



სამედიცინო ინფორმაციის დაცვის ეთიკური და სამართლებრივი ასპექტები

ელექტრონულ მმართველობაში

Ethical and Legal Aspects of Medical Information Protection

in Electronic Government

 <https://doi.org/10.52340/healthecosoc.2025.09.02.15>

ილონა ბიტაროვა^{1a}, ლუკ მარკსი^{2,3b}, გიორგი დუღაშვილი^{4c}

Ilona Bitarova^{1a}, Luc Marks^{2,3b}, Giorgi Dugashvili^{4c}

¹ საჯარო მმართველობის და პოლიტიკის სკოლა, გრიგოლ რობაქიძის სახელობის უნივერსიტეტი, თბილისი, საქართველო

² მედიცინისა და ჯანდაცვის მეცნიერებათა ფაკულტეტი, ანტვერპენის უნივერსიტეტი, ანტვერპენი, ბელგია

³ განსაკუთრებული მზრუნველობის სტომატოლოგიისა და ქალა-ყბა-სახის ქირურგიის განყოფილება, ანტვერპენის უნივერსიტეტის საავადმყოფო, ედგემი, ბელგია

⁴ მედიცინის სკოლა, გრიგოლ რობაქიძის სახელობის უნივერსიტეტი, თბილისი, საქართველო

¹School of Public Administration and Politics, Grigol Robakidze University, Tbilisi, Georgia

²Faculty of Medicine & Health Sciences, University of Antwerp, Antwerp, Belgium

³Special care in dentistry, department of Cranio-Maxillofacial Surgery, Antwerp University Hospital, Edegem, Belgium

⁴School of Medicine, Grigol Robakidze University, Tbilisi, Georgia

^a ilona.bitarova@gruni.edu.ge, ^b Luc.Marks@uza.be, ^c giorgi.dugashvili@gruni.edu.ge



^{*} <https://orcid.org/0009-0001-5161-485X>, ^{**} <https://orcid.org/0000-0001-5098-6726>,

^{***} <https://orcid.org/0009-0005-2995-3256>

აბსტრაქტი

შესავალი: ჯანდაცვის სისტემის დიგიტალიზაციამ მნიშვნელოვნად გააძლიერა სამედიცინო მომსახურების ეფექტურობა, ხელმისაწვდომობა და მონაცემებზე სწრაფი წვდომა, თუმცა ამავე დროს წარმოშვა ახალი ეთიკური და სამართლებრივი გამოწვევები პაციენტების პერსონალური სამედიცინო ინფორმაციის დაცვის კუთხით. ელექტრონული მმართველობის განვითარება მოითხოვს მკაფიოდ განსაზღვრულ რეგულაციებს, რომლებიც უზრუნველყოფს კონფიდენციალურობას, ინფორმირებულ თანხმობას, კიბერუსაფრთხოებას და ჯანდაცვის სისტემის მიმართ ნდობის გაზრდას. **მეთოდოლოგია:** სტატიაში გამოყენებულია დოკუმენტური და სამართლებრივი ანალიზის მეთოდი, რომელიც მოიცავს: საერთაშორისო რეგულაციების (GDPR, HIPAA, 108-ე კონვენცია) შედარებით განხილვას, საქართველოს კანონმდებლობის (პერსონალური მონაცემების დაცვა, ჯანმრთელობის დაცვის შესახებ კანონი, სამედიცინო საქმიანობის შესახებ კანონი) ანალიზს, WHO, OECD და სხვა ავტორიტეტული წყაროების შეფასებებს, COVID-19 პანდემიის მაგალითზე დიგიტალიზაციის დაჩქარების ეფექტის შესწავლას. მეთოდოლოგია ემყარება ეთიკური პრინციპების (ავტონომია, სამართლიანობა, უვნებლობა, ანგარიშვალდებულება) სისტემურ შეფასებას. **შედეგები:** კვლევამ გამოავლინა რამდენიმე კრიტიკული საკითხი: სამედიცინო მონაცემებზე კიბერშეტევებისა და მონაცემების გამჟღავნების მაღალი რისკი; პაციენტების არასაკმარისი ინფორმირებულობა და რთული თანხმობის ფორმები; პერსონალის არათანაბარი ციფრული უნარები და ინფრასტრუქტურული

სირთულეები; საერთაშორისო სტანდარტებთან შესაბამისობის დეკლარირებული, მაგრამ არასრულად განხორციელებული პრაქტიკა; პანდემიით დაჩქარებული დიგიტალიზაცია, რომელმაც ხელი შეუწყო მომსახურების უწყვეტობას, თუმცა გაზარდა მონაცემთა დაცვის გამოწვევები; ხანდაზმულებისა და შეზღუდული შესაძლებლობის მქონე პირებისათვის ხელმისაწვდომობის პრობლემები. ობიექტური უპირატესობების მიუხედავად (ეფექტიანობა, უწყვეტობა, სწრაფი წვდომა), დიგიტალური მმართველობა მოითხოვს რისკების კომპლექსურ მართვას. **დასკვნა.** დიგიტალური ჯანდაცვის უსაფრთხო ფუნქციონირება დამოკიდებულია სამართლებრივი ჩარჩოს გაძლიერებაზე, კიბერუსაფრთხოების უზრუნველყოფაზე, თანხმობის გამარტივებულ და გამჭვირვალე მექანიზმებზე, პაციენტებისა და პერსონალის ციფრული განათლების ზრდაზე და საერთაშორისო სტანდარტების ინტეგრაციაზე. აუცილებელია მონაცემთა დაცვის ტექნიკური, სამართლებრივი და ეთიკური სისტემების გაძლიერება, რათა გაიზარდოს ნდობა, ხარისხი და პაციენტთა უფლებების დაცვა ელექტრონულ მმართველობაში.

საკვანძო სიტყვები: სამედიცინო მონაცემები, ელექტრონული მმართველობა, ჯანდაცვის დიგიტალიზაცია, კონფიდენციალურობა, კიბერუსაფრთხოება.

რეკომენდირებული ციტირება: ბიტაროვა ი, მარკსი ლ, დუღაშვილი გ. (2025). სამედიცინო ინფორმაციის დაცვის ეთიკური და სამართლებრივი ასპექტები ელექტრონულ მმართველობაში. *ჯანდაცვის პოლიტიკა, ეკონომიკა და სოციოლოგია*, 9 (2). DOI: <https://doi.org/10.52340/healthecosoc.2025.09.02.15>.

Abstract

Introduction: The digital transformation of healthcare systems has significantly enhanced the efficiency, accessibility, and continuity of medical services. Electronic governance and health information technologies enable faster access to medical records, improved coordination among institutions, and data-driven clinical decision-making. However, the rapid integration of digital tools into healthcare introduces substantial ethical and legal challenges related to safeguarding patients' personal medical information. Ensuring confidentiality, informed consent, cybersecurity, and accountability has become essential for maintaining trust in electronic health systems. International regulations such as the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and Convention 108, together with national legislative frameworks, require healthcare institutions to implement robust data protection standards. **Methods:** This study employs a document analysis and legal review methodology. International regulatory documents, including GDPR, HIPAA, OECD recommendations, and WHO guidelines, were examined to identify core principles of digital health data governance. Georgian legislation, particularly the Law on Personal Data Protection, the Law on Health Care, and the Law on Medical Practice, was analyzed to assess its alignment with international norms. In addition, ethical principles such as autonomy, justice, non-maleficence, transparency, and accountability were evaluated as guiding frameworks for medical data protection. The analysis also incorporates insights from global literature on digital health transformation during the COVID-19 pandemic, which served as a catalyst for accelerated digital adoption, remote consultations, and large-scale electronic data processing. **Results:** The findings highlight several critical issues associated with the electronic management of medical information. First, the risk of cyberattacks and data breaches remains high, given that medical information is among the most sensitive categories of personal data. Unauthorized access, system errors, and insufficient cybersecurity measures can lead to significant harm, including discrimination, psychological distress, and financial loss. Second, patients frequently lack adequate understanding of informed consent procedures. Complex legal documents and technical terminology make it difficult for individuals to grasp what data are collected, how they are processed, and who has access to them. This undermines autonomy and reduces trust in digital health systems. Third, disparities in digital literacy create additional barriers, particularly for older adults and persons with disabilities, limiting their ability to use electronic health services effectively. Fourth, the rapid digitization triggered by the COVID-19 pandemic improved service continuity but also exposed weaknesses in data protection practices, particularly in contexts with limited infrastructure. Fifth, despite the existence of legal frameworks, practical implementation gaps remain within healthcare institutions, including insufficient staff training and inconsistent application of information security protocols. Nevertheless, electronic governance offers substantial benefits, such as improved transparency, timely access to health information, enhanced coordination, and better allocation of medical resources. These advantages underscore the need for

strengthened governance mechanisms rather than retreat from digital systems. **Conclusion:** Ensuring the secure and ethical management of medical information in digital healthcare requires a comprehensive approach. Strengthening the legal framework, improving cybersecurity infrastructure, simplifying informed consent procedures, and enhancing digital competencies among both patients and healthcare professionals are essential steps. International cooperation and harmonization with global standards play a crucial role in creating resilient systems capable of adapting to technological advancements. Ultimately, building trustworthy, transparent, and ethically grounded electronic health governance will not only protect patient privacy but also enhance the quality, equity, and reliability of healthcare services in the digital era.

Keywords: Medical data, electronic governance, healthcare digitalization, confidentiality, cybersecurity.

Recommended Citation: Bitarova I, Marks L, Dugashvili G. (2025). Ethical and Legal Aspects of Medical Information Protection in Electronic Government. *Health Policy, Economics and Sociology*, 9(2). <https://doi.org/10.52340/healthecosoc.2025.09.02.15>.

შესავალი

ტექნოლოგიების განვითარების ეპოქაში სამედიცინო მონაცემების დაცვა მნიშვნელოვანი ამოცანაა როგორც ეთიკური, ასევე სამართლებრივი თვალსაზრისით. ჯანდაცვის სექტორში ელექტრონული მმართველობის სისტემების განვითარება იწვევს ახალ გამოწვევებს პაციენტების პერსონალური მონაცემების კონფიდენციალურობისა და უსაფრთხოების სფეროში.

ელექტრონული მმართველობის სისტემები სამთავრობო უწყებებს საშუალებას აძლევს ეფექტურად მართონ სამედიცინო ჩანაწერები, უზრუნველყონ სამედიცინო სერვისებზე დისტანციური წვდომა და გააუმჯობესონ პერსონალიზებული მომსახურება. თუმცა, ციფრული ტექნოლოგიების ფართო გამოყენება სამედიცინო სფეროში ქმნის მონაცემთა უნებართვო გამჟღავნების, არავტორიზებული წვდომისა და კონფიდენციალური ინფორმაციის ბოროტად გამოყენების რისკებს. შედეგად, საჭიროა კომპლექსური მიდგომა, რომელიც აერთიანებს საკანონმდებლო რეგულირებას, ტექნოლოგიურ გადაწყვეტილებებს და ეთიკურ პრინციპებს, რომლებიც მიმართულია პაციენტების პერსონალური მონაცემების დაცვაზე.

კვლევის მიზანია გაანალიზოს სამედიცინო ინფორმაციის დაცვის ეთიკური და სამართლებრივი ასპექტები ჯანდაცვის სისტემის დიგიტალიზაციის პირობებში, შეაფასოს საერთაშორისო (GDPR, HIPAA, 108-ე კონვენცია) და ეროვნული რეგულაციების შესაბამისობა თანამედროვე ტექნოლოგიურ გამოწვევებთან, გამოავლინოს პაციენტის კონფიდენციალურობის, ინფორმირებული თანხმობისა და კიბერუსაფრთხოების ძირითადი პრობლემები და შეიმუშაოს რეკომენდაციები სამედიცინო მონაცემთა დაცვითი მმართველობის გაუმჯობესებისთვის.

მეთოდოლოგია

სტატიაში გამოყენებულია დოკუმენტური და სამართლებრივი ანალიზის მეთოდი, რომელიც მოიცავს: საერთაშორისო რეგულაციების (GDPR, HIPAA, 108-ე კონვენცია) შედარებით განხილვას, საქართველოს კანონმდებლობის (პერსონალური მონაცემების დაცვა, ჯანმრთელობის დაცვის შესახებ კანონი, სამედიცინო საქმიანობის შესახებ კანონი) ანალიზს, WHO, OECD და სხვა ავტორიტეტული წყაროების შეფასებებს, COVID-19 პანდემიის მაგალითზე დიგიტალიზაციის დაჩქარების ეფექტის შესწავლას. მეთოდოლოგია ემყარება ეთიკური პრინციპების (ავტონომია, სამართლიანობა, უვნებლობა, ანგარიშვალდებულება) სისტემურ შეფასებას.

სამედიცინო მონაცემთა დაცვის ეთიკური ასპექტები

სამედიცინო ეთიკის ერთ-ერთი მთავარი პრინციპია პაციენტის მონაცემების კონფიდენციალურობის დაცვა. სამედიცინო საქმიანობის აღსრულებისას ჯანმრთელობის დაცვის პერსონალმა უნდა იხელმძღვანელოს ეთიკური ფასეულობებით – ადამიანის პატივისა

და ღირსების აღიარების, სამართლიანობის, თანაგრძნობის პრინციპებით („ჯანმრთელობის დაცვის შესახებ“ საქართველოს კანონი, 1997, მუხლი 30).

სამედიცინო ეთიკის მთავარი პრინციპია:

1. **ავტონომიის პრინციპი** – პაციენტს აქვს უფლება გააკონტროლოს, ვინ და რა მიზნით იყენებს მის პირად სამედიცინო მონაცემებს. ეს პრინციპი ეყრდნობა ადამიანის უფლებების დაცვას და თვითგამორკვევის თავისუფლებას (Beauchamp & Childress, 2019). საქართველოს კონსტიტუციის 15-ე მუხლი იცავს პირად ცხოვრებაში ჩარევისგან (საქართველოს პარლამენტი, 1995).
2. **უვნებლობის პრინციპი** – სამედიცინო მონაცემების უნებართვო გამჟღავნებამ ან ბოროტად გამოყენებამ შესაძლოა გამოიწვიოს ფსიქოლოგიური ზიანი, დისკრიმინაცია, სოციალური სტიგმა ან ეკონომიკური ზარალი (Gostin & Halabi, 2020). პერსონალურ მონაცემთა დაცვის ინსპექტორის ანგარიშები ხშირად მოიცავს შემთხვევებს, როდესაც მონაცემთა უნებართვო გამჟღავნებამ ზიანი მიაყენა მოქალაქეებს (პერსონალურ მონაცემთა დაცვის სამსახური, 2023).
3. **სამართლიანობის პრინციპი** – სამედიცინო ინფორმაციის ხელმისაწვდომობა უნდა დარეგულირდეს ისე, რომ უზრუნველყოფილი იყოს ყველა მოქალაქის თანაბარი უფლებები (Daniels, 2008). ჯანმრთელობის დაცვაზე თანაბარი წვდომის უფლება გათვალისწინებულია „ჯანმრთელობის დაცვის შესახებ“ საქართველოს კანონში (საქართველოს პარლამენტი, 1997, მუხლი 5).
4. **ინფორმირებული თანხმობის პრინციპი** – პაციენტის თანხმობის მოპოვების მოთხოვნა მისი მონაცემების დამუშავებაზე, („საექიმო საქმიანობის შესახებ“ საქართველოს კანონი, 2001, მუხლი 44, პუნქტი 1).
5. **მონაცემთა მინიმუზაციის პრინციპი** – მხოლოდ სამედიცინო დახმარების უზრუნველსაყოფად საჭირო ინფორმაციის შეგროვება (პერსონალურ მონაცემთა დაცვის სამსახური, 2023).
6. **გამჭვირვალობა** – პაციენტებს უნდა ჰქონდეთ მკაფიო ინფორმაცია იმასთან დაკავშირებით, თუ როგორ და ვინ იყენებს მათ მონაცემებს. გამჭვირვალობა ზრდის ნდობას და ამცირებს კონფლიქტებს (Nuffield Council on Bioethics, 2015). პერსონალურ მონაცემთა დაცვის ინსპექტორის ვებგვერდი უზრუნველყოფს მოქალაქეთა ინფორმირებულობას მონაცემთა დამუშავების წესების შესახებ (პერსონალურ მონაცემთა დაცვის სამსახური, 2023).
7. **პასუხისმგებლობა და ანგარიშვალდებულება** – ჯანდაცვის ორგანიზაციებს ეკისრებათ პასუხისმგებლობა, უზრუნველყონ მონაცემთა დაცვა და მზად იყვნენ აიღონ პასუხისმგებლობა დარღვევების შემთხვევაში (OECD, 2021).

2023 წელს მიღებული ცვლილებებით საქართველოს კანონი პერსონალურ მონაცემთა შესახებ აკონკრეტებს ჯანდაცვის დაწესებულებების ვალდებულებებს მონაცემთა უსაფრთხოების უზრუნველყოფის კუთხით (საქართველოს პარლამენტი, 2023).

სამედიცინო მონაცემების სამართლებრივი რეგულირება დიგიტალიზაციის პირობებში

საერთაშორისო დონეზე პერსონალური მონაცემების დაცვა რეგულირდება ისეთი აქტებით, როგორიცაა:

- **მონაცემთა დაცვის ზოგადი რეგულაცია (GDPR)** – ადგენს მკაცრ წესებს პერსონალური მონაცემების, მათ შორის სამედიცინო მონაცემების დამუშავებისთვის და არეგულირებს მონაცემთა ტრანსსასაზღვრო გადაცემას (European Council, 2024).
- **ჯანმრთელობის დაზღვევის პორტაბელურობისა და ანგარიშვალდებულების აქტი (HIPAA, აშშ)** – არეგულირებს ჯანმრთელობის ინფორმაციისა და პაციენტის უფლებების დაცვას ციფრულ გარემოში (CDC, 2024).
- **ეროვნული რეგულაციები** – თითოეული ქვეყანა შეიმუშავებს საკუთარ კანონებსა და რეგულაციებს, რომლებიც არეგულირებს ჯანმრთელობის მონაცემების ციფრულ სისტემებში დამუშავებას.

108-ე კონვენცია იყო პირველი იურიდიულად სავალდებულო საერთაშორისო დოკუმენტი პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის სფეროში (კონვენცია, 2025). რის შედეგად ის საქართველოს კანონმდებლობის ნაწილი გახდა.

ელექტრონული მმართველობის სფეროში ძირითადი სამართლებრივი გამოწვევები მოიცავს პერსონალური მონაცემების დაცვას, კიბერუსაფრთხოებას, საიმედო ციფრული იდენტიფიკაციის სისტემის შექმნას, ქვეყნებს შორის მონაცემების გაცვლის რეგულირებას, სახელმწიფო ორგანოების გამჭვირვალობისა და ანგარიშვალდებულების უზრუნველყოფას, იურიდიულ პროცესებში ელექტრონული სახით მტკიცებულებების გამოყენებას. მნიშვნელოვანია, რომ კანონმდებლობა იყოს მოქნილი და სწრაფად მოერგოს ტექნოლოგიურ ცვლილებებს, რაც უზრუნველყოფს ელექტრონული მმართველობის ეფექტურ და უსაფრთხო ფუნქციონირებას.

სამედიცინო ინფორმაციის ელექტრონული მართვის დანერგვა

სამედიცინო მონაცემების დამუშავების ელექტრონულ ფორმატში დანერგვა აუცილებელი გახდა ჯანდაცვის სისტემის ეფექტურობისა და ხარისხის გასაუმჯობესებლად. ელექტრონული სისტემები შესაძლებელს ხდის სამედიცინო ინფორმაციის შეგროვების, შენახვისა და დამუშავების ავტომატიზირებას, რაც აჩქარებს მონაცემებზე წვდომას და აუმჯობესებს პაციენტთა სამედიცინო მომსახურებას. დიგიტალიზაცია ამარტივებს სამედიცინო ინფორმაციის გაცვლას დაწესებულებებს შორის, რაც გადამწყვეტია გადაუდებელი დახმარებისა და მკურნალობის უწყვეტობის უზრუნველსაყოფად. ელექტრონული სამედიცინო ჩანაწერები ეხმარება მედიცინის სფეროს წარმომადგენლებს მიიღონ უფრო ინფორმირებული გადაწყვეტილებები, ამცირებენ შეცდომების ალბათობას და აუმჯობესებენ დიაგნოსტიკისა და მკურნალობის ხარისხს. გარდა ამისა, ასეთი სისტემები ხელს უწყობს რესურსების ეფექტურ მართვას, რაც უზრუნველყოფს მედიკამენტებისა და აღჭურვილობის ოპტიმალურ განაწილებას. ელექტრონული მმართველობის დანერგვა საშუალებას იძლევა შესრულდეს პერსონალური მონაცემების დაცვის სამართლებრივი მოთხოვნები, ასევე, გაუმჯობესდეს კონტროლი ჯანდაცვის სტანდარტებთან შესაბამისობაზე.

COVID-19-ის პანდემიამ მნიშვნელოვნად დააჩქარა ელექტრონული სამედიცინო სისტემების დანერგვა, მათ შორის პაციენტის ჯანმრთელობის დისტანციური მონიტორინგი (Wosik et al., 2020). ფიზიკური ურთიერთქმედების შეზღუდვით და კონტაქტის მინიმუმამდე შემცირების აუცილებლობით, ჯანმრთელობის ელექტრონული მონაცემების მართვა გახდა არა მხოლოდ მოსახერხებელი, არამედ აუცილებელი ინსტრუმენტი სამედიცინო მომსახურეობის გაწევის უწყვეტობის უზრუნველსაყოფად. კერძოდ, დისტანციური კონსულტაციის პლატფორმების გამოყენებამ ექიმებს საშუალება მისცა გააგრძელონ პაციენტებზე ზრუნვა ინფექციის რისკის გარეშე. თუმცა, ტექნოლოგიის ამ დაჩქარებულმა მიღებამ ახალი გამოწვევები წარმოშვა პერსონალური მონაცემების დაცვაში. პანდემიის პერიოდში მოქალაქეთა ჯანმრთელობის მდგომარეობის შესახებ დიდი მოცულობის მონაცემების დამუშავება ხშირად მიმდინარეობდა შეზღუდული ინფრასტრუქტურისა და დიგიტალიზაციის დაჩქარებული ტემპის პირობებში. ამან გამოიწვია მონაცემთა უნებართვო გამჟღავნების რისკის ზრდა, რაც მოითხოვდა პაციენტების კონფიდენციალურობის უფლებების დაცვისა და ეთიკის სტანდარტების დანერგვის მექანიზმების სწრაფ გაუმჯობესებას. მეორე მხრივ, შექმნილმა გარემოებებმა ახალ რეგულაციათა შექმნას მისცა ბიძგი, რაც გადაუდებელ შემთხვევებში სამედიცინო მონაცემების ხელმისაწვდომობასა და დამუშავებას აადვილებს. რიგ ქვეყნებში, როგორცაა ევროპის სახელმწიფოები, აშშ და დიდი ბრიტანეთი, შემოიღეს დროებითი მექანიზმები, რომლებიც პანდემიასთან ბრძოლისთვის პაციენტის ინფორმირებულ თანხმობაზე დაფუძნებულ მონაცემთა დამუშავების პროცესს ამარტივებს.

ამრიგად პანდემიამ კატალიზატორის როლი შეასრულა სამედიცინო მონაცემების ელექტრონული მართვის განვითარებაში და იმოქმედა არა მხოლოდ სამედიცინო პრაქტიკაზე, არამედ ჯანდაცვის სექტორში პერსონალური მონაცემების რეგულირებასა და დაცვაზე, ასევე ხაზი გაუსვა რეგულაციების მოქნილობის მნიშვნელობას საგანგებო სიტუაციებში.

აქედან გამომდინარე, ჯანდაცვის სისტემის დიგიტალიზაცია აადვილებს ჯანმრთელობის ინფორმაციის ხელმისაწვდომობას, გამჭვირვალობას და უსაფრთხოებას, რაც აუმჯობესებს ჯანდაცვის საერთო ხარისხს.

სამედიცინო მონაცემების ელექტრონული დამუშავება და მართვა წარმოშობს ახალ ეთიკურ დილემებს, როგორც კონფიდენციალურობისა და საზოგადოებრივი ინტერესების დაბალანსების აუცილებლობა (მაგ. ეპიდემიოლოგიური მონიტორინგის ან სამეცნიერო კვლევის დროს). ასევე, დიდი რაოდენობით მონაცემების შეგროვება და ანალიზი შესაძლებელს ხდის დაავადების გავრცელების ტენდენციების იდენტიფიცირებას და მათთან ბრძოლის ეფექტური სტრატეგიების შემუშავებას, მაგრამ ეს აგრეთვე ზრდის პაციენტის კონფიდენციალურობის დარღვევის რისკს.

გარდა ამისა, ჯანდაცვის ციფრული მართვა და განვითარება მოითხოვს პასუხისმგებლობის საზღვრების მკაფიო განსაზღვრას სხვადასხვა დაინტერესებულ მხარეებს შორის - სამთავრობო უწყებებს, ჯანდაცვის დაწესებულებებს, კერძო კომპანიებსა და ასევე პაციენტებს შორის. ხელოვნური ინტელექტისა და ციფრული ალგორითმების გამოყენება სამედიცინო მონაცემების ანალიზისას უნდა ემყარებოდეს ეთიკურ სტანდარტებს. მნიშვნელოვანია, რომ ეს ტექნოლოგიები იყოს გამოყენებული გამჭვირვალედ, პაციენტების უფლებების დარღვევისა და დისკრიმინაციული გადაწყვეტილებების გარეშე (ნამორაძე, 2024).

ამრიგად, სამედიცინო ინფორმაციის დაცვა მოითხოვს არა მხოლოდ კონფიდენციალურობის არსებული რეგულაციების მკაცრ დაცვას, არამედ ახალი ეთიკური სტანდარტების შემუშავებას, რომელიც ითვალისწინებს თანამედროვე დროის ტექნოლოგიურ რეალობას.

სამედიცინო მონაცემების დამუშავების ელექტრონული მენეჯმენტის უარყოფითი მხარეები

მრავალი უპირატესობის მიუხედავად, სამედიცინო მონაცემების დამუშავების ელექტრონული მართვის განხორციელებას ასევე აქვს გარკვეული უარყოფითი მხარეები:

ერთ-ერთი მთავარი რისკი კიბერშეტევებისა და მონაცემთა უნებართვო გამჟღავნების საფრთხეა. კიბერშეტევები კვლავაც გამოწვევად რჩება (Weiss, 2025), სამედიცინო ინფორმაცია არის ყველაზე დელიკატური ინფორმაცია და მისმა უნებართვო გამჟღავნებამ, შეიძლება გამოიწვიოს სერიოზული შედეგები, მათ შორის კონფიდენციალურობის დარღვევა და მონაცემთა ბოროტად გამოყენება. ავტომატიზაციის მიუხედავად, მონაცემთა დამუშავების შეცდომები და შესაძლო არაავტორიზებული წვდომა პრობლემად რჩება, ხოლო ტექნოლოგიაზე დამოკიდებულება ზრდის რისკებს სისტემის გაუმართაობის შემთხვევაში. ახალ სისტემებთან მუშაობისას პერსონალის გამოუცდელობამ ასევე შეიძლება შეამციროს მათი გამოყენების ეფექტურობა.

აგრეთვე უარყოფით მხარეს წარმოადგენს ელექტრონული სისტემების შემუშავების, დანერგვისა და შენარჩუნების მაღალი ფინანსური ხარჯები, რაც შეიძლება იყოს ბარიერი მცირე სამედიცინო დაწესებულებებისთვის ჯანდაცვის სისტემაში.

ამრიგად, მნიშვნელოვანი უპირატესობების მიუხედავად, როგორც სამედიცინო სერვისების გაზრდილი ეფექტურობა და ხელმისაწვდომობა, ელექტრონული მმართველობის დანერგვა მოითხოვს კომპლექსურ მიდგომას ამ რისკების გადასაჭრელად. აუცილებელია მონაცემთა საიმედო დაცვის უზრუნველყოფა, პერსონალის ტრენინგის ჩატარება და სისტემების რეგულარულად განახლება და შენარჩუნება ჯანდაცვის სექტორში ციფრულ ტექნოლოგიებზე გადასვლასთან დაკავშირებული პოტენციური საფრთხეებისა და პრობლემების შესამცირებლად.

პაციენტის ინფორმირებულ თანხმობასთან დაკავშირებული საკითხები სამედიცინო მონაცემების ელექტრონულად დამუშავების პრობლემის ერთ-ერთი ძირითადი ასპექტია პაციენტის თანხმობის საკითხი და მისი ინფორმირებულობა პერსონალური მონაცემების დამუშავების პროცესის შესახებ. სამედიცინო სერვისების დიგიტალიზაციის პროცესში, სადაც ინფორმაციის უმეტესი ნაწილი გროვდება და მუშავდება ელექტრონული სისტემების მეშვეობით, ძალზედ მნიშვნელოვანია იმის უზრუნველყოფა, რომ პაციენტებმა მისცენ

ინფორმირებული და ნებაყოფლობითი თანხმობა მათი პერსონალური მონაცემების დამუშავებაზე (ვერულავა, 2018).

„ინფორმირებული თანხმობა წინ უნდა უსწრებდეს ადამიანის ბიოსამედიცინო კვლევაში ჩართვის პროცესს. კვლევაში შესაძლო ჩართულ პირს წინასწარ უნდა მიეწოდოს ინფორმაცია კვლევის მიზნების, მეთოდების, მოსალოდნელი შედეგების, კვლევის რისკისა და მასთან დაკავშირებული დისკომფორტის შესახებ“ (დულაშვილი, 2022).

ერთ-ერთი მთავარი პრობლემა არის ის, რომ პაციენტებს ყოველთვის ბოლომდე არ ესმით, რას ეთანხმებიან და რა მონაცემები მუშავდება. თანხმობა ხშირად ხდება რთული სამართლებრივი ფორმებითა და შეთანხმებებით, რომლებიც ძნელად გასაგებია ფართო აუდიტორიისთვის. ამან შეიძლება გამოიწვიოს სიტუაცია, როდესაც პაციენტებმა არ იციან რა მონაცემები გროვდება მათ შესახებ, როგორ იქნება გამოყენებული და ვის ექნება მასზე წვდომა. მონაცემთა კონფიდენციალურობის უფლებებისა და დაცვის არარსებობამ შეიძლება შეამციროს ნდობა ციფრული ჯანდაცვის სისტემების მიმართ. არსებული საკანონმდებლო ღონისძიებები, როგორიცაა ინფორმირებული თანხმობის მოთხოვნა, საჭიროებს მოდიფიკაციას თანამედროვე ტექნოლოგიების კონტექსტში, რაც იძლევა მონაცემთა შეგროვების და დამუშავების საშუალებას (კარტოზია და სხვ., 2018).

ამ საკითხების გადასაჭრელად აუცილებელია შემუშავდეს უფრო მარტივი და მკაფიო თანხმობის მექანიზმები, ასევე საგანმანათლებლო პროგრამები, რათა გაიზარდოს პაციენტის ცნობიერება მათი უფლებების შესახებ. მნიშვნელოვანია, პაციენტები არამარტო დაეთანხმონ მონაცემთა დამუშავებას, არამედ ადვილად გაიგონ, თუ მათი რა მონაცემები მუშავდება, როგორ არის ისინი დაცული და როგორ გააუქმონ თანხმობა საჭიროების შემთხვევაში.

პაციენტების ინფორმირების მიზნით მათი კონფიდენციალურობის უფლებებისა და მონაცემთა დაცვის შესახებ საჭიროა უფრო გამჭვირვალე და ხელმისაწვდომი მექანიზმების დანერგვა რაც ხელს შეუწყობს ელექტრონული ჯანდაცვის მიმართ ნდობის გაზრდას, ასევე პერსონალური მონაცემების დამუშავების ეთიკური პრაქტიკის გაუმჯობესებას (ვერულავა, 2023).

საქართველოში ერთ-ერთი მთავარი პრობლემა არის ციფრული უნარების განვითარების არადამაკმაყოფილებელი დონე მოსახლეობაში (საქართველოს ეკონომიკისა და მდგრადი განვითარების სამინისტრო, 2024), განსაკუთრებით ხანდაზმულებში. ეს ზღუდავს წვდომას თანამედროვე ჯანდაცვის სერვისებზე, როგორიცაა ონლაინ კონსულტაციები და ელექტრონული რეცეპტები. მიუხედავად პერსონალური მონაცემების დაცვის სფეროში კანონმდებლობის მიღებისა და საერთაშორისო ხელშეკრულებების რატიფიცირებისა, სამედიცინო მონაცემთა დამუშავების სისტემისადმი ნდობის დონე რჩება დაბალი, რაც ზღუდავს ელექტრონული სერვისების ეფექტურ გამოყენებას ჯანდაცვაში.

ევროკავშირის უმეტეს ქვეყნებში ციფრული უნარების განვითარების შედარებით მაღალი დონე აღინიშნება მოსახლეობაში, თუმცა არის პრობლემები, რომლებიც დაკავშირებულია ინფორმაციის ხელმისაწვდომობასთან მოსახლეობის გარკვეული ჯგუფებისთვის, როგორიცაა ხანდაზმული და შეზღუდული შესაძლებლობის მქონე პირები. ევროპის ქვეყნებში აქტიურად მუშაობენ პაციენტთა ინფორმირებულობის გაუმჯობესებისთვის მათი მონაცემთა დაცვის უფლებების შესახებ, რასაც მხარს უჭერს ისეთი კანონმდებლობა, როგორიცაა GDPR. თუმცა, სამედიცინო მონაცემების გამოყენებისას თანხმობის და გამჭვირვალობის პირობების გაგებასთან დაკავშირებული პრობლემები რჩება, რაც ამცირებს სისტემისადმი ნდობის დონეს.

მიუხედავად იმისა, რომ გაერო დადებითად აფასებს შეზღუდული შესაძლებლობების მქონე პირთა უფლებების დაცვის მიმართულებით პოლიტიკის განვითარების პროგრესს და ხაზს უსვამს მისი განხორციელების მნიშვნელობას საქართველოში (OHCHR, 2023), მეტი ძალისხმევაა საჭირო ბარიერების აღმოსაფხვრელად, იმის უზრუნველსაყოფად, რომ ჯანმრთელობის შესახებ ინფორმაცია და სერვისები ხელმისაწვდომი იყოს მოსახლეობის ყველა სეგმენტისთვის, მათ შორის შეზღუდული შესაძლებლობის მქონე პირებისთვის.

დასკვნა

ჯანდაცვის მართვის სისტემის დიგიტალიზაცია ზრდის სამედიცინო სერვისების ხელმისაწვდომობას და ხარისხს, მაგრამ ქმნის რისკებს, რომლებიც დაკავშირებულია პერსონალური მონაცემების დაცვასთან. ელექტრონული მმართველობის გამართული ფუნქციონირებისთვის მნიშვნელოვანია მონაცემთა კონფიდენციალურობის დაცვა და მათი სწრაფი გაცვლის აუცილებლობა. ძირითადი საკითხები მოიცავს კიბერშეტევებს, პაციენტების ინფორმირებულობის ნაკლებობას და კომპლექსურ მარეგულირებელ ჩარჩოებს.

რეკომენდებულია საკანონმდებლო ბაზის გაუმჯობესება, ციფრული ტექნოლოგიების გამოყენების უნარების გაზრდა და კიბერუსაფრთხოების ზომების გაძლიერება. ასევე საჭიროა საერთაშორისო თანამშრომლობა მონაცემთა დაცვის სფეროში და კანონმდებლობის ადაპტაცია ტექნოლოგიურ განვითარებასთან. საიმედო სამედიცინო მონაცემთა მართვის სისტემის შექმნა გაზრდის პაციენტების ნდობას და უზრუნველყოფს მათი პირადი ინფორმაციის დაცვას.

გამოყენებული ლიტერატურა

დულაშვილი, გ. (2022). სამედიცინო სამართლისა და მენეჯმენტის ჟურნალი, 1(2022), 125 და მომდევნო გვერდები.

ვერულავა, თ. (2018). სამედიცინო მომსახურებაზე პაციენტის ინფორმირებული თანხმობა საქართველოში. III საერთაშორისო სამეცნიერო კონფერენციის „გლობალიზაციის გამოწვევები ეკონომიკასა და ბიზნესში“ შრომების კრებული. ივანე ჯავახიშვილის სახელობის თბილისის სახელმწიფო უნივერსიტეტი. 134-139.

ვერულავა, თ. (2023). სამედიცინო მომსახურებაზე ინფორმირებული თანხმობა და პაციენტები. აკაკი წერეთლის სახელმწიფო უნივერსიტეტის მოამბე. 22 (2): 195-210.

კარტოზია, დ., რევია, ნ., ედიბერიძე, მ., შალამბერიძე, ა., ლიპარტია, თ., ფირცხალაიშვილი, ი., ახმდინაშვილი, ა. (2018). ქირურგიული ჩარევის შესახებ ინფორმირებული თანხმობა. ჯანდაცვის პოლიტიკა, ეკონომიკა და სოციოლოგია, 2. <https://heconomic.cu.edu.ge/index.php/healthecosoc/article/view/6809>

ნამორაძე, ე. (2024). მედიცინის სფეროში ხელოვნური ინტელექტის დანერგვა. ჯანდაცვის პოლიტიკა, ეკონომიკა და სოციოლოგია, 8(1).

საქართველოს პარლამენტი. (1995). საქართველოს კონსტიტუცია.

საქართველოს პარლამენტი. (1997). საქართველოს კანონი „ჯანმრთელობის დაცვის შესახებ“ (№29980). სსიპ სამართლებრივი აქტების ოფიციალური გამოქვეყნების სისტემა „მაცნე“.

საქართველოს პარლამენტი. (2023). საქართველოს კანონი „პერსონალურ მონაცემთა დაცვის შესახებ“ (ცვლილებები 2023). სსიპ სამართლებრივი აქტების ოფიციალური გამოქვეყნების სისტემა „მაცნე“.

საქართველოს ციფრული ეკონომიკისა და საინფორმაციო საზოგადოების განვითარების 2025–2030 წლების ეროვნული სტრატეგია. (2024).

პერსონალურ მონაცემთა დაცვის სამსახური. (2023). პერსონალურ მონაცემთა დაცვის წლიური ანგარიში.

პერსონალურ მონაცემთა დაცვის სამსახური. (2023). პერსონალურ მონაცემთა დაცვის წლიური ანგარიში 2022. სსიპ სახელმწიფო ინსპექტორის სამსახური.

პერსონალურ მონაცემთა დაცვის სამსახური. (2025). მოქალაქეთა ინფორმირებულობა მონაცემთა დამუშავების წესების შესახებ.

„პერსონალური მონაცემების ავტომატური დამუშავებისას ფიზიკური პირების დაცვის შესახებ“ კონვენცია. (2025). სსიპ „საქართველოს საკანონმდებლო მაცნე“.

„საექიმო საქმიანობის შესახებ“ საქართველოს კანონის 44-ე მუხლის 1-ლი პუნქტი. (2001). სსიპ „საქართველოს საკანონმდებლო მაცნე“.

„ჯანმრთელობის დაცვის შესახებ“ საქართველოს კანონის 30-ე მუხლი. (1997). სსიპ „საქართველოს საკანონმდებლო მაცნე“.

Beauchamp, T.L., Childress, J.F. (2019). Principles of biomedical ethics (8th ed.). Oxford University Press.

CDC. (2024, September 10). Health Insurance Portability and Accountability Act of 1996 (HIPAA). Centers for Disease Control and Prevention.

Countries in the European Region commit to disability-inclusive health systems and societies. (n.d.). World Health Organization.

Daniels, N. (2008). Just health: Meeting health needs fairly. Cambridge University Press.

Digital solutions during the pandemic. (n.d.). European Commission.

European Council. (2024, June 13). The General Data Protection Regulation. Consilium.

Gostin, L.O., Halabi, S.F. (2020). Health data and privacy in the digital era. JAMA, 323(3), 211–212.

Nuffield Council on Bioethics. (2015). The collection, linking and use of data in biomedical research and health care: Ethical issues.

OECD. (2021). OECD recommendation on health data governance. Organisation for Economic Co-operation and Development.

Weiss, E. (2025, March 13). New cybersecurity policies could protect patient health data. Health-ISAC.

Wosik, J., Fudim, M., Cameron, B., Gellad, Z. F., Cho, A., Phinney, D., Curtis, S., Roman, M., Poon, E. G., Ferranti, J., Katz, J. N., Tcheng, J. (2020). Telehealth transformation: COVID-19 and the rise of virtual care. Journal of the American Medical Informatics Association, 27(6), 957–962.