ორგანიზაციის სახელი ობიექტი ან განყოფილება		პოლიტიკა **ინფორმაციის უსაფრთხოებისა და წვდომის კონტროლის პოლიტიკა**	
დოკუმენტის ID	DIG-POL-001	**ვერსია**	1.0
სტატუსი	ცარიელი ფორმა, მოსარგებად	**გამოშვების თარიღი**	
გადახედვის თარიღი		**ანაცვლებს**	
პასუხისმგებელი		**დაამტკიცა**	
ხელმოწერა			

Standards › › Standard 2APolicies

პოლიტიკა · DIG-POL-001 · ვერსია 1.1 · დამტკიცებულია ASF ექსპერტთა კომიტეტის მიერ

მხარს უჭერს: 2A.4

მოკლედ

- თითოეულ პირს მიანიჭეთ წვდომა მხოლოდ იმ ჯანმრთელობის ინფორმაციაზე, რომელიც მათი სამუშაოსთვისაა საჭირო.
- გამოიყენეთ უნიკალური ანგარიში და ძლიერი პაროლი. არასოდეს გაუზიაროთ თქვენი ანგარიში.
- ეკრანი ჩაკეტეთ სამუშაო სადგურიდან წასვლისას.
- ნებისმიერი ეჭვმიტანილი დარღვევა დაუყოვნებლივ აცნობეთ დარღვევის პროცედურით.
- ყოველ კვარტალში ხელახლა იხილეთ, ვის აქვს წვდომა, და წვდომა მოხსენით პირის წასვლისას.
- დაუყოვნებლივ შეაჩერეთ და მიიღეთ დახმარება, თუ: ეჭვობთ, რომ პაციენტის ინფორმაცია ნანახია, კოპირებულია ან არასწორ პირს გაეგზავნა. შეაჩერეთ და დაუყოვნებლივ აცნობეთ.

1. 1. მიზანი

პაციენტის ჯანმრთელობის ინფორმაციის დაცვა არაავტორიზებული წვდომის, დაკარგვის, ცვლილებისა და გამჟღავნებისგან, პრაქტიკული უსაფრთხოების ზომების გამოყენებით [E-006, EC].

2. 2. სფერო

ვრცელდება	ყველა თანამშრომელი, სტუდენტი, კონტრაქტორი და ყველა, ვისაც აქვს წვდომა დაწესებულების სისტემებსა ან ქაღალდის ჩანაწერებზე
ადგილები	ყველა ობიექტი, სისტემა, მოწყობილობა და ქაღალდის ჩანაწერი
როდის	ყოველთვის
არ ვრცელდება	კლინიკური გადაწყვეტილებები ინფორმაციის გამოყენების შესახებ, რომლებიც კონფიდენციალურობისა და ჩანაწერების პოლიტიკით რეგულირდება

3. 3. განმარტებები

ტერმინი	მნიშვნელობა
ჯანმრთელობის ინფორმაცია	ნებისმიერი ინფორმაცია, რომელიც პაციენტს იდენტიფიცირებს და მის მოვლას უკავშირდება
წვდომის კონტროლი	წესები და ინსტრუმენტები, რომლებიც განსაზღვრავს, ვინ შეიძლება ნახოს, შეცვალოს ან გაუზიაროს ინფორმაცია
დარღვევა	ჯანმრთელობის ინფორმაციაზე ნებისმიერი არაავტორიზებული წვდომა, დაკარგვა, გამჟღავნება ან ცვლილება

4. 4. საფუძვლები

პაციენტები ჯანმრთელობის ინფორმაციას აზიარებენ იმ პირობით, რომ ის კონფიდენციალური დარჩება. დარღვევამ შეიძლება ზიანი, შფოთვა და ნდობის დაკარგვა გამოიწვიოს. კრიტერიუმი 2A.4 მოითხოვს წვდომის კონტროლსა და დარღვევაზე რეაგირების გეგმას, რომელსაც დაწესებულება თავისი რესურსებით რეალურად შეძლებს.

5. 5. პასუხისმგებლობები

როლი	პასუხისმგებლობა	კომპეტენცია

IT ხელმძღვანელი	ადგენს წვდომის კონტროლს; ატარებს წვდომის გადახედვას; მართავს უსაფრთხოების ინსტრუმენტებს	IT უსაფრთხოების კომპეტენცია
მონაცემთა დაცვის ხელმძღვანელი	იძლევა იურიდიულ რჩევას; ხელმძღვანელობს დარღვევის შეფასებას; აწარმოებს დარღვევების ჟურნალს	მონაცემთა დაცვის კომპეტენცია
ხაზოვანი მენეჯერები	მოითხოვეთ და დაამტკიცეთ წვდომა; აცნობეთ IT-ს, როდესაც პირი ცვლის როლს ან წავა	მენეჯმენტის სწავლება
ყოველი მომხმარებელი	დაიცავით ანგარიში და მოწყობილობა; აცნობეთ დარღვევებს; მიჰყევით წესებს	ინდუქცია და ყოველწლიური სწავლება

6. 6. მასალები და აღჭურვილობა

ერთეული	მოთხოვნა	პირობა
წვდომის წესები (როლებზე დაფუძნებული სია)	დაწერილია თითო როლზე	ყოველ კვარტალში ხელახლა იხილება
ძლიერი პაროლის სტანდარტი	სიგრძე და წესები განსაზღვრულია IT ხელმძღვანელის მიერ (EC)	იძულებით ახორციელებს სისტემა
ეკრანის ჩაკეტვა	დაყენებულია ჩაკეტვაზე უმოქმედობის მოკლე პერიოდის შემდეგ (EC)	ყველა სამუშაო სადგურზე
დარღვევაზე რეაგირების გეგმა (DIG-SOP-001)	მიმდინარე	ხელმისაწვდომია დარღვევაზე მომუშავე ჯგუფისთვის

7. 7. უსაფრთხოება

- პაროლები ქაღალდზე სამუშაო სადგურთან არ ჩაწეროთ.
- ჯანმრთელობის ინფორმაცია პირად ანგარიშებზე ან დაუმტკიცებელ სერვისებზე ელფოსტით არ გაგზავნოთ.

- ქაღალდის ჩანაწერები უყურადღებოდ არ დატოვოთ. გამოიყენეთ დაკეტილი საცავი.

8. 8. დაწყებამდე

- შეამოწმეთ, რომ თქვენი წვდომა სწორია თქვენი როლისთვის.
- შეამოწმეთ, რომ მოწყობილობა ჩაკეტილია, როცა უყურადღებოდ ხართ.

9. 9. პროცედურა

ეტაპი 1. დააყენეთ წვდომა როლის მიხედვით.

- თითოეული როლისთვის შეადგინეთ წვდომის სია: რა ინფორმაცია, რა სისტემები, რა ქმედებები (ნახვა, შეცვლა, ექსპორტი).
- წვდომა მიანიჭეთ როლის საფუძველზე და არა პირის.
- თითოეული მომხმარებლისთვის გამოიყენეთ უნიკალური ანგარიში.

მთავარი დებულება: როლებზე დაფუძნებული წვდომა ზღუდავს, რის ნახვაც შეუძლია პირს, მისი სამუშაოს საჭიროებებით.

ეტაპი 2. დაიცავით ანგარიშები და მოწყობილობები.

- გამოიყენეთ ძლიერი პაროლი და მრავალფაქტორიანი ავტორიზაცია, სადაც სისტემა საშუალებას იძლევა.
- ეკრანი ჩაკეტეთ წასვლისას. გაზიარებული მოწყობილობებიდან გამოდით.
- მოწყობილობები დაშიფრული შეინახეთ იქ, სადაც საავადმყოფოს ამის საშუალება აქვს (EC).

მთავარი დებულება: დარღვევების უმრავლესობა იწყება მოპარული ან გაზიარებული ანგარიშით.

ეტაპი 3. წვდომა ყოველ კვარტალში ხელახლა შეამოწმეთ.

- IT ხელმძღვანელი და ხაზოვანი მენეჯერები ხელახლა იხილავენ მომხმარებლების სიასა და მათ წვდომას.
- მოხსენით წვდომა, რომელიც აღარ არის საჭირო. მოხსენით წვდომა იმავე დღეს, როდესაც პირი წავა.
- აღრიცხეთ გადახედვის თარიღი და ცვლილებები.

მთავარი დებულება: წვდომა, რომელიც არასოდეს იხილება, იზრდება მანამ, სანამ არავინ იცის, ვის შეუძლია ჩანაწერების ნახვა.

ეტაპი 4. აკონტროლეთ და აღრიცხეთ წვდომა.

- ელექტრონულ ჩანაწერებზე წვდომის ჟურნალები აწარმოეთ, სადაც სისტემა საშუალებას იძლევა.
- ყოველთვიურად შეამოწმეთ უჩვეულო წვდომა (მაგალითად, იმ პაციენტების ჩანაწერები, რომლებიც პირის მოვლაში არ არიან).

მთავარი დებულება: ჟურნალები გვიჩვენებს, ვინ ნახა ჩანაწერი, რაც აუცილებელია დარღვევის ეჭვის შემთხვევაში.

ეტაპი 5. ქაღალდის ჩანაწერები დაიცავით.

- ქაღალდის ჩანაწერები შეინახეთ დაკეტილ კარადებში, კონტროლირებადი გასაღებებით.
- აკონტროლეთ ჩანაწერების საწყობიდან გატანა.
- ქაღალდის ჩანაწერები განადგურდეს მხოლოდ დამტკიცებული განადგურების პროცესით.

მთავარი დებულება: ქაღალდის დარღვევები ხდება მაგიდებსა და მანქანებში დატოვებული ჩანაწერებით.

ეტაპი 6. ნებისმიერი დარღვევა დაუყოვნებლივ აცნობეთ.

- დაუყოვნებლივ აცნობეთ თქვენს ხაზოვან მენეჯერსა და მონაცემთა დაცვის ხელმძღვანელს, DIG-SOP-001-ის გამოყენებით.
- არ სცადოთ მარტო გამოძიება ან რაიმეს წაშლა.

მთავარი დებულება: ადრეული შეტყობინება ზიანს ზღუდავს და მოითხოვს დარღვევის პროცედურა.

10. 10. გადაწყვეტილების წერტილები

- თუ დარღვევა დადასტურდება, რომ ბევრ პაციენტს ეხება, აღმასრულებელი დირექტორი წყვეტს, აცნობოს თუ არა მარეგულირებელ ორგანოს და პაციენტებს, როგორც კანონი მოითხოვს (EC).

11. 11. განსაკუთრებული სიტუაციები

სიტუაცია	მოქმედება
დისტანციური მუშაობა	გამოიყენეთ მხოლოდ დამტკიცებული მოწყობილობები და კავშირები. პირად მოწყობილობებზე ჯანმრთელობის ინფორმაცია არ შეინახოთ, თუ IT ხელმძღვანელი არ დაამტკიცებს (EC).
მესამე მხარის სისტემები	კონტრაქტებში უნდა განისაზღვროს უსაფრთხოების ვალდებულებები და დარღვევის შეტყობინების ვადები (EC).

12. 12. ესკალაცია

- დარღვევები დაუყოვნებლივ მიდის მონაცემთა დაცვის ხელმძღვანელთან, და იმავე დღეს აღმასრულებელ დირექტორთან.

13. 13. მონიტორინგი

მაჩვენებელი	სამიზნე	სიხშირე	პასუხისმგებელი	თუ არ შესრულდა
წვდომის გადახედვები ყოველ კვარტალში სრულდება	100%	ყოველკვარტალური	IT ხელმძღვანელი	ესკალაცია მთავარ აღმასრულებელთან
წვდომა მოხსნილია იმავე დღეს, როდესაც პირი წავა	100%	თვიური ნიმუში	HR ხელმძღვანელი	გადახედვა და შესწორება
დარღვევები ეცნობება აღმოჩენიდან 24 საათში	100%	ყოველთვიურად	მონაცემთა დაცვის ხელმძღვანელი	შეტყობინების დაგვიანების გადახედვა

14. 14. ჩანაწერები

ჩანაწერი	ინახება	შენახვის ვადა
წვდომის გადახედვის ჩანაწერი	IT ფაილი	დაწესებულების ჩანაწერების პოლიტიკით დადგენილი წლები
დარღვევების ჟურნალი	მონაცემთა დაცვის ფაილი	დაწესებულების ჩანაწერების პოლიტიკით დადგენილი წლები

15. 15. ტრენინგი

- ყველა თანამშრომელი იღებს სწავლებას ინფორმაციის უსაფრთხოებაში ინდუქციისას და ყოველწლიურად (EC).
- IT და მონაცემთა დაცვის პერსონალი იღებს სპეციალურ სწავლებას (EC).

16. 16. დაკავშირებული დოკუმენტები

ID	სათაური	გამოყენება
DIG-SOP-001	პაციენტის მონაცემთა დარღვევაზე რეაგირების პროცედურა	გამოიყენება დარღვევის შემთხვევაში
DIG-FRM-001	დარღვევაზე რეაგირების ტესტის ჩანაწერი	ტესტის ჩანაწერი
REC-POL-001	ჩანაწერების მართვა და შენახვა	შენახვა და განადგურება
SOP-087	კონფიდენციალურობის პოლიტიკა (ზოგადი)	კონფიდენციალურობის ვალდებულებები
SOP-108	კონფიდენციალურობის სტანდარტი (ზოგადი)	პირადი ცხოვრების დაცვის ვალდებულებები

17. 17. მტკიცებულებები

მითითება	შენიშვნა
E-006	ASF Policy Framework v1.2. ადაპტირებული.
E-009	ASF ექსპერტთა კომიტეტის კონსენსუსი. პაროლის, დაშიფვრისა და ჟურნალირების წესები განსაზღვრავს IT ხელმძღვანელი და მოწმდება ეროვნულ მონაცემთა დაცვის კანონთან შესაბამისობაზე.

18. 18. ცვლილებების ისტორია

ვერსია	თარიღი	რა შეიცვალა	დამტკიცება
1.0	დამტკიცების თარიღი	პირველი ვერსია ადაპტირებულია ASF პოლიტიკებიდან 37 და 71	დამტკიცებულია ASF ექსპერტთა კომიტეტის მიერ
1.1	დამტკიცების თარიღი	შიდა ხარისხის მიმოხილვა: შესწორდა ჯვარედინი მითითებები, სტატუსის ფორმულირებები და დოკუმენტების კონტროლი	დამტკიცებულია ASF ექსპერტთა კომიტეტის მიერ

19. წყაროები

Accréditation Sans Frontières (2026). ASF Policy Framework v1.2. (E-006)

Accréditation Sans Frontières (2026). ASF Expert Committee consensus on Standard 1. (E-009)