ორგანიზაციის დასახელება დაწესებულება ან სტრუქტურული ერთეული	დოკუმენტი **IT და მონაცემთა უსაფრთხოების პოლიტიკა**		
დოკუმენტის ID	IT-DATA-SECURITY-POLICY	**ვერსია**	2
სტატუსი	ცარიელი ფორმა, მოსარგებად	**გამოშვების თარიღი**	
გადასინჯვის თარიღი		**ანაცვლებს**	
მფლობელი		**დაამტკიცა**	
ხელმოწერა			

მმართველობის დოკუმენტი — 2026 წლის გამოცემა. ამ დოკუმენტში მმართველობის, ეთიკისა და ხარისხის სისტემის დებულებები ძალაში რჩება. იქ, სადაც ნახსენებია „შემფასებლები“ ან „შეფასებები“, მიმდინარე აკრედიტაციის მოდელი იყენებს **ოთხი დასახელებული როლი** (პასუხისმგებელი პირი, დირექტორი, კოორდინატორი, მონიტორი) და **კვარტალური ციკლი**. ტერმინოლოგიის შესაბამისი გადასინჯული გამოცემა მზადდება.

სტრატეგია, მითითება და სამართალი

IT და მონაცემთა უსაფრთხოების პოლიტიკა

საჯარო რეესტრის, საჩივრების მიღებისა და ASF-ის ყოველი ჩანაწერის უკან მდგომი ციფრული სისტემების დაცვა

ASF-SECURITY-001-v2 · გამოქვეყნებულია · 2026 წლის 12 სექტემბერი · 13 გვერდი

> ეს არის სრული ტექსტი **IT და მონაცემთა უსაფრთხოების პოლიტიკა** (ASF-SECURITY-001-v2). PDF არის კონტროლირებადი ვერსია; ეს გვერდი გამოქვეყნებულია წაკითხვის, ძიებისა და ციტირებისთვის. ნაწილია ASF **დოკუმენტების ბიბლიოთეკის**.

1. წინასიტყვაობა

ASF-ის სტანდარტების შემუშავებისა და გადასინჯვის ფორმირების მე-11 განყოფილება ეხება განმცხადებელთა ინფორმაციის დაცვასა და კონფიდენციალურობას. ASF-ის საჯარო საჩივრებისა და უკუკავშირის პოლიტიკა ეხება საჩივრის ავტორის ვინაობის კონფიდენციალურობას. არცერთი მათგანი არ განიხილავს ინფორმაციულ უსაფრთხოებას როგორც ცალკე დისციპლინას — ფაქტობრივ ტექნიკურ და ორგანიზაციულ კონტროლებს, რომლებიც ამ მონაცემებს შემცველ სისტემებს იცავს. DNV Healthcare-ის საკუთარი NIAHO სტანდარტები ამ მიზეზით შეიცავს გამოყოფილ თავს უსაფრთხოების მართვის შესახებ, მმართველობისგან განცალკევებულს [1]. რადგან ASF-ის საჯარო რეესტრი, საჩივრების მიღება და დოკუმენტების რეპოზიტორია ASF-ის საკუთარ ვებგვერდზე გადადის, ეს აღარ არის თეორიული ხარვეზი.

1. მიზანი და მოქმედების სფერო

ის არ იმეორებს კონფიდენციალურობის ვალდებულებებს, რომლებიც სხვაგან არის დადგენილი; ის არეგულირებს ტექნიკურ და ორგანიზაციულ კონტროლებს, რომლებიც ამ ვალდებულებებს პრაქტიკაში რეალურად აღსრულებადს ხდის.

2. რატომ აქვს ამას მნიშვნელობა: შეცდომის რეალური ღირებულება

ეს თეორიული შეშფოთება არ არის. ჯანდაცვა ერთ ათწლეულზე მეტი ხანია მონაცემთა გაჟონვებით ყველაზე ძვირადღირებული დარგია, და ჯანდაცვის საშუალო გაჟონვა უახლეს ანგარიშებულ წელს US$6.64 მილიონი ღირდა — ყველა გაზომილ სხვა სექტორზე მეტი [3]. კონკრეტულად ევროპაში, მონაცემთა დაცვის ორგანოებმა ერთ ბოლო წელს GDPR-ის ჯარიმებად თითქმის €1.2 მილიარდი შეაფასეს, ხოლო რეგულაციის შემოღების შემდეგ კუმულაციური ჯარიმები €7.1 მილიარდს აჭარბებს [4].

ექსპოზიციის ხასიათი მისი ღირებულების მსგავსად მნიშვნელოვანია. ჯანდაცვაში საშუალო გაჟონვის გამოვლენასა და შეზღუდვას 279 დღე სჭირდება — დარგთაშორის საშუალოზე თვეზე მეტით მეტი — რაც რეალურ გაჟონვას აძლევს მეტ დროს, რომ რეალური ზიანი მიაყენოს, სანამ ვინმე შეამჩნევს, რომ ის საერთოდ მოხდა [5]. სწორედ ამიტომ მიიჩნევს ამ პოლიტიკის მე-6 განყოფილება გამოვლენის სისწრაფეს, და არა მხოლოდ პრევენციას, რეალურ, ცალკე მოთხოვნად.

> *ASF არ არის დიდი საავადმყოფოს სისტემა და არ ფლობს იმ მოცულობის მონაცემს, რომელსაც დარგთაშორისი მაჩვენებლები აღწერს. მაგრამ ძირითადი ექსპოზიცია — კონფიდენციალური შეფასების შედეგები, საჩივრის ავტორთა ვინაობა, სენტინელური მოვლენების ანგარიშები — ზუსტად იმ კატეგორიის მონაცემია, რომელსაც ეს სტატისტიკა ყველაზე ძვირადღირებულად და ყველაზე სამიზნედ აღწერს. მასშტაბი ცვლის პოტენციური ინციდენტის ზომას; მისი ძირითადი ბუნება არ იცვლება.*

3. მონაცემთა კლასიფიკაცია

ASF-ის მიერ შენახული მონაცემთა ყოველი კატეგორია კლასიფიცირდება ASF-ის საჯარო აკრედიტაციის რეესტრის პოლიტიკის მე-2 განყოფილებაში უკვე დადგენილი საჯარო/კონფიდენციალური განსხვავების შესაბამისად, აქ გავრცელებული ASF-ის მონაცემთა მთელ ფონდზე:

- საჯარო — გამოქვეყნებული სტანდარტები, რეესტრის ჩანაწერები და ნებისმიერი დოკუმენტი, რომელიც ASF-მა განზრახ გახადა საჯაროდ ხელმისაწვდომი; დაცულია არაავტორიზებული ცვლილებისგან, და არა გამჟღავნებისგან
- კონფიდენციალური — შეფასების შედეგები, საჩივრის ავტორთა ვინაობა, სენტინელური მოვლენების ანგარიშები, მაუწყებლების ანგარიშები და პერსონალის ჩანაწერები; დაცულია როგორც არაავტორიზებული ცვლილებისგან, ისე არაავტორიზებული გამჟღავნებისგან
- შეზღუდული — კონფიდენციალური მონაცემების ის ქვეჯგუფი, რომელსაც ყველაზე მაღალი მგრძნობელობა აქვს, მათ შორის მაუწყებლების ანგარიშები ASF-ის შიდა მაუწყებლის დაცვის პოლიტიკის მიხედვით და ნებისმიერი მონაცემი, რომელზეც ვრცელდება განსაკუთრებული კატეგორიის დაცვა ASF-ის სტანდარტების შემუშავებისა და გადასინჯვის მე-11 განყოფილების მიხედვით; ხელმისაწვდომია მხოლოდ იმ კონკრეტული პირებისთვის, რომელთა როლიც რეალურად მოითხოვს მას

4. წვდომის კონტროლი

კონფიდენციალურ ან შეზღუდულ მონაცემებზე წვდომა ენიჭება მხოლოდ იმ პირებს, რომელთა ფუნქცია ASF-ის პერსონალის კომპეტენციისა და ცნობიერების პოლიტიკის შესაბამისად რეალურად მოითხოვს მას, და იგი იხილება ყოველ ჯერზე, როცა ამ პირის ფუნქცია იცვლება. წვდომა არასდროს ენიჭება ნაგულისხმევად მთელ გუნდს ან

როლის კატეგორიას იმ შემთხვევაში, როცა ფაქტობრივი სამუშაო ამ მონაცემის მხოლოდ ნაწილს მოითხოვს.

5. მონაცემების დაცვა გადაცემისას და შენახვისას

6. უსაფრთხოების ინციდენტებზე რეაგირება

უსაფრთხოების ინციდენტი — არაავტორიზებული წვდომა, მონაცემთა გაჟონვა, ან ამ ორიდან ერთის რეალური მცდელობა — განიხილება როგორც ცალკე კატეგორია პაციენტის უსაფრთხოების სენტინელური მოვლენისგან ან ზოგადი შიდა შეუსაბამობისგან, თუმცა გამოძიდება ორივეს იგივე სიზუსტით. კონფიდენციალურ ან შეზღუდულ მონაცემებზე მომქმედი უსაფრთხოების ინციდენტი:

- იზოლირდება და დაუყოვნებლივ ფასდება აღმოჩენისთანავე
- იმ შემთხვევაში, თუ ინციდენტი პერსონალურ მონაცემებს ეხება, ეცნობება კომპეტენტურ მონაცემთა დაცვის ორგანოს ASF-ისთვის მის შესახებ ცნობის მიღებიდან სამოცდათორმეტი საათის განმავლობაში, იმ რეალური შეტყობინების ვადის შესაბამისად, რომელსაც მონაცემთა დაცვის ზოგადი რეგულაცია აწესებს ნებისმიერ ორგანიზაციაზე, რომელიც ევროკავშირში პერსონალურ მონაცემებს ამუშავებს [6]
- გამოიძებნება ძირეული მიზეზი ASF-ის შიდა შეუსაბამობისა და გასწორების პროცედურის ფარგლებში
- ეცნობება ნებისმიერ პირს, რომლის კონფიდენციალური მონაცემებიც რეალურად დაზიანდა, ASF-ის სტანდარტების შემუშავებისა და გადასინჯვის მე-11 განყოფილების მონაცემთა დაცვის პრინციპების შესაბამისად

> *მონაცემთა გაჟონვა, რომელიც საჩივრის ავტორის ან მაუწყებლის ვინაობას ეხება, მხოლოდ IT პრობლემა არ არის — ის ამ ორი პირისთვის სახელით გარანტირებული კონკრეტული დაცვის პირდაპირი მარცხია. ეს პოლიტიკა მას ამ სერიოზულობით ეპყრობა და არა როგორც ნაკლებად მნიშვნელოვან, მხოლოდ ტექნიკურ საკითხს.*

7. ადამიანური ფაქტორი

ყველა დარგში მონაცემთა გაჟონვების დაახლოებით ოთხმოცდარვა პროცენტი ადამიანურ შეცდომას უბრუნდება — არა დახვეწილ გარე შეტევას, რომელიც ძლიერ ტექნიკურ დაცვას არღვევს, არამედ შეცდომას ადამიანისგან, რომელსაც კანონიერი წვდომა აქვს [7]. სწორედ ამიტომ ეს პოლიტიკა მარტო არ დგას: მის გამოყენებაში კომპეტენცია აუცილებელი ელემენტია ASF-ის პერსონალის კომპეტენციისა და ცნობიერების პოლიტიკისთვის ნებისმიერი პირისთვის, რომელიც ამ პოლიტიკის მე-4 განყოფილებით განსაზღვრულ ფუნქციას ასრულებს, და იმის გაცნობიერება, თუ რატომაა ეს მნიშვნელოვანი — და არა მხოლოდ წესი თავისთავად — ამ პოლიტიკის საკუთარი მე-4 განყოფილებით განსაზღვრულ რეალურ, ცალკე მოთხოვნად ითვლება.

2. წყაროები

1. DNV. NIAHO® Accreditation Requirements, Interpretive Guidelines and Surveyor Guidance for Hospitals and Critical Access Hospitals, Revision 25-1. Høvik: DNV; 2025.
2. International Organization for Standardization. 2022.
3. Becker's Hospital Review, citing IBM Cost of a Data Breach Report 2026 (Ponemon Institute). Healthcare Data Breaches Cost $6.64M on Average. 2026.
4. CNiC Solutions. Cybersecurity Compliance Statistics 2026: GDPR, HIPAA, PCI & CMMC Data. 2026.
5. Fax Sip IT. Healthcare Cybersecurity Statistics: Breach Costs & Data in 2026. 2026.
6. European Union. General Data Protection Regulation (EU) 2016/679, Article 33 (Notification of a Personal Data Breach to the Supervisory Authority). 2016.
7. HIPAA Compliant Hosting. Healthcare Data Breach Statistics 2026: HIPAA Enforcement. 2026.

---

3. დანართი A — უსაფრთხოების ინციდენტის ჩანაწერი

> *ივსება ყოველ უსაფრთხოების ინციდენტზე, რომელიც ამ პოლიტიკით არის გამოვლენილი.*

აღმოჩენის თარიღი: _____

დაზარალებული სისტემები ან მონაცემები:

_____

- ☐ საჯარო მონაცემები
- ☐ კონფიდენციალური მონაცემები

☐ შეზღუდული მონაცემები

შეზღუდვა

მიღებული ზომა: _____

შეზღუდვის თარიღი: _____

მარეგულირებელი შეტყობინება (თუ პერსონალური მონაცემები დაზარალდა)

მონაცემთა დაცვის ორგანო ეცნობა (72 საათში):

_____

დაზარალებული პირები

☐ საჭირო შეტყობინება და შესრულებულია

☐ პირის მონაცემები რეალურად არ დაზარალებულა

ძირეული მიზეზი

_____

გადაეცა შეუსაბამობის პროცედურას: _____

4. საძიებელი

72-საათიანი შეტყობინება, 6

წვდომის კონტროლი, 4

კონფიდენციალური მონაცემები, 3

მონაცემთა კლასიფიკაცია, 3

GDPR, 2, 6

ადამიანური ფაქტორი, 7

ინციდენტზე რეაგირება, 6

საჯარო მონაცემები, 3

შეზღუდული მონაცემები, 3

უსაფრთხოების ინციდენტის ჩანაწერი, დანართი A

ყოველი დაცვა, რომელსაც ეს ფონდი პაციენტს, საჩივრის ავტორს ან მაუწყებელს ჰპირდება, მხოლოდ იმდენად რეალურია, რამდენადაც მისი მონაცემების შემცველი სისტემა. ეს პოლიტიკა არის ის, რაც ამ დაპირებას ტექნიკურად ჭეშმარიტს ხდის და არა მხოლოდ დაწერილს.

დოკუმენტის კონტროლი

დოკუმენტის სათაური	ASF IT და მონაცემთა უსაფრთხოების პოლიტიკა
დოკუმენტის ნომერი	ASF-SECURITY-001-v2
ვერსია / გამოცემა	ვერსია 2
სტატუსი	გამოქვეყნებულია
გამოქვეყნების თარიღი	2026 წლის 12 სექტემბერი
გამოქვეყნების ადგილი	პარიზი, საფრანგეთი
გამომცემი ორგანო	ASF საერთაშორისო სტანდარტების საბჭო, Accréditation Sans Frontières
ორიგინალის ენა	ინგლისური
ამოქმედების თარიღი	2026 წლის 12 სექტემბერი
შემდეგი დაგეგმილი გადახედვა	2029 წლის 12 სექტემბერი
ანაცვლებს	ვერსია 1

ამ გვერდზე

წინასიტყვაობა

1. მიზანი და მოქმედების სფერო

2. რატომ აქვს ამას მნიშვნელობა: შეცდომის რეალური ღირებულება

3. მონაცემთა კლასიფიკაცია

4. წვდომის კონტროლი

5. მონაცემების დაცვა გადაცემისას და შენახვისას

6. უსაფრთხოების ინციდენტებზე რეაგირება

7. ადამიანური ფაქტორი

წყაროები

დანართი A — უსაფრთხოების ინციდენტის ჩანაწერი

საძიებელი

5. გაქვთ შეკითხვა ამ დოკუმენტთან დაკავშირებით?

შესწორებები, თარგმანის მოთხოვნები და წინადადებები შემდეგი გადახედვის ციკლისთვის ყველასგან მისალმებულია.

მოგვწერეთ

QR კოდი

დაასკანერეთ გასახსნელად. დაბეჭდეთ გასაზიარებლად.

გაზიარება

Facebook LinkedIn X WhatsApp

ბმულის კოპირება

დოკუმენტი QR-ის ჩამოტვირთვა ბეჭდვა / PDF