარებთ აღნიშნულ მიდგომას, რომ EHR სისტემას აქვს მეტი პოტენციალი ხარისხიანი სამედიცინო ინფორმაციის შესაგროვებლად, ვიდრე სამედიცინო დოკუმენტაციის წარმოების ტრადიციულ ფორმებს და გვჯერა, რომ მას პოზიტიურ გავლენის მოხდენა შეუძლია როგორც სამედიცინო მომსახურების ხარისხზე, ისე მთლიანად სექტორის ეფექტიანობაზე. თუმცა, ამავე დროს, ხაზი უნდა გაესვას იმ გარემობას რომ **EHR სისტემა განაპირობებს პაციენტის შესახებ დიდი მოცულობის, განსაკუთრებული კატეგორიის მონაცემების მაღალ ხელმისაწვდომობას პირთა ფართო წრისთვის.** (27 000-ზე მეტი ექიმი, სამედიცინო დაწესებულებები და მინიმუმ 4 საჯარო დაწესებულება - სამინისტრო და მისი მმართველობის სფეროში მოქმედი სამი სსიპ-ი).

შესაბამისად, პერსონალურ მონაცემთა დაცვის თვალსაზრისით, EHR სისტემის შექმნა წარმოშობს დამატებით და თვისობრივად განსხვავებულ რისკებს, რამდენადაც ის არსებითად ცვლის/ზრდის პაციენტის შესახებ სამედიცინო ინფორმაციის შესაძლო არასწორი გამოყენების მასშტაბებს.

აქვე უნდა აღინიშნოს, რომ EHR სისტემა და პაციენტების შესახებ მასში შეტანილი მონაცემები საკმაოდ საინტერესო/მიმზიდველი შეიძლება იყოს ისეთი სუბიექტებისთვის როგორიცაა სადაზღვევო კომპანიები, სამართალდამცავი ორგანოები და სხვები, რაც ასევე ზრდის მონაცემთა არასწორი, უკანონო დამუშავების რისკებს.

ამდენად, ერთმნიშვნელოვნად უნდა ითქვას, რომ 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 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, მსგავს EHR სისტემების შექმნისას განსაკუთრებული ყურადღებით ეკიდებიან პერსონალურ მონაცემთა დაცვის საკითხს და შეიძლება ითქვას რომ სისტემის შექმნის დროს, მის ეფექტურობასა და ტექნიკურ გამართულობასთან ერთად, თანაბარმნიშვნელოვან საზრუნავად მიიჩნევენ პერსონალურ მონაცემთა დაცვას. შესაბამისად, ამ პრიზმაში ხდება სისტემის ყველა კონცეპტუალრი, სამართლებრივ-პროცედურული და ტექნოლოგიური საკითხის განხილვა/გადაწყვეტა.

მაგალითად ***ავსტრიის რესპუბლიკაში*** EHR-ის მსგავსი სისტემის - ELGA-ს მოქმედებისთვის მონაცემთა დაცვის ძალიან მკაცრი და დეტალური წესებია გაწერილი, რაც კარგი პრაქტიკის მაგალითად ითვლება. აქვე გასათვალისწინებელია ავსტრიის რესპუბლიკის სპეციფიკა, სადაც არ არსებობს მოქალაქის პირადი ნომერი და თითოეული სექტორის მიხედვით (მაგ. ჯანდაცვის სექტორი, საფინანსო სექტორი და ა.შ.) მოქალაქეს ენიჭება დამოუკიდებელი 'სექტორული ნომერი', რომელიც არ არის დაკავშირებადი მის სხვა მონაცემებთან. ასევე, ავსტრიის კანონმდებლობის თანახმად, პაციენტს უფლება აქვს უარი თქვას (opt-out) სისტემაში მონაწილეობაზე სრულად ან ნაწილობრივ.

ესტონეთშიც გარანტირებულია პაციენტის უფლება უარი თქვას ჯანდაცვის ელექტორნულ სისტემაში მონაწილეობაზე.

ნიდერლანდების შემთხვევაში კი EHR სისტემების დანერგვამდე მრავალი გზამკვლევი თუ ეთიკის სახელმძღვანელო იქნა მიღებული, რომელთა მეშვეობითაც ხდება სისტემაზე ზედამხედველობა და რომელიც შეიცავს სპეციფიკურ და ტექნიკურ მოთხოვნებს სისტემაში ავტორიზაციის წესებთან, მონაცემთა უსაფრთოხოებასა და ლოგირებასთან და ა.შ. დაკავშირებით.

ჩამოთვლილ და ევროპის სხვა ქვეყნებს ის საერთო მახასიათებელიც აერთიანებთ, რომ თითოეულ ქვეყანაში სისტემის დანერგვა-ამოქმედებამდე რამდენიმე წლის მანძილზე

მიმდინარეობდა საკითხის დეტალური კვლევა და ფართო საზოგადოებრივი დისკუსია, მათ შორის მონაცემთა დაცვისა და ინფორმაციული უსაფრთხოების სპეციალისტების ჩართულობით. რაც, ერთი მხრივ, დაცულობის გაცილებით მაღალი ხარისხის გარანტიაა, ხოლო, მეორე მხრივ, ზრდის საზოგადოების ნდობას ამ და მსგავსი სისტემების მიმართ.

საერთაშორისო პრაქტიკის შესაბამისად, მსგავსი სისტემების შექმნამდე რეკომენდებულია მთელი რიგი ღონისძიებების გატარება, მათ შორის:

- პერსონალურ მონაცემთა დაცვაზე გავლენის შეფასება (DPIA), რისკების იდენტიფიცირება და შესაბამისი კონტროლის ღონისძიებების განსაზღვრა;
- EHR სისტემასთან დაკავშირებული, მონაცემთა დამუშავების საშუალებებისა და პროცესების ზუსტი იდენტიფიცირება, აღრიცხვა და დოკუმენტირება;
- „მონაცემთა დამუშავების მინიმიზაციისა“ და სხვა პრინციპის დაცვის მიზნით, EHR სისტემასთან დაკავშირებულ თანამშრომელთა ფუნქციებისა და სამუშაო აღწერილობების ანალიზი მონაცემთა დაცვის ჭრილში, რათა დადგინდეს მათთვის საჭირო ინფორმაციის მინიმალური მოცულობა და შესაბამის წვდომის დონეები;
- პოლიტიკებისა და პროცედურების შემუშავება, რომლებმაც უნდა უზრუნველყოს მონაცემებზე სხვადასხვა ფუნქციის მქონე თანამშრომელთა დაშვების შესახებ გადაწყვეტილებების რაციონალური და არაერთპიროვნული მიღება;
- ორგანიზაციაში პერსონლაურ მონაცემთა მართვის სისტემის შექმნა, რაც გულისხმობს როლებისა და პასუხისმგებლობების განსაზღვრას და შესაბამისი პროცედურული ინსტრუმენტებით უზრუნველყოფას;
- მონაცემთა უკანონო დამუშავებისთვის არსებული პასუხისმგებლობის ზომების საკმარისობის შეფასება და საჭიროების შემთხვევაში შესაბამისი სამართლებრივი ცვლილებების ინიცირება;
- თანამშრომელთა შორის ცნობიერების ამაღლება პერსონალურ მონაცემა დაცვის თაობაზე, შესაბამისი ტრენინგების მიწოდება;
- პერსონალურ მონაცემთა დაცვის მდგომარეობის პერიოდული აუდიტის საჭიროების განხლივა და შესაბამისი წესების დადგენა.

ამ თვალსაზრისით მიგვაჩნია, რომ საქართველოს ოკუპირებული ტერიტორიებიდან დევნილთა, შრომის, ჯანმრთელობისა და სოციალური დაცვის მინისტრის ბრძანების შესაბამისად შექნილი EHR სისტემა და ზოგადად სამინისტრო, დღეისათვის შორსაა იმ

კონდიციისგან, რომლითაც შეუძლია პერსონალურ მონაცემთა დაცვის არსებულ რისკებთან გამკლავება და სისტემის მიმართ მოქალაქეთა ნდობის დამსახურება.

მიგვაჩნია, რომ არსებობს კონცეპტუალური და სამართებლრივი სისუსტეები, როგორც EHR სისტემაში პერსონალურ მონაცემთა დაცვისკენ მიმართული გადაწყვეტების შერჩევის, ასევე გასატარებელი ორგანიზაციული ღონისძიებების თვალსაზრისით.

ქვემოთ განხილულია რამოდენიმე, ჩვენი აზრით პრობლემური საკითხი, რომელთა შესახებ მსჯელობა შესაძლებელი გახდა ბრძანების ტექსტსა და სხვა საჯაროდ ხელმისაწვდომ ინფორმაციაზე დაყრდნობით[1].

EHR სისტემაში დამუშავებული მონაცემების ღიაობა თუ პაციენტმა არ განახორციელა აქტიური მოქმედებები მათ დასაფარად

ბრძანების მე-3 მუხლის თანახმად EHR სისტემის ნაწილია ე.წ. ექიმის გვერდი რომელშიც ექიმს

> *„შეაქვს მონაცემები პაციენტის ჰოსპიტალიზაციის თითოეული ეპიზოდის/თითოეული ამბულატორიული ვიზიტის შესახებ . .“*

ამავე ბრძანების მე-4 მუხლის თანახმად სამედიცინო დაწესებულება/ექიმი ვალდებულია:

> *ა) ამბულატორიული ვიზიტის შესახებ ინფორმაცია EHR სისტემაში გადასცეს ამბულატორიული ვიზიტის დასრულებიდან 1 სამუშაო დღის ვადაში;*
>
> *ბ) სტაციონარული შემთხვევების შესახებ ინფორმაცია EHR სისტემაში გადასცეს პაციენტის გაწერიდან 5 სამუშაო დღის ვადაში.*

[1] EHR სისტემისა და პერსონალურ მონაცემთა დაცვისკენ მიმართული ღონისძიებების/დოკუმენტების შესახებ, სამინისტროდან გამოთხოვილი იქნა საჯარო ინფორმაცია 2019 წლის 18 იანვარს. ასევე, სამინისტროს ეთხოვა მათი მხრიდან ამ თემაში გარკვეულ სპეციალისტებთან შეხვედრის ორგანიზება, ცალკეულ ბუნდოვან საკითხებზე სამსჯელოდ. 28 იანვრის მდგომარეობით ჩვენს წერილზე არანაირი პასუხი/რეაგირება არ მიგვიღია.

ექიმის მიერ სისტემაში შეტანილი მონაცემები ხელმისაწვდომი ხდება სისტემის ავტორიზებული მომხმარებელებისთვის (ჩვენი ინფორმაციით 27 ათასი ექიმი), თუ თავად პაციენტმა არ მოისურვა მონაცემთა დაფარვა. ანუ სისტემაში შეტანილი მონაცემები თავისთავად ღიაა სისტემის მომხმარებლებისათვის, მანამ სანამ პაცინეტი 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 ხდება პაციენტის გაწერიდან 5 სამუშაო 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 წარმოაიშვას დავა თუ კონკრეტულად რა მოთხოვნით გადასცა კოდი პაციენტმა და შეესაბამება თუ არა ექიმის მოქმედება (მონაცემთა დაფარვის დონე) 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.

აღნიშნულთან დაკავშირებით შეიძლება არსებობდეს არგუმენტი, რომ დაფარვის გარეშე არსებული - ხილული მონაცემები მაინც არ იქნება თავისუფლად ხელმისაწვდომი სისტემის მომხმარებლებისთვის, ვინაიდან ექიმს შეუძლია მხოლოდ იმ შემთხვევაში ჰქონდეს წვდომა კონკრეტული პაციენტის მონაცემებზე, თუ ის მოახდენს პაციენტის იდენტიფიცირებას პირადი ნომრითა და დაბადების თარიღით, რასაც ვერ განახორციელებს პაციენტის ნების გარეშე. სამწუხაროდ, აღნიშნული არგუმენტი ქართული კონტექსტის გათვალისწინებით საფუძველს მოკლებულია, ვინაიდან პირადი ნომრისა და დაბადების თარიღის მოძიება პაციენტთა დიდი ნაწილის შემთხვევაში სხვადასხვა გზებით ადვილად არის შესაძლებელი.

<u>ინფორმაციის დამუშავების ლოგირება</u>

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 ბრძანების თანახმად, პაციენტს შეუძლია მისი გვედრიდად თვალი ადევნის 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.** თუ გავითვალისწინებთ, რომ სისტემის მფლობელია სამინისტრო, რომლიც მის მიერვე შექმნილი ტექნიკური/პროგრამული საშუალებებით ახორციელებს სისტემის წარმოებას, რა იცავს მომხმარებელს იმისგან რომ „საჭიროების შემთხვევაში“ არ მოხდება ლოგების ცვლილება, ცალკეული მოქმედებების წაშლა/დაფარვა მომხმარებლისთვის?

EHR სისტემის სავადებული ხასიათი და პაციენტის უფლება დაფაროს მონაცემები

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?

ვფიქრობთ რომ ამ და სხვა მსგავს საკითხებს დაზუსუტება სჭირდება ბრძანების ტექსტში.

მონაცემთა დამუშავების საფუძვლები - რა საფუძვლით აქვთ წვდომა სამინისტროს სახელმწიფო კონტროლს დაქვემდებარებული სსიპ-ებს EHR სისტემაზე

ბრძანების მე-3 მუხლის თანახმად EHR სისტემის მფლობელია სამინისტრო, ხოლო მისი მომხმარებლები 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.

ამავე 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.“

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

აქვე ისიც უნდა აღინიშნოს, რომ ბრძანების ტექსტიდან 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 მონაცეემებზე თუ სისტემის ანალიტიკური გვერდის საშუალებით მონაცემთა დამუშავება გულისხმობს, მათ შორის, კონკრეტულ პაციენტთა პერსონალურ/სამედეიცინო მონაცემებზე წვდომასაც? ან თუ ეს წვდომები დეპერსონიფიცირებულია, რითია უზრუნველყოფილი აღნიშნული?

პერსონალურ მონაცემთა დაცვის პროგრამა (privacy management framework/ data protection program)

ჩვენს ხელთ არსებული ინფორმაციით სამინისტროს, ისევე როგორც EHR სისტემის მომხმარებელ საჯარო დაწესებულებებს (სამინისტროს სსიპ-ებს), დღეისათვის არ გააჩნიათ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხების მართვის სისტემა (privacy management framework/data protection program) შესაბამისი როლებით, პერსონალურ მონაცემთა დაცვის სფეროში საკმარისი კომპეტენციის მქონე პასუხისმგებელი პირებით და შესაბამისი პოლიტიკებით/პროცედურებით. ამდენად, პრინციპულად გაუმართლებლად მიგვაჩნია, რომ EHR სისტემის შექმნასა და ფუნქციონირებაზე პასუხსიმგებელი იყოს დაწესებულება, რომელსაც პერსონალურ მონაცემთა დაცვის მაღალი სტანდარტი არ აქვს დამკვიდრებული.

მონაცემთა დაცვისა და უსაფრთხოებისკენ მიმართული წესებისა და პროცედურების შესრულება - აუდიტის საჭიროება

ბრძანების მე-3 მუხლის ადგენს რომ

> *„EHR სისტემის მომხმარებელთა უფლებამოსილება შეზღუდულია კანონმდებლობით დადგენილი მიზნით და ფარგლებით. . . ინფორმაციის უსაფრთხოების მიზნებისათვის, სამინისტრო ადგენს პაციენტის, სამედიცინო დაწესებულების, პაციენტის ინფორმაციის დამუშავებაში ჩართული მხარეების სისტემასთან წვდომისათვის საჭირო აუთენტიფიკაციისა და ავტორიზაციის წესებს.“* ხოლო მე-17 მუხლის თანახმად - *„EHR სისტემაში არსებული პერსონალური მონაცემების უსაფრთხოების საკითხები წესრიგდება ,,პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონისა და ,,ინფორმაციული უსაფრთხოების შესახებ“ საქართველოს კანონის შესაბამისად.“*

ბუდოვანია, თუ როგორ აპირებს სამინისტრო შეამოწმოს მუშაობს/სრულდება თუ არა პრაქტიკაში ზემოაღნიშნული და პერსონალურ მონაცემთა დაცვის მიზნებისთვის მნიშვნელოვანი სხვა წესები და პროცედურები. არც ბრძანებაში და არც სხვა ჩვენთვის ხელმისაწვდომ საჯარო დოკუმენტებში არაფერია ნახსენები პერსონალურ მონაცემთა დაცვის შიდა ან/და გარე აუდიტის ჩატარების მიზანშეწონილობასა თუ სავალდებულოობაზე.

EMR -ის მიმართ წაყენებული მოთხოვნების მონიტორინგი/პერსონალურ მონაცემთა დაცვის მდგომარეობა სამედიცინო დაწესებულებებში

ბრძანება ადგენს EMR[2]-ის მიმართ მოთხოვნებს EHR სისტემასთან ინტეგრაციისათვის, კერძოდ ბრძანების მე-12 მუხლის პირველ პუნქტში აღნიშნულია:

> *„იმ შემთხვევაში, თუ სამედიცინო დაწესებულება EHR სისტემასთან წვდომას ახორციელებს მისი ლოკალური EMR სისტემის გამოყენებით, აუცილებელია მისი EMR სისტემა აკმაყოფილებდეს შემდეგ მოთხოვნებს:*

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

ა) EMR სისტემაზე წვდომა ხორციელდება მხოლოდ ავტორიზებული პირების მიერ. ავტორიზებული პირი შეიძლება იყოს ექიმი;

გ) EMR სისტემაზე ყოველი წვდომისას აუცილებელია, EMR სისტემა ითხოვდეს ავტორიზაციის გავლას;

გ) სამედიცინო დაწესებულება ვალდებულია, შეინახოს მისი შიდა საინფორმაციო სისტემის მომხმარებელთა რეგისტრი, მათ მიერ შექმნილი ჩანაწერები და წვდომის უფლებები ამ დანართით დადგენილი ვადებით; . . . “

ამავე მუხლის მე-2 პუნქტის თანახმად კი

„სამინისტროს უფლება აქვს, გონივრული ეჭვის საფუძველზე, მოითხოვოს EMR სისტემის ამ მუხლში აღნიშნულ მოთხოვნებთან შესაბამისობის შემოწმება.“

ეს ნიშნავს, რომ სამინისტრო პრაქტიკაში, როგორც წესი, არ განახორციელებს EMR სისტემის, ბრძანების მოთხოვნებთან შესაბამისობის შემოწმებას და ამ უფლებას იტოვებს მხოლოდ „გონივრული ეჭვის“ არსებობის მომენტისთვის, რაც ვფიქრობთ ზედმეტად „ოპტიმისტური“ დამოკიდებულებაა, თუ მხედველობაში მივიღებთ ცალკეული სამედიცინო დაწესებულებების მხრიდან მსგავსი საკითხებისადმი ზედაპირულ/ინდეფერენტულ და უპასუხისმგებლო დამოკიდებულებას, რაც არაერთხელ გამოვლენილა პაციენტის შესახებ ინფორმაციის გამჟღავნებაში.

აქვე უნდა აღინიშნოს, რომ EHR სისტემის მომხმარებლები ხდებიან სამედიცინო დაწესებულებები, რომლეთა 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 ცნობიერების დონეც დაბალია; ეს მდგომარეობა კიდევ უფრო ზრდის EHR სისტემიდან მომდინარე რისკებს რაც პერსონალური მონაცემების დაცვას უკავშირდება.

პასუხისმგებლობის ზომები მონაცემთა დამუშავების წესების დარღვევისთვის და მონაცემთა სუბიექტისთვის მიყენებული ზიანის ანაზღაურება

მსგავსი სისტემების დანერგვამდე მიზანშეწონილია ჩატარდეს სამართლებრივი ანალიზი და შეფასდეს, თუ რამდენად პროპორციულია მონაცემთა დამუშავების წესების დარღვევისთვის დადგენილი პასუხისმგებლობის ზომები, მიყენებული ზიანის ანაზღაურების მექანიზმები და რამდენად ეფექტურად შეიძლება ისინი ჩაითვალოს. საჭიროების შემთხვევაში კი უნდა განხორციელდეს შესაბამისი სამართლებრივი ცვლილებები, რომელიც დაადგენს პასუხისმგებლობის ადეკვატურ ზომებს, უშუალოდ მსგავსი სისტემის უსაფრთხოების მიზნებისთვის.

რამდენადაც ჩვენვის ცნობილია, მსგავსი ანალიზი/შეფასება არ ჩატარებულა და შესაბამისი დასკვნები არ მომზადებულა. ამდენად ბუნდოვანია თუ რა პასუხისმგებლობის ზომებს ითვალისწინებს საქართველოს კანონმდებლობა, EHR სისტემაში შეტანილი პერსონალური მონაცემების უკანონო დამუშავების შემთხვევებისთვის, გარდა პერსონალურ მონაცემთა დაცვის შესახებ საქართველოს კანონით გათვალისწინებული სრულიად არაადეკვატური და არაეფექტური ჯარიმებისა.

ყოველივე ზემოაღნიშნულის გათვალისწინებით, მიგვაჩნია რომ დღეისათვის არც სამინისტრო და არც სამედიცინო დაწესებულებები მზად არ არიან EHR სისტემის სრულყოფილად ასამოქმედებლად და პერსონალურ მონაცემთა დაცვასთან დაკავშირებულ რისკებთან გასამკლავებლად. პაციენტების პერსონალურ მონაცემთა დამუშავებასთან დაკავშირებულმა ინციდენტებმა და მოსალოდნელმა დარღვევებმა, შესაძლოა გამოიწვიოს სისტემის მიმართ უნდობლობა და მისი სრული დისკრედიტაცია.

აქვე შეგახსენებთ, რომ პერსონალურ მონაცემთა დაცვასთან დაკავშირებული საკითხები ასევე მნიშვნელოვანია საქართველოს ევროინტეგრაციის კონტექსტში - ევროკავშირთან ვიზების ლიბერალიზაციის სამოქმედო გეგმაში ცალკე მოთხოვნას წარმოადგენდა როგორც შესაბამისი კანონის არსებობა, ასევე მისი სწორი იმპლემენტაცია. ხოლო ევროკავშირთან „ასოცირების შესახებ შეთანხმება“ ადგენს ვალდებულებას, რომ

„თითოეული მხარე, წინამდებარე ან სხვა შეთანხმებების იმპლემენტაციის კონტექსტში, უზრუნველყოფს მონაცემთა დაცვის სამართლებრივ დონეს, რომელიც მინიმუმ შეესაბამება [ევროკავშირის სტანდარტებს]“

ასევე საგულისხმოა გასულ წელს ამოქმედებული ევროკავშირის მონაცემთა დაცვის ზოგადი რეგულაცია - GDPR, რომელიც სხვა მრავალ თავისებურებასთან ერთად ექსტრატერიტორიულობის პრინციპით გამოირჩევა, რაც ნიშნავს, რომ მისი მოქმედება ვრცელდება იმ კომპანიებზეც, რომლებიც არ არიან დაფუძნებული ევროკავშირის ტერიტორიაზე, მაგრამ საკუთარ სერვისს სთავაზობენ ევროკავშირის ტერიტორიაზე მყოფ პირებს. როგორც ჩვენთვის ცნობილია, სამედიცინო მომსახურების სფეროში მომუშავე ცალკეული ქართული კომპანიები განიხილავენ შესაძლებლობას საკუთარ მომსახურება შესთავაზონ ცენტრალური თუ აღმოსავლეთ ევროპის ქვეყნებს/მოსახელობას, რაც გამოიწვევს მათზე აღნიშნული რეგულაციის გავრცელებას. თუ ასეთი ქართული კომპანიები აღმოჩნდებიან ჩართული ისეთ EHR სისტემაში, რომელიც არ არის შესაბამისობაში ევროკავშირის სტანდარტებთან, ეს მნიშვნელოვანად დააბრკოლებს და პრობლემებს შეუქმნის აღნიშნული ბიზნესის განვითარებას ევროკავშირის ბაზრის მიმართულებით.

ასეთ ვითარებაში საუკეთესო გამოსავლად მიგვაჩნია - სამინისტრომ დროებით შეაჩეროს სისტემის ამოქმედების პროცესი, დაუყოვნებლივ დაიწყოს მუშაობა აღნიშნული სისტემის პერსონალურ მონაცემთა დაცვაზე გავლენის შესაფასებლად და გაატაროს ცნობიერების ამაღლებისა და სხვა საჭირო ღონისძიებები. აღნიშნული უნდა გაკეთდეს საუკეთესო ევროპული პრაქტიკის მხედველობაში მიღებით და მხოლოდ ამის შემდეგ დაიწყოს სისტემის გაშვება.

ამავე დროს, მივმართავთ პერსონალურ მონაცემთა დაცვის ინსპექტორის აპარატს, არ შემოიფარგლოს მხოლოდ შესაბამისი ნორმატიული აქტების (მინისტრი ბრძანების ტექსტის) ანალიზით, საკუთარი ინიციატივით, საფუძვლიანად შეისწავლოს EHR სისტემასთან დაკავშირებით პერსონალურ მონაცემთა დაცვის პრაქტიკული მდგომარეობა, სამინისტროს მზაობა მოსალოდნელ რისკებთან დაკავშირებით, დაეხმაროს სამინისტროს მონაცემთა დაცვის საკითხის სათანადო გაგებაში და გასცეს რეკომენდაციები გასატარებელი კომპლექსური ღონისძიებების შესახებ.