DIG-SOP-001: პაციენტის მონაცემთა დარღვევაზე რეაგირების პროცედურა

სტანდარტული საოპერაციო პროცედურა (SOP) · DIG-SOP-001 · ვერსია 1.1 · დამტკიცებულია ASF ექსპერტთა კომიტეტის მიერ

მხარს უჭერს: 2A.4

მოკლედ

- შეზღუდეთ: შეაჩერეთ წვდომა ან დაკარგვა, თუ ეს უსაფრთხოა. არაფერი წაშალოთ.
- დაუყოვნებლივ მოახსენეთ მონაცემთა დაცვის ხელმძღვანელს და თქვენს უშუალო მენეჯერს.
- მონაცემთა დაცვის ხელმძღვანელი დარღვევას 24 საათში აფასებს და აღნუსხავს.
- აღმასრულებელ დირექტორთან ერთად გადაწყვიტეთ, უნდა ეცნობოს თუ არა მარეგულირებელს და დაზარალებულ პაციენტებს.
- მიზეზი განიხილეთ და კონტროლები შეცვალეთ 30 დღეში.
- დაუყოვნებლივ შეაჩერეთ და მიმართეთ დახმარებას, თუ: დარღვევა ჯერ კიდევ მიმდინარეობს, ან ინფორმაცია საფრთხეშია, რომ შემდგომში გაიგზავნოს. ჯერ შეზღუდეთ.

1. მიზანი

იმის უზრუნველსაყოფად, რომ პაციენტის ინფორმაციის ნებისმიერი დარღვევა შეიზღუდოს, შეფასდეს, მოხსენდეს სადაც საჭიროა და გამოყენებულ იქნას კონტროლების გასაძლიერებლად [EC].

2. სფერო

ვრცელდება	ყველა, ვინც აღმოაჩენს, მოახსენებს ან ეხება ეჭვმიტანილ დარღვევას
ადგილები	ყველა საიტი, სისტემა და ქაღალდის ჩანაწერი
როდის	როგორც კი დარღვევა ან ეჭვმიტანილი დარღვევა აღმოჩნდება
არ ვრცელდება	რუტინული შეცდომები გამჟღავნების გარეშე, რომლებიც ინციდენტის პოლიტიკით მუშავდება, მაგრამ აქაც აღინუსხება

3. განმარტებები

ტერმინი	მნიშვნელობა
დარღვევა	ჯანმრთელობის ინფორმაციაზე არაავტორიზებული წვდომა, დაკარგვა, გამჟღავნება ან ცვლილება
შეზღუდვა	ქმედება შემდგომი ზიანის შესაჩერებლად, მაგალითად, შესვლის გათიშვა ან დოკუმენტის აღდგენა
დარღვევის გუნდი	მონაცემთა დაცვის ხელმძღვანელი, IT ხელმძღვანელი, შესაბამისი მომსახურების უფროსი და აღმასრულებელი დირექტორი ან მისი წარმომადგენელი

4. საფუძვლები

დარღვევისას სიჩქარე მნიშვნელოვანია. შეზღუდვა და ადრეული მოხსენება პაციენტებისთვის ზიანს ზღუდავს. კანონმა შეიძლება მოითხოვოს შეტყობინება დადგენილ ვადებში, რომელიც ქვეყნისთვის უნდა დადასტურდეს (EC).

5. პასუხისმგებლობები

როლი	პასუხისმგებლობა	კომპეტენცია
დარღვევის აღმომჩენი პირი	ზღუდავს, თუ უსაფრთხოა; დაუყოვნებლივ მოახსენებს	ორიენტაცია
მონაცემთა დაცვის ხელმძღვანელი	ხელმძღვანელობს შეფასებას; ინახავს დარღვევების ჟურნალს; იძლევა რჩევას შეტყობინებაზე	მონაცემთა დაცვის კომპეტენცია

IT ხელმძღვანელი	იცავს სისტემებს; ინახავს ჟურნალებს; აღადგენს მონაცემებს	IT უსაფრთხოება
აღმასრულებელი დირექტორი	წყვეტს მარეგულირებლისა და პაციენტების შეტყობინებას	აღმასრულებელი ხელმძღვანელობა

6. მასალები და აღჭურვილობა

ერთეული	მოთხოვნა	მდგომარეობა
დარღვევის მოხსენების ფორმა	თარიღი, დრო, რა, ვინ, როგორ აღმოაჩინეს	შევსებული
დარღვევების ჟურნალი	მიმდინარე	განახლებული ყოველი დარღვევისთვის

7. უსაფრთხოება

- გამოძიებისთვის ინფორმაცია არ გადაუგზავნოთ და არ დააკოპიროთ.
- დაზარალებულ პაციენტს არ დაუკავშირდეთ, სანამ დარღვევის გუნდი შეტყობინებას არ შეათანხმებს.

8. დაწყებამდე

- იცოდეთ, ვინ არიან თქვენი მონაცემთა დაცვის და IT ხელმძღვანელები და როგორ დაუკავშირდეთ სამუშაო საათების გარეთ.

9. პროცედურა

ეტაპი 1. დარღვევის შეზღუდვა.

- თუ უსაფრთხოა, შეაჩერეთ წვდომა: გამოდით სისტემიდან, გათიშეთ ანგარიში ან დაიცავით ქაღალდის ჩანაწერი.
- არ წაშალოთ შეტყობინებები, ფაილები ან ჟურნალები.
- აღნიშნეთ, როდის აღმოაჩინეთ დარღვევა და რა გააკეთეთ.

მთავარი: შეზღუდვა ზიანს ზღუდავს. წაშლა მტკიცებულებას ანადგურებს.

ეტაპი 2. დაუყოვნებლივ მოხსენება.

- დაუყოვნებლივ აცნობეთ თქვენს უშუალო მენეჯერს და მონაცემთა დაცვის ხელმძღვანელს, საჭიროებისას ტელეფონით.
- დარღვევის მოხსენების ფორმა 24 საათში შეავსეთ.

მთავარი: შეტყობინების ვადა იწყება, როცა დაწესებულებამ იცის. ადრეული მოხსენება იცავს დაწესებულებასაც და პაციენტებსაც.

ეტაპი 3. დარღვევის შეფასება 24 საათში.

- მონაცემთა დაცვის ხელმძღვანელი აღნუსხავს, რა ინფორმაცია იყო ჩართული, რამდენი პაციენტი, რა ზიანი შეიძლება მოჰყვეს და იყო თუ არა შემთხვევითი ან განზრახ.
- შეინახეთ სისტემის ჟურნალები და ელფოსტები.

მთავარი: შეფასება წყვეტს, რა უნდა გაკეთდეს შემდეგ.

ეტაპი 4. შეტყობინების გადაწყვეტა.

- დარღვევის გუნდი და აღმასრულებელი დირექტორი წყვეტენ, უნდა ეცნობოს თუ არა მარეგულირებელს და დაზარალებულ პაციენტებს, და რა ვადაში.
- აღნუსხეთ გადაწყვეტილება და მიზეზები.

მთავარი: შეტყობინების გადაწყვეტილებები უნდა აღინუსხოს, მაშინაც კი, როცა გადაწყვეტილება შეუტყობინებლობაა.

ეტაპი 5. დაზარალებულების ინფორმირება.

- სადაც შეტყობინებაა საჭირო, პაციენტს მიეცით მკაფიო, გულწრფელი ინფორმაცია: რა მოხდა, რა ინფორმაცია, რა შეუძლია მას, და ვის დაუკავშირდეს.
- აღნუსხეთ თარიღი და მეთოდი.

მთავარი: პაციენტებს ეკუთვნით სიმართლე, მკაფიოდ და დროულად მიწოდებული.

ეტაპი 6. დარღვევიდან სწავლა.

- 30 დღეში ჩაატარეთ ძირეული მიზეზის განხილვა (INC-SOP-001).
- შეცვალეთ კონტროლები, ტრენინგი ან წვდომა, რომელიც ვერ

იმუშავა, და აღნუსხეთ ქმედება.
- დახურვა აღნუსხეთ დარღვევების ჟურნალში.

მთავარი: დარღვევა, რომელიც არაფერს არ ცვლის, კვლავ მოხდება.

10. გადაწყვეტილების წერტილები

- თუ დარღვევა სისხლის სამართლის დანაშაულს შეიცავს, პოლიციას აცნობეთ აღმასრულებელი დირექტორის მეშვეობით, შეზღუდვის ეტაპის შემდეგ.

11. განსაკუთრებული სიტუაციები

სიტუაცია	მოქმედება
დარღვევა პერსონალის წევრის მიერ	შეფასების შემდეგ მიჰყევით დისციპლინარულ პროცედურას. შედეგს წინასწარ ნუ განსაჯით.

12. ესკალაცია

- მძიმე დარღვევები მიდის აღმასრულებელ დირექტორთან და მმართველ ორგანოსთან შემდეგ შეხვედრაზე, ან უფრო ადრე, თუ გადაუდებელია.

13. მონიტორინგი

მაჩვენებელი	სამიზნე	სიხშირე	პასუხისმგებელი	თუ არ შესრულდა
დარღვევები მოხსენებული 24 საათში	100%	ყოველი დარღვევა	მონაცემთა დაცვის ხელმძღვანელი	მოხსენების დაგვიანების განხილვა
დარღვევები შეფასებული 24 საათში	100%	ყოველი დარღვევა	მონაცემთა დაცვის ხელმძღვანელი	ესკალაცია მთავარ აღმასრულებელთან
ძირეული მიზეზის განხილვები	100%	ყოველთვიურად	მონაცემთა დაცვის ხელმძღვანელი	ესკალაცია

დასრულებული 30 დღეში				

14. ჩანაწერები

ჩანაწერი	ინახება	შენახვის ვადა
დარღვევის მოხსენების ფორმა	მონაცემთა დაცვის ფაილი	დაწესებულების ჩანაწერების პოლიტიკით დადგენილი პერიოდი, წლები
დარღვევების ჟურნალი და ძირეული მიზეზის განხილვა	მონაცემთა დაცვის ფაილი	დაწესებულების ჩანაწერების პოლიტიკით დადგენილი პერიოდი, წლები

15. ტრენინგი

- დარღვევაზე რეაგირება შედის ორიენტაციასა და წლიურ ტრენინგში (EC).
- დარღვევის გუნდი ყოველწლიურად ვარჯიშობს DIG-FRM-001-ის მეშვეობით (EC).

16. დაკავშირებული დოკუმენტები

ID	სათაური	გამოყენება
DIG-POL-001	ინფორმაციის უსაფრთხოებისა და წვდომის კონტროლის პოლიტიკა	წვდომის წესების წყარო
DIG-FRM-001	დარღვევაზე რეაგირების ტესტის ჩანაწერი	წლიური ტესტი
INC-POL-001	ინციდენტების მოხსენება და მართვა	დარღვევა ასევე აღინუსხება როგორც ინციდენტი

17. მტკიცებულებები

მითითება	შენიშვნა
E-009	ASF ექსპერტთა კომიტეტის კონსენსუსი. შეტყობინების ვადები ეროვნულ კანონთან უნდა დადასტურდეს დამტკიცებამდე.

18. ცვლილებების ისტორია

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

ამ დოკუმენტის ელექტრონული სწავლება

- **Records, Confidentiality and Data Protection** (T-11)
- Security Protocols & Incident Response (SEC-01)

წყაროები

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