დამტკიცებულია
თსსუ-ის წარმომადგენლობითი საბჭოს
2024 წლის 21 თებერვლის N 23/5 დადგენილებით

სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტში პერსონალურ მონაცემთა დაცვის წესი

მუხლი 1. ზოგადი დებულებანი

1. საჯარო სამართლის იურიდიული პირის -თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის (შემდგომში - უნივერსიტეტი) „პერსონალურ მონაცემთა დაცვის წესი “შემუშავებულია საქართველოს კონსტიტუციის, საქართველოს სამოქალაქო კოდექსის, „პერსონალურ მონაცემთა დაცვის“ შესახებ საქართველოს კანონის, ადამიანის უფლებათა და ძირითად თავისუფლებათა დაცვის კონვენციის, თსსუ-ის წესდებისა და თსსუ-ის შინაგანაწესის საფუძველზე.
2. წინამდებარე წესის მიზანია მონაცემების დამუშავებისას და გაცემისას უზრუნველყოს უნივერსიტეტის ადმინისტრაციული, აკადემიური, დამხმარე, მოწვეული პერსონალის, სტუდენტების, ასევე, იმ მესამე პირთა, რომლებიც უნივერსიტეტის სახელით ახორციელებენ თავიანთ უფლებამოსილებას, უფლებათა და თავისუფლებათა, მათ შორის პირადი ცხოვრების ხელშეუხებლობის დაცვა; ჩამოაყალიბოს პერსონალურ მონაცემთა დაცვის სტრატეგია, მონაცემთა დაცვის ძირითადი პრინციპები და მექანიზმები.
3. უნივერსიტეტში პერსონალურ მონაცემთა დამუშავების პრინციპებია: სამართლიანობა, კანონიერება, კონკრეტული კანონიერი მიზნის არსებობის აუცილებლობა, ადეკვატურობა, პროპორციულობა, ნამდვილობა, სიზუსტე, მონაცემების შენახვის ვადა;
4. თსსუ-ის სამეცნიერო-კვლევით ერთეულებსა და კლინიკებში პერსონალური მონაცემების დაცვა და შენახვის წესები ხორციელდება წინამდებარე წესის შესაბამისად, ხოლო თსსუ-ის კლინიკებში ასევე ამ კლინიკების შიდა ადმინისტრაციულ-სამართლებრივი აქტებით.

მუხლი 2. ტერმინთა განმარტება

პერსონალური მონაცემი (შემდგომში მონაცემი)- ნებისმიერი ინფორმაცია, რომელიც უკავშირდება იდენტიფიცირებულ ან იდენტიფიცირებად ფიზიკურ პირს.
განსაკუთრებული კატეგორიის მონაცემი- მონაცემები დაკავშირებული პირის რასობრივ ან ეთნიკურ კუთვნილებასთან, პოლიტიკურ შეხედულებებთან, რელიგიურ ან ფილოსოფიურ მრწამსთან, პროფესიულ კავშირში გაწევრიანებასთან, ჯანმრთელობის მდგომარეობასთან, სქესობრივ ცხოვრებასთან, ნასამართლობასთან, ადმინისტრაციულ პატიმრობასთან, პირისთვის აღკვეთის ღონისძიების შეფარდებასთან, პირთან საპროცესო შეთანხმების დადებასთან, განრიდებასთან, დანაშაულის მსხვერპლად აღიარებასთან ან დაზარალებულად ცნობასთან, აგრეთვე ბიომეტრიული და გენეტიკური მონაცემები, რომლებიც ზემოაღნიშნული ნიშნებით ფიზიკური პირის იდენტიფიცირების საშუალებას იძლევა.
მონაცემთა სუბიექტი - ნებისმიერი ფიზიკური პირი (სტუდენტი, აკადემიური, ადმინისტრაციული, მოწვეული პერსონალი და სხვა, ვისი მონაცემებიც მუშავდება უნივერსიტეტის მიერ).
მონაცემთა დამმუშავებელი - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი, რომელიც თავისი კომპეტენციის ფარგლებში განსაზღვრავს პერსონალურ მონაცემთა დამუშავების

მიზნებსა და საშუალებებს და მონაცემების დამუშავებას ახდენს უშუალოდ ან უფლებამოსილი პირის მეშვეობით.
უფლებამოსილი პირი - ნებისმიერი ფიზიკური ან იურიდიული პირი, რომელიც ამუშავებს მონაცემებს უნივერსიტეტისთვის ან მისი სახელით. მონაცემებზე წვდომა საკუთარი კომპეტენციის ფარგლებში, კონკრეტულ გარემოებათა არსებობისას, შესაძლებელია ჰქონდეს თსსუ-ის წესდებით განსაზღვრულ ადმინისტრაციულ პერსონალს.
მონაცემთა მიმღები არის ნებისმიერი დაწესებულება, ფიზიკური ან იურიდიული პირი, კერძო ან საჯარო სექტორის თანამშრომელი, რომელსაც უნივერსიტეტი გადასცემს მონაცემებს, გარდა პერსონალურ მონაცემთა დაცვის ინსპექტორისა.
მესამე პირი- ნებისმიერი ფიზიკური ან იურიდიული პირი, საჯარო დაწესებულება, გარდა მონაცემთა სუბიექტისა, პერსონალურ მონაცემთა დაცვის ინსპექტორის, მონაცემთა დამმუშავებლისა და უფლებამოსილი პირისა.
ინციდენტი არის მონაცემთა უსაფრთხოების დარღვევა, რომელიც იწვევს მონაცემების არამართლზომიერ ან შემთხვევით დაზიანებას, დაკარგვას, აგრეთვე უნებართვო გამჟღავნებას, განადგურებას, შეცვლას, მათზე წვდომას, მათ შეგროვებას ან სხვაგვარ უნებართვო დამუშავებას.
პერსონალურ მონაცემთა დაცვის ოფიცერი - დამუშავებისთვის პასუხიმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ განსაზღვრული/ დანიშნული პირი, რომელიც ასრულებს წინამდებარე წესით განსაზღვრულ ფუნქციებს.

მუხლი 3. მონაცემთა დამუშავება

1. უნივერსიტეტი მონაცემებს ამუშავებს , როგორც ავტომატური, ნახევრად ავტომატური ასევე, არაავტომატური საშუალებების გამოყენებთ.
2. უნივერსიტეტი ამუშავებს სტუდენტის, აკადემიური და ადმინისტრაციული პერსონალის, ასევე, სხვა პირის პერსონალურ მონაცემებს.
3. უნივერსიტეტი ამუშავებს და ბრძანების სახით გამოსცემს ისეთ პერსონალურ მონაცემებს, რომელიც დაკავშირებულია პირისთვის სტუდენტის სტატუსის მინიჭებასთან, შეწყვეტასთან, შეჩერებასთან, აღდგენასთან, ასევე მისთვის სოციალური შეღავათებისა და სტიპენდიების დანიშვნასთან. უნივერსიტეტი უფლებამოსილია ბრძანება გამოაქვეყნოს საჯარო გაცნობისათვის თუ ეს განსაზღვრულია კანონით ან ეხება 50-ზე მეტ პირს.
4. უნივერსიტეტი, სტუდენტების ინტერესებიდან გამომდინარე ამუშავებს განსაკუთრებული კატეგორიის მონაცემებს, როგორიცაა მონაცემები ჯანმრთელობის მდგომარეობასთან დაკავშირებით, მხოლოდ მონაცემთა სუბიექტის მიმართვის და მისი თანხმობის საფუძველზე. სუბიექტის თანხმობის ფორმა განსაზღვრულია განცხადების შაბლონში.
5. უნივერსიტეტს უფლება აქვს დაამუშავოს მონაცემები პლაგიატიზმის პრევენციისა და მისი გამოვლენის მიზნით.
6. უნივერსიტეტი უფლებამოსილია დაამუშავოს პერსონალური მონაცემები დისციპლინური ღონისძიებების გატარების დროს.
7. უნივერსიტეტი ამუშავებს არასრულწლოვან პირთა მონაცემებს კანონიერი წარმომადგენლის თანხმობის საფუძველზე.
8. უნივერსიტეტი უზრუნველყოფს მუდმივად პერსონალურ მონაცემთა დაცვის მონიტორინგის განხორციელებას.
9. უნივერსიტეტი უზრუნველყოფს პერსონალური მონაცემების დამუშავების შესახებ დასაქმებულისა და სტუდენტის ინფორმირებას ხელშეკრულებისა და წინამდებარე წესის

მეშვეობით.

მუხლი 4. პერსონალური მონაცემების დაცვა

1. უნივერსიტეტი უზრუნველყოფს ელექტრონული ინფორმაციის დამმუშავებელი მოწყობილობის დაცვას არაავტორიზებული წვდომისგან და განზრახ დაზიანებისაგან. ამასთანავე იღებს ზომებს, რათა მონაცემები დაცული იყოს უკანონო გამჟღავნებისაგან, შეცვლისგან ნებისმიერი სხვა ფორმით უკანონო გამოყენებისა და შემთხვევითი ან უკანონო დაკარგვისგან.
2. უნივერსიტეტი უზრუნველყოფს მონაცემთა ბაზების იმგვარ ადმინისტრირებას,რომ ინფორმაცია ყველა სტუდენტს და აკადემიურ პერსონალს მიეწოდოს ინდივიდუალურად.
3.ნებისმიერი პირი, რომელიც აღმოაჩენს დარღვევებს პერსონალურ მონაცემთა დამუშავებასთან მიმართებით, ვალდებულია ამის შესახებ ინფორმაცია დაუყოვნებლივ მიაწოდოს უნივერსიტეტის ადმინისტრაციას.
4.უნივერსიტეტი პერსონალური მონაცემების უკანონოდ დამუშავებას განიხილავს სისხლის სამართლის დანაშაულად და უზრუნველყოფს ინფორმაციის მიწოდებას შესაბამისი სამართლადამცავი ორგანოებისთვის.

მუხლი 5. მონაცემთა დამუშავების საფუძვლები

1.მონაცემთა დამუშავება დასაშვებია თუ:
ა) არსებობს მონაცემთა სუბიექტის თანხმობა;
ბ) მონაცემთა დამუშავება გათვალისწინებულია კანონით;
გ) მონაცემთა დამუშავება საჭიროა უნივერსიტეტის მიერ მისთვის კანონმდებლობით დაკისრებული მოვალეობის შესასრულებლად;
დ)მონაცემთა დამუშავება საჭიროა მონაცემთა სუბიექტის სასიცოცხლო ინტერესების დასაცავად;
ე) მონაცემთა დამუშავება აუცილებელია მონაცემთა დამმუშავებლის (უნივერსიტეტის) ან მესამე პირის კანონიერი ინტერესის დასაცავად, გარდა იმ შემთხვევისა, როდესაც არსებობს მონაცემთა სუბიექტის უფლებებისა და თავისუფლებების დაცვის აღმატებული ინტერესი;
ვ)კანონის თანახმად, მონაცემები საჯაროდ ხელმისაწვდომია ან მონაცემთა სუბიექტმა ისინი ხელმისაწვდომი გახადა;
ზ) მონაცემთა დამუშავება აუცილებელია კანონის შესაბამისად მნიშვნელოვანი საჯარო ინტერესების დასაცავად;
თ) მონაცემთა დამუშავება აუცილებელია მონაცემთა სუბიექტის განცხადების განსახილველად (მისთვის მომსახურების გასაწევად);
2.იმისთვის, რომ პერსონალური მონაცემების დამუშავებას საფუძვლად დაედოს მონაცემთა სუბიექტის თანხმობა, აუცილებელია ეს თანხმობა :
ა) იყოს ნებაყოფლობითი;
ბ) გამოხატული იყოს წინასწარ მონაცემთა დამუშავებამდე;
გ)გამოხატული იყოს მონაცემთა დამუშავებასთან დაკავშირებული ინფორმაციის მიღების შემდეგ;
დ) გამოხატული იყოს კონკრეტული მკაფიოდ განსაზღვრული კანონიერი მიზანი მონაცემთა დამუშავებაზე;
ე) გამოხატვის საშუალება იყოს ნათელი, რომლითაც დგინდება მონაცემთა სუბიექტის ნება.

მუხლი 6. პერსონალური მონაცემების მოპოვება მესამე პირებისგან

1.თბილისის სახელმწიფო სამედიცინო უნივერსიტეტმა მონაცემთა სუბიექტის პერსონალური მონაცემები შესაძლოა მესამე პირებისგან მოიპოვოს შემდეგი მიზნებისათვის: მონაცემთა სუბიექტის სრულყოფილი მომსახურებისთვის, საქართველოს კანონმდებლობით განსაზღვრულ შემთხვევებში, საქართველოს კანონმდებლობით უნივერსიტეტისთვის დაკისრებული მოვალეობების შესრულების მიზნით, ასევე, მესამე პირებისგან, სახელმწიფო სექტორში მოქმედ ორგანიზაციებთან, პარტნიორ ორგანიზაციებთან გაფორმებული ხელშეკრულებებიდან გამომდინარე უნივერსიტეტის მიერ ნაკისრი ვალდებულებების შესრულების მიზნებისათვის.

2. მესამე პირს წარმოადგენს ფიზიკური და/ან იურიდიული პირი, სახელმწიფო სექტორში მოქმედი ორგანიზაციები.

მუხლი 7. განსაკუთრებული კატეგორიის მონაცემთა დამუშავება

1.უნივერსიტეტში აკრძალულია განსაკუთრებული კატეგორიის მონაცემთა დამუშავება, გარდა იმ შემთხვევისა, როცა არსებობს სუბიექტის წერილობითი თანხმობა;
2. ნასამართლობასა და ჯანმრთელობის მდგომარეობასთან დაკავშირებული მონაცემების დამუშავება აუცილებელია შრომითი ვალდებულებების და ურთიერთობების ხასიათიდან გამომდინარე, მათ შორის დასაქმების თაობაზე გადაწყვეტილების მისაღებად;
3. მონაცემები მუშავდება სპეციალური საგანმანათლებლო საჭიროების მქონე პირთა განათლების უფლების რეალიზების მიზნით;

მუხლი 8. გარდაცვლილი პირის შესახებ მონაცემთა დაცვა

1.გარდაცვლილი პირის მონაცემების დამუშავება, რომელიც დაცულია უნივერსიტეტში, დასაშვებია:
ა) გარდა იმ შემთხვევისა, თუ ამ მონაცემთა დამუშავებაზე შეზღუდვის შესახებ არსებობს მონაცემთა სუბიექტის მშობლის, შვილის, შვილიშვილის ან მეუღლის მიერ წერილობითი დოკუმენტი.
ბ) როდესაც გარდაცვლილმა სუბიექტმა გარდაცვალებამდე წერილობით აკრძალა მისი გარდაცვალების შემდეგ, მის შესახებ მონაცემთა დამუშავება.

მუხლი 9. პერსონალის უფლება-მოვალეობანი

1. უნივერსიტეტში დასაქმებული პირები ვალდებულნი არიან დაიცვან წინამდებარე წესი.
2. უნივერსიტეტი უზრუნველყოფს პერსონალის ინფორმირებას, წინასახელშეკრულებო ურთიერთობისას როგორი სახის პერსონალურ მონაცემებს დაამუშავებს მის შესახებ უნივერსიტეტი.
3. დასაქმებულ პირებს ეკრძალებათ პერსონალური მონაცემების შემცველი დოკუმენტებისა და ფაილების უყურადღებოდ დატოვება.
4. უნივერსიტეტის პერსონალი ვალდებულია არ გაამჟღავნოს და არ გადასცეს სხვისი პერსონალური მონაცემები სხვა პირებს. პერსონალური მონაცემების დაცვის ვალდებულება გააჩნიათ იმ შემთხვევაშიც, თუ ისინი აღარ იქნებიან დასაქმებულნი უნივერსიტეტში.

5. იმ შემთხვევაში, თუ პირები აღარ არიან დასაქმებულნი უნივერსიტეტში და დაარღვევენ წინამდებარე წესს, პასუხისმგებლობა დადგება მოქმედი კანონმდებლობის შესაბამისად.
6. პერსონალური მონაცემების დამუშავების შესახებ დადგენილი წესების დარღვევა არის უნივერსიტეტის პერსონალის მიმართ დისციპლინური წარმოების დაწყების საფუძველი.

მუხლი 10. მონაცემთა სუბიექტის უფლებები და ვალდებულებები

1. მონაცემთა სუბიექტს უფლება აქვს მოსთხოვოს უნივერსიტეტს ინფორმაცია მის შესახებ მონაცემთა დამუშავების თაობაზე . უნივერსიტეტი შეტყობინების მიღებიდან არაუგვიანეს 10 (ათი) კალენდარული დღისა უზრუნველყოფს მონაცემთა სუბიექტისთვის ინფორმაციის მიწოდებას, თუ რომელი კატეგორიის ინფორმაცია მუშავდება, რა მიზნით და რა სამართლებრივი საფუძვლით, ასევე, გაცემულია თუ არა მისი მონაცემები მესამე პირზე, და ასეთის არსებობის შემთხევასი ვისზე გაიცა ეს მონაცემი.

2. მონაცემთა სუბიექტს უფლება აქვს ნებისმიერ დროს, ყოველგვარი განმარტების ან დასაბუთების გარეშე გამოიხმოს მის მიერ გაცემული თანხმობა. ამ შემთხვევაში, მონაცემთა სუბიექტის მოთხოვნის საფუძველზე, მონაცემთა დამუშავება უნდა შეწყდეს ან/და დამუშავებული მონაცემები წაიშალოს ან განადგურდეს მოთხოვნიდან არაუგვიანეს 10 სამუშაო დღისა, თუ მონაცემთა დამუშავების სხვა საფუძველი არ არსებობს.

3. მონაცემთა სუბიექტის მიერ თანხმობის გამოხმობა არ იწვევს თანხმობის გამოხმობამდე და თანხმობის ფარგლებში წარმოშობილი სამართლებრივი შედეგების გაუქმებას.

მუხლი 11. სტუდენტის უფლება-მოვალეობები

1.უნივერსიტეტი სტუდენტებს უნივერსიტეტთან მომსახურების ხელშეკრულების გაფორმებამდე აწვდის ინფორმაციას, როგორი სახის პერსონალურ მონაცემებს ამუშავებს მის შესახებ უნივერსიტეტი.
2. სტუდენტები (წარმომადგენლები, ასეთის არსებობის შემთხვევაში) ვალდებულნი არიან:

ა)დაიცვან წინამდებარე წესი, როდესაც ისინი წარმოადგენენ უნივერსიტეტს და უნივერსიტეტის სახელით მონაწილეობენ სხვადასხვა აქტივობაში.
ბ)შეატყობინონ უნივერსიტეტს თავისი პერსონალური მონაცემების ცვლილების შესახებ.

3. თსსუ-ის „პერსონალურ მონაცემთა დაცვის წესის“ დარღვევა არის სტუდენტის მიმართ დისციპლინური წარმოების დაწყების საფუძველი.
4. სტუდენტებისათვის პროგრამის ,,სახელმწიფო სტიპენდიები სტუდენტებს” ფარგლებში სტიპენდიების (შემდგომში - ,,სტიპენდია“) დანიშვნის წარმოების პროცესში არსებული პერსონალური მონაცემების დამუშავება აუცილებელია აღნიშნული სტიპენდიის კონკრეტულ პირთა წრისათვის (სტუდენტებისათვის) დანიშვნის მიზნით, რაც ემსახურება მათი სწავლის უფლების რეალიზების დამატებით ხელშეწყობას.
5.16 წელს მიღწეული არასრულწლოვანი სტუდენტის შესახებ მონაცემთა დამუშავება დასაშვებია მისი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა, მათ შორის, როდესაც მონაცემთა დამუშავებისთვის აუცილებელია 16 წლიდან

18 წლამდე არასრულწლოვანისა და მისი მშობლის ან სხვა კანონიერი წარმომადგენლის თანხმობა.
6.არასრულწლოვანის შესახებ განსაკუთრებული კატეგორიის მონაცემთა დამუშავება დასაშვებია მხოლოდ მისი მშობლის ან სხვა კანონიერი წარმომადგენლის წერილობითი თანხმობის საფუძველზე, გარდა კანონით პირდაპირ გათვალისწინებული შემთხვევებისა.

მუხლი 12. უნივერსიტეტის შენობაში ვიდეომონიტორინგის განხორციელება

1. უნივერსიტეტის შენობაში ხორციელდება ვიდეომონიტორინგი, პირთა უსაფრთხოების, უნივერსიტეტის ინვენტარის, საიდუმლო ინფორმაციის დაცვისა და გამოცდის/ტესტირების მიზნებისათვის.
2.ვიდეოსათვალთვალო სისტემაზე წვდომის უფლებამოსილების მქონე პირ(ებ)ის სამსახურიდან წასვლის ან/და მივლინების ან/და შვებულების დროს პერსონალურ მონაცემებზე წვდომის უფლებამოსილება გააჩნია უფლებამონაცვლე პირ(ებ)ს, რომლ(ებ)ზეც გადადის იგივე უფლება-მოვალეობები.
3. უნივერსიტეტი უფლებამოსილია, ვიდეოჩანაწერი გამოიყენოს მტკიცებულებად პირველ პუნქტში გათვალისწინებული მიზნებისთვის. ვიდეოჩანაწერში მოხვედრილი სხვა პირების პერსონალური მონაცემები უნდა დაიშიფროს ან უნდა არსებობდეს მათი თანხმობა.
4. ოპერატიულ-სამძებრო ღონისძიებებისა და დანაშაულის გამოძიების მიზნით, მოთხოვნის საფუძველზე, უნივერსიტეტი ვიდეოჩანაწერს გადასცეს შესაბამის უწყებებს, მხოლოდ მოსამართლის განჩინების, ან გადაუდებელი აუცილებლობის შემთხვევაში პროკურორის მოტივირებული დადგენილების საფუძველზე.
5.აუდიოკონტროლის განხორციელება დასაშვებია მხოლოდ უნივერსიტეტის მიერ დისტანციური მომსახურების განხორციელებისას ან მომსახურების გაუმჯობესების მიზნებიდან გამომდინარე, სუბიექტის წინასწარი ინფორმირების შემთხვევაში;
6. ვიდეომონიტორინგის /აუდიომონიტორინგის შედეგად მიღებული ჩანაწერი ინახება არა უმეტეს 1 თვისა.

მუხლი 13. ელექტრონული ფოსტისა და ტელეფონის ნომრის გამოყენება
1. ეფექტური და სწრაფი კომუნიკაციის მიზნით, უნივერსიტეტი ამუშავებს დასაქმებული პირების, ადმინისტრაციული პერსონალის, აკადემიური და მოწვეული პერსონალის, სტუდენტებისა და კურსდამთავრებულების ელ-ფოსტებსა და ტელეფონის ნომრებს.

მუხლი 14. ინციდენტი

1. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი ვალდებულია აღრიცხოს ინციდენტი, დამდგარი შედეგი, მიღებული ზომები, ინციდენტის აღმოჩენიდან არა უგვიანეს 72 საათისა, მის შესახებ წერილობით ან ელექტრონულად შეატყობინოს წარუდგინოს პერსონალურ მონაცემთა დაცვის სამსახურს, გარდა იმ შემთხვევისა, როდესაც ნაკლებსავარაუდოა, რომ ინციდენტი მნიშვნელოვან ზიანს გამოიწვევს ან/და მნიშვნელოვან საფრთხეს შეუქმნის ადამიანის ძირითად უფლებებსა და თავისუფლებებს.

2. დამუშავებაზე უფლებამოსილი პირი ვალდებულია, აღრიცხოს მონაცემთა დამუშავებასთან დაკავშირებული, მათ შორის ინციდენტის შესახებ ინფორმაცია. აღნიშნული ვალდებულება ყველა აღმოჩენილ ინციდენტზე ვლინდება, მიუხედავად იმისა, ექვემდებარება თუ არა

ინციდენტი პერსონალურ მონაცემთა დაცვის სამსახურისთვის ან/და მონაცემთა სუბიექტისთვის შეტყობინებას.

მუხლი 15. ინციდენტის შეფასება

1.ინციდენტის შედეგად ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმე სსიპ -თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის ან დამუშავებისათვის პასუხისმგებელი პირის მიერ უნდა შეფასდეს შემდეგი კრიტერიუმების გათვალისწინებით:

1.1 . ინციდენტის სახე
ინციდენტი ყოველთვის უკავშირდება პერსონალურ მონაცემებს და ინფორმაციული უსაფრთხოების საყოველთაოდ აღიარებული პრინციპების შესაბამისად იყოფა შემდეგ სახეებად:
ა)კონფიდენციალურობის დარღვევა;
ბ)მთლიანობის დარღვევა;
გ)ხელმისაწვდომობის დარღვევა.
1.2. იმ პერსონალური მონაცემების კატეგორია, რომლებზეც ინციდენტი გავლენას ახდენს;
ა) განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონდე პირები, როგორც მონაცემთა სუბიექტები;
ბ) მონაცემთა სუბიექტების იდენტიფიცირების შესაძლებლობის ხარისხი;
გ) მონაცემთა სუბიექტ(ებ)ის უფლებებისა და ინტერესების მიმართ დამდგარი შედეგი;
დ) დამუშავებისათვის პასუხისმგებელი პირის საქმიანობის განსაკუთრებული ხასიათი;
ე) ინციდენტის მასშტაბი, მონაცემთა სუბიექტის და/ან პერსონალური მონაცემის რაოდენობის და/ან მოცულობის თვალსაზრისით;
ვ) სხვა გარემოებები.

მუხლი 16. ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის განსაზღვრის კრიტერიუმები

1. ინციდენტი, ადამიანის უფლებებისა და თავისუფლებების შელახვის სიმძიმის თვალსაზრისით, მნიშვნელოვანი ზიანის გამომწვევად უნდა იქნეს მიჩნეული, მათ შორის, იმ შემთხვევებში, თუ მას მოჰყვა/შესაძლოა მოჰყვეს ერთ-ერთი შემდეგი შედეგი:
ა) მონაცემთა სუბიექტის დისკრიმინაცია (ვინაობის მითვისება ან გაყალბება, ფინანსური ზიანი, მონაცემთა სუბიექტის რეპუტაციის შელახვა, პროფესიული საიდუმლოებით დაცული პერსონალური მონაცემების კონფიდენციალობის დარღვევა, ან სხვა სახის მნიშვნელოვანი სოციალური ან/და ეკონომიკური ზიანი);

ბ) მონაცემთა სუბიექტის „პერსონალურ მონაცემთა დაცვის შესახებ“ საქართველოს კანონით გათვალისწინებული უფლებების რეალიზებისათვის ხელის შეშლა, მათ შორის, მონაცემთა სუბიექტის უფლებების კანონით დადგენილ ვადებში რეალიზების შეზღუდვა;

გ) პერსონალური მონაცემების იმგვარი წაშლა/განადგურება, რომელიც არ ექვემდებარება აღდგენას, ან მისი აღდგენა არაპროპორციულად დიდ დროსა და ძალისხმევას საჭიროებს, გარდა იმ შემთხვევისა, როდესაც პერსონალური მონაცემების (გარდა განსაკუთრებული

კატეგორიის პერსონალური მონაცემისა) დამუშავების მიზნიდან გამომდინარე, მათი წაშლის/განადგურების შედეგად, მონაცემთა სუბიექტს მნიშვნელოვანი ზიანი არ ადგება;

დ) განსაკუთრებული კატეგორიის მონაცემების უკანონო გამჟღავნება;

ე) ფიზიკური ზიანი, მათ შორის, სამედიცინო მომსახურების მიღების შეზღუდვა, თუ აღნიშნული იწვევს სამედიცინო მანიპულაციის ან ოპერაციის გადადებას, რაც პაციენტის მკურნალობაზე ახდენს უარყოფით გავლენას;

ვ) არასრულწლოვნების, შეზღუდული შესაძლებლობების მქონე პირებისა და სხვა განსაკუთრებული სოციალური თუ სამართლებრივი დაცვის საჭიროების მქონე მონაცემთა სუბიექტ(ებ)ის პერსონალური მონაცემების უკანონო დამუშავება.

2.ინციდენტით მონაცემთა სუბიექტების უფლებებისადმი გამოწვეული შესაძლო შედეგის სიმძიმის შეფასების შემდეგ საჭიროა სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის მიერ ამ შედეგის დადგომის ალბათობის განსაზღვრა.

3.შედეგის დადგომის ალბათობა შეიძლება იყოს დაბალი, საშუალო ან მაღალი.

მუხლი 17. პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულება, ფორმა და ვადები

1.სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი ვალდებულია ინციდენტის თაობაზე შეატყობინოს პერსონალურ მონაცემთა დაცვის სამსახურს იმ შემთხვევებში, თუ:

ა) არსებობს გარკვეული ალბათობა, რომ ინციდენტი გამოიწვევეს იმგვარ შედეგს, რომელიც, ზემოაღნიშნული კრიტერიუმების შესაბამისად, ადამიანის ძირითად უფლებებისა და თავისუფლებებისადმი მნიშვნელოვანი ზიანის გამომწვევად/მნიშვნელოვანი საფრთხის შემცველად მოიაზრება;

ბ) აღნიშნული ალბათობა არის საშუალო ან მაღალი, ან ასეთი შედეგი უკვე დამდგარია.

2. თითოეული შეტყობინების დროულობის შეფასებისას მხედველობაში უნდა იქნეს მიღებული ინციდენტის ხასიათი, მასშტაბი და მონაცემთა სუბიექტების უფლებებისადმი მოსალოდნელი შედეგების სიმძიმე.
3.შეტყობინება, ფორმის შევსება და მისი წარდგენა უნდა განახორციელოს პერსონალურ მონაცემთა დაცვის ოფიცერმა, ხოლო მისი არყოფნის შემთხვევაში, დამუშავებისთვის პასუხისმგებელი პირის მიერ განსაზღვრულმა სხვა პირმა.

4.პერსონალურ მონაცემთა დაცვის სამსახურისათვის მიწოდებული ინფორმაცია უნდა შეიცავდეს კანონით გათვალისწინებულ რეკვიზიტებს.

მუხლი 18 . პერსონალურ მონაცემთა დაცვის ოფიცერი (ამოქმედდეს 01.06.2024 წლიდან)

1. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტში პერსონალურ მონაცემთა დამუშავების პროცესების პერსონალურ მონაცემთა დაცვის კანონმდებლობასთან

შესაბამისობის უზრუნველყოფას ხელშეკრულების საფუძველზე ახორციელებს პერსონალურ მონაცემთა დაცვის ოფიცერი, რომელიც თავის საქმიანობაში დამოუკიდებელია და ექვემდებარება რექტორს.

2. პერსონალურ მონაცემთა დაცვის ოფიცრის კომპეტენცია:

1. პერსონალურ მონაცემთა დაცვის ოფიცერი:
ა) აკონტროლებს უნივერსიტეტში პერსონალურ მონაცემთა დამუშავების პროცესს;
ბ) საჭიროების შემთხვევაში მონაწილეობს მონაცემთა დამუშავების რისკების შეფასების პროცესში;
გ) საჭიროების შემთხვევაში თანამშრომლობს პერსონალურ მონაცემთა დაცვის სამსახურთან;
დ) უზრუნველყოფს თანამშრომელთა ინფორმირებასა და გადამზადებას პერსონალურ მონაცემთა დაცვის საკითხებზე;
ე) განიხილავს მონაცემთა სუბიექტის განცხადებებს, საჩივრებს და/ან მომართვებს;
ვ) პერსონალურ მონაცემთა დაცვის საკითხზე კონსულტაციას უწევს ადმინისტრაციულ და აკადემიურ პერსონალს, მოწვეულ ლექტორებს, სტუდენტებს, კურსდამთავრებულებს და უნივერსიტეტში დასაქმებულ პირებს;
ზ) აწარმოებს და პერსონალურ მონაცემთა დაცვის სამსახურს წარუდგენს ფაილური სისტემების კატალოგებს;
თ) გამოავლენს, შეისწავლის და სათანადო რეაგირებას ახდენს პერსონალურ მონაცემთა დარღვევის ფაქტებზე;
ი)მონაცემთა დაცვასთან დაკავშირებულ საკითხებზე, მათ შორის, მარეგულირებელი სამართლებრივი ნორმების მიღების ან შეცვლის შესახებ, დამუშავებისთვის პასუხისმგებელი პირის, დამუშავებაზე უფლებამოსილი პირისა და მათი თანამშრომლების ინფორმირებას, მათთვის კონსულტაციისა და მეთოდური დახმარებისგაწევას;
კ) მონაცემთა დამუშავებასთან დაკავშირებული შიდა რეგულაციებისა და მონაცემთა დაცვაზე ზეგავლენის შეფასების დოკუმენტის შემუშავებაში მონაწილეობას, აგრეთვე დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ საქართველოს კანონმდებლობისა და შიდა ორგანიზაციული დოკუმენტების შესრულების მონიტორინგს;
ლ) მონაცემთა დამუშავებასთან დაკავშირებით შემოსული განცხადებებისა და საჩივრების ანალიზსა და შესაბამისი რეკომენდაციების გაცემას;
მ)პერსონალურ მონაცემთა დაცვის სამსახურისგან კონსულტაციების მიღებას, დამუშავებისთვის პასუხისმგებელი პირისა და დამუშავებაზე უფლებამოსილი პირის წარმომადგენლობას პერსონალურ მონაცემთა დაცვის სამსახურთან ურთიერთობაში, მისი მოთხოვნით ინფორმაციისა და დოკუმენტების წარდგენას და მისი დავალებებისა და რეკომენდაციების შესრულების კოორდინაციასა და მონიტორინგს;
ნ)მონაცემთა სუბიექტის მიმართვის შემთხვევაში მისთვის მონაცემთა დამუშავების პროცესებისა და მისი უფლებების შესახებ ინფორმაციის მიწოდებას;
ო)დამუშავებისთვის პასუხისმგებელი პირის ან დამუშავებაზე უფლებამოსილი პირის მიერ მონაცემთა დამუშავების სტანდარტების ამაღლების მიზნით სხვა ფუნქციების შესრულებას. (ამოქმედდეს 2024 წლის 1 ივნისიდან);
2. პერსონალურ მონაცემთა დაცვის ოფიცერს უნდა ჰქონდეს სათანადო ცოდნა მონაცემთა დაცვის სფეროში.

3. პერსონალურ მონაცემთა დაცვის ოფიცერს უფლება აქვს, შეასრულოს სხვა ფუნქციაც, თუ ეს არ წარმოშობს ინტერესთა კონფლიქტს.
4. პერსონალურ მონაცემთა დაცვის ოფიცერი კონკრეტული ვითარების გათვალისწინებით ანგარიშვალდებულია სსიპ - თბილისის სახელმწიფო სამედიცინოუნივერსიტეტის რექტორის და ადმინისტრაციის ხელმძღვანელის (კანცლერის) წინაშე.
5. დამუშავებისთვის პასუხისმგებელმა პირმა და დამუშავებაზე უფლებამოსილმა პირმა უნდა უზრუნველყონ პერსონალურ მონაცემთა დაცვის ოფიცრის სათანადო ჩართულობა მონაცემთა დამუშავებასთან დაკავშირებით მნიშვნელოვანი გადაწყვეტილების მიღების პროცესში, უზრუნველყონ იგი შესაბამისი რესურსებით, აგრეთვე უზრუნველყონ მისი დამოუკიდებლობა საქმიანობის განხორციელებისას.
6. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი ვალდებულია პერსონალურ მონაცემთა დაცვის ოფიცრის დანიშვნიდან ან მისი შეცვლიდან არა უგვიანეს 10 სამუშაო დღის ვადაში მისი ვინაობა და საკონტაქტო ინფორმაცია აცნობოს პერსონალურ მონაცემთა დაცვის სამსახურს, რომელიც აქვეყნებს აღნიშნულ ინფორმაციას.
7. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტი ვალდებულია პერსონალურ მონაცემთა დაცვის ოფიცრის ვინაობა და საკონტაქტო ინფორმაცია პროაქტიულად გამოაქვეყნოს უნივერსიტეტის ოფიციალურ ვებგვერდზე.
8. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტის პერსონალურ მონაცემთა დაცვის ოფიცრის დროებითი არყოფნის ან მისი უფლებამოსილების შეწყვეტის შემთხვევაში ვალდებულია გაუმართლებელი დაყოვნების გარეშე პერსონალურ მონაცემთა დაცვის ოფიცრის უფლებამოსილებით აღჭურვოს სხვა პირი.

მუხლი 19. უნივერსიტეტის მიერ პერსონალურ მონაცემთა დაცვის სამსახურის ინფორმირების ვალდებულების გამომრიცხავი გარემოებები

1.ინციდენტის შესახებ მონაცემთა სუბიექტების ინფორმირების ვალდებულება არ წარმოიშობა, თუ ეს საფრთხეს შეუქმნის:
ა) საზოგადოებრივი უსაფრთხოების ინტერესებს;
ბ) დანაშაულის თავიდან აცილებას, ოპერატიულ-სამძებრო საქმიანობას, დანაშაულის გამოძიებას, სისხლისსამართლებრივ დევნას;
გ) მართლმსაჯულების განხორციელებას;
2. მონაცემთა სუბიექტების ინფორმირების ვალდებულება ასევე არ წარმოიშობა იმ შემთხვევაში, თუ დამუშავებისთვის პასუხისმგებელმა პირმა მიიღო შესაბამისი უსაფრთხოების ზომები, რის შედეგადაც თავიდან იქნა აცილებული ადამიანის ძირითადი უფლებებისა და თავისუფლებების დარღვევის მნიშვნელოვანი საფრთხე.

მუხლი 20. დასკვნითი დებულებები

1. დაევალოს შესაბამის სამსახურებს, განახორციელონ შესაბამისი ცვლილებები ხელშეკრულებებში, რათა დაცული იყოს პერსონალურ მონაცემთა დაცვის კანონის მოთხოვნები.

2. სსიპ - თბილისის სახელმწიფო სამედიცინო უნივერსიტეტისათვის პირ(ებ) ის პერსონალურ მონაცემთა დაცვა სავალდებულოა.
3. ინციდენტის შესახებ პერსონალურ მონაცემთა დაცვის სამსახურისთვის შეტყობინების ვალდებულების, ისევე, როგორც ინციდენტის შესახებ მონაცემთა სუბიექტისთვის შეტყობინების ვალდებულების არაჯეროვანი შესრულება წარმოადგენს ადმინისტრაციულ სამართალდარღვევას.
4. წინამდებარე წესი ძალაშია დამტკიცებისთანავე.
5. წინამდებარე წესის გაუქმება, მასში ცვლილებების შეტანა ხდება მიღებისათვის დადგენილი წესით.