

Процесите и предизвиците во уредувањето  
на пристапот до медицински податоци:  
Европски искуства и примена во Северна  
Македонија

Кристина Мишева  
Марија Амповска



## ЛИСТА НА КРАТЕНКИ

<b>ACSS</b>	Administração Central do Sistema de Saúde Агенција за здравствени услуги во Португалија
<b>CAIC</b>	Comissão de Acompanhamento da Informatização Clínica Комисија за следење на клиничката дигитализација
<b>CRPP</b>	Centralni Register Podatkov o Pacientih Централен регистар на податоци за пациенти во Словенија
<b>EHDS</b>	European Health Data Space Европски простор за здравствени податоци
<b>EHR</b>	Electronic Health Record Електронска здравствена евиденција
<b>ENHS</b>	Estonian National Health Information System Естонски национален здравствен информативен систем
<b>EHPB</b>	The Estonian Healthcare Picture Bank (SA Eesti Tervishoiu Pildipank) Естонска банка за дигитални дијагностички слики
<b>GDPR</b>	General Data Protection Regulation Општа регулатива за заштита на податоци
<b>INSA</b>	Instituto Nacional de Saúde Dr. Ricardo Jorge Национален институт за здравје во Португалија
<b>NHS</b>	National Health Service Национален здравствен систем
<b>HWISC</b>	Health and Welfare Information Systems Centre Центар за информациски системи за здравје и благосостојба
<b>PPoP</b>	Резиме на пациентот во словенскиот zVEM портал
	Resumo Clínico Único do Utente
<b>RCU2</b>	Единствено клиничко резиме за корисниците на NHS

<b>SARS-CoV-2</b>	коронавирусот кој ја предизвика пандемијата COVID-19
<b>SNS (Serviço Nacional de Saúde)</b>	Serviço Nacional de Saúde Национален здравствен систем во Португалија
<b>SClinico /Hospital Health Care (HHC)</b>	Национален клинички регистар во Португалија
<b>SPMS</b>	Serviço de Provedores de Saúde Сервис за здравствени податоци и системи
<b>TEHIK</b>	Health and Welfare Information Systems Centre Центар за информациски системи за здравје и благосостојба во Естонија
<b>TEHDAS</b>	Проект за европски здравствени податоци Towards European Health Data Space
<b>zVEM</b>	Портал за здравствени услуги во Словенија Zdravstvene Vsebine Elektronskega Mrežnega Sistema
<b>ZVOP-2</b>	Zakon o Varstvu Osebnih Podatkov, Ver. 2 Закон за заштита на лични податоци во Словенија
<b>ZZPPZ</b>	Zakon o Zdravstvenih Podatkovnih Bazi Закон за бази на податоци од областа на здравствената заштита во Словенија
<b>ZZPPZ-B</b>	Закон за изменување и дополнување на Законот за бази на податоци од областа на здравствената заштита на Словенија
<b>EEЗ</b>	Европска економска заедница
<b>ЕЗК (EHR)</b>	Електронски здравствени картони
<b>ЕУ</b>	Европска Унија
<b>ХИВ</b>	вирусот причинител на имунитетски недостаток кај човекот

*Здружението „Заедно посилни“ Скопје искажува благодарности на Жаклина Чаџороска и Управата за електронско здравство за придонесот и соработката во подготовката на оваа публикација.*

# СОДРЖИНА

Листа на кратенки .....	2
1. <b>ВОВЕДНИ ЗАБЕЛЕШКИ</b> .....	6
2. <b>ЕУ – КРАТОК ОСВРТ</b> .....	8
2.1. Европска конвенција за заштита на човековите права .....	9
2.2. Повелба за основните права во ЕУ (Charter of Fundamental Rights of the European Union, 2012/C 326/02) .....	11
2.3. Договор за функционирање на Европската Унија .....	12
2.4. Закон за податоци на ЕУ и Европски простор за здравствени податоци (European Health Data Space- EHDS) .....	14
3. <b>РЕГУЛАЦИЈА НА МЕДИЦИНСКИТЕ ПОДАТОЦИ ВО ЕСТОНИЈА</b> .....	16
3.1. Правна рамка – краток осврт .....	18
3.2. Закон за заштита на личните податоци на Естонија (Personal Data Protection Act – Riigi Teataja) .....	19
3.3. Закон за јавна здравствена заштита (Public Health Act – Riigi Teataja) ..	19
3.4. Закон за организација на здравствените услуги .....	20
3.5. Уредба на Здравствениот информациски систем .....	26
3.6. Кратко резиме .....	27
4. <b>РЕГУЛАЦИЈА НА МЕДИЦИНСКИ ПОДАТОЦИ ВО СЛОВЕНИЈА</b> .....	30
4.1. Закон за заштита на личните податоци .....	31
4.2. Закон за бази на податоци од областа на здравствената заштита ..	35
4.3. Правилник за забрана за преглед на изводот од податоците за пациентот во Централниот регистар на податоци за пациенти .....	38
4.4. Портал за здравствени услуги zVEM и Централен регистар за податоци на пациентите (CRPP) во Словенија .....	41
4.5. Правилник за овластувања за обработка на податоци .....	43
4.6. Кратко резиме .....	47
5. <b>РЕГУЛАЦИЈА НА МЕДИЦИНСКИТЕ ПОДАТОЦИ ВО ПОРТУГАЛИЈА</b> .....	50
5.1. Правна рамка .....	50
5.2. Закон за заштита на личните податоци во согласност со Регулацијата (ЕУ) 2016/679 на Парламентот и на Советот од 2016 година (GDPR) .....	51
5.3. Основен закон за здравство од 2019 година .....	53
5.4. Закон за лични генетски информации и здравствени информации од 2005 година .....	57
5.5. Кратко резиме .....	59
6. <b>ПРЕПОРАКИ И ПРЕДИЗВИЦИ ЗА СЕВЕРНА МАКЕДОНИЈА</b> .....	62
6.1. Препораки за законски измени и технички решенија .....	62
6.2. Препорака за примена на принципи за транспарентност и ограничен пристап од словенечкиот модел .....	64
7. <b>ЗАКЛУЧОК</b> .....	68

## 1

## ВОВЕДНИ ЗАБЕЛЕШКИ

Пристапот до медицински податоци претставува еден од најважните аспекти на традиционалното, а особено на дигиталното здравство, кој има клучна улога во балансирањето на заштитата на приватноста на медицинските податоци, на потребата за ефикасно обезбедување здравствена грижа и услуги, но и на овозможувањето научни истражувања. Некои европски земји, како што се Естонија, Словенија и Португалија, развиле правни и институционални механизми кои нудат различни решенија за обработка и пристап до медицински податоци, со фокус врз заштитата на личните информации и генетските податоци. Овие земји се водечки примери за успешна интеграција на е-здравствените системи и за имплементација на модерни здравствени политики и регулативи кои обезбедуваат правична и транспарентна обработка на податоците и на пристапот до нив. Ова се земји членки на ЕУ кои имаат остварено делумна или целосна дигитализација (како Естонија) на медицинските податоци на населението. Затоа, нивниот значителен придонес на национално ниво и нивните практики може да бидат препознаени и применливи како добри практики и во нашата земја.

Првиот дел од извештајот дава осврт на актуелните регулативи и директиви на Европската Унија кои ги регулираат процесите на обработка и пристап до медицински податоци. Европските акти, како што е Општата регулатива за заштита на податоци (GDPR), играат клучна улога во формирањето на основните принципи за заштита на личните податоци во здравствените системи на земјите членки. Тие се основа за создавање унифицирани стандарди за заштита на приватноста, безбедноста и транспарентноста во процесите на обработка на податоци.

Вториот, третиот и четвртиот дел од извештајот се фокусира врз конкретните

анализи од трите земји: Естонија, Словенија и Португалија. Во секој од овие делови, се анализира правната рамка која ги регулира медицинските податоци, како и институционалната поставеност и практиките за пристап до податоците. По анализата на секоја од земјите, следува кратко резиме на клучните поенти, што ќе служи како основа за формулирање конкретни предлози и решенија кои би можеле да се применат во Северна Македонија.

На крајот од извештајот е даден краток сумарен приказ (заклучок) од целокупната анализа.

Со оваа структура, извештајот има за цел да обезбеди сеопфатен и детално организиран пристап за подобро разбирање на регулативите за пристап и заштита на медицински податоци, од една страна, и лапидарен, информативен приказ на состојбите за пошироката јавност, од друга страна. Овие анализи ќе послужат како основа за развој на предлог-решенија кои би можеле да се применат во македонското законодавство и практика, со цел да се создаде баланс помеѓу потребата за заштита на приватноста на пациентите и потребата за пристап до податоци, кои се од суштинско значење за здравствената заштита и јавната здравствена политика.



# 2

## ЕУ- КРАТОК ОСВРТ

Советот на Европа и Европската Унија имаат усвоено, односно применуваат општи акти кои се фокусираат врз заштитата на личните податоци, а во последно време и на здравствените податоци на физичките лица, во процесот на обработката, преносот, контролата и пристапот до овие податоци. Современите тенденции на ЕУ одат во насока на усогласување и стандардизација на примена на правилата во оваа област во сите земји членки. Таквите општи акти се базираат врз премисата „Секој има право на заштита на личните податоци кои се однесуваат на него/неа“, а тие се:

1. Европската конвенција за заштита на основните човекови права и слободи од 1950 година (European Convention of Human Rights – Convention for the Protection of Human Rights and Fundamental Freedoms);
2. Повелбата за основните права во Европската Унија од 2000 година, заменета со Повелбата од 2012 година (Charter of Fundamental Rights of the European Union, 2012/C 326/02), со влегувањето на сила на Договорот од Лисабон.
3. Договорот за функционирање на Европската Унија од 2010 година (Treaty on the functioning of the European Union);
4. Регулативата за заштита на личните податоци од 2016 година (General Data Protection Regulation – GDPR); и
5. Законот за податоците од 2024 година (Health Data Act).

Овие акти имаат големо влијание во процесот на креирање на националните законодавства на земјите членки на ЕУ, односно на одредбите кои ја регулираат

ефективната заштита на личните податоци и обврските на субјектите кои ги обработуваат, ги процесираат и овозможуваат пристап до личните податоци, меѓу кои спаѓаат и медицинските податоци.

Сите овие акти целосно, во поголема или помала мера, опфаќаат материја која се однесува на обработката и пристапот до медицинските податоци како посебна категорија лични податоци. Земјите членки на ЕУ и земјите кандидати за членство во ЕУ ги хармонизираат националните законодавства со законодавството на ЕУ.

## 2.1. ЕВРОПСКА КОНВЕНЦИЈА ЗА ЗАШТИТА НА ЧОВЕКОВИТЕ ПРАВА

Член 8 од Европската конвенција за заштита на основните човекови права и слободи (European Convention for the Protection of Human Rights and Fundamental Freedoms) го уредува правото на почитување на приватниот и семејниот живот и гласи: *Секој има право на почитување на неговото приватно и семејно живото, својот дом и својот семеен живот. Јавната власт не смее да се меша во остварувањето на ова право, освен ако тоа мешање е предвидено со закон и ако претставува мерка која е во интерес на државната и јавната безбедност, економската благосостојба на земјата, заштитата на поредоците и спречувањето на кривични дела, заштитата на здравјето и моралот, или заштитата на правата и слободите на други, во едно демократско општество<sup>1</sup>.*

Конвенцијата регулира дека уживањето на правата и слободите, признати со Конвенцијата, треба да се обезбеди без никаква дискриминација заснована врз полот, расата, бојата на кожата, јазикот, верата, политичкото или какво и да е друго мислење, националното или социјалното потекло, припадноста на национално малцинство, материјалната положба, потеклото по раѓање или каков и да е друг статус<sup>2</sup>.

И покрај тоа што членот таксативно не го споменува здравјето, формулацијата „каков и да е друг статус“ го опфаќа и здравјето на човекот.

### 2.1.1. ПРАКТИКА НА ЕВРОПСКИОТ СУД ЗА ЧОВЕКОВИ ПРАВА

Европскиот суд за човекови права редовно го толкува правото на приватност како заштита на чувствителните податоци, како што се здравствените информации, кои се тесно поврзани со достоинството и автономијата на поединецот. Важен е принципот дека секое мешање во ова право мора да биде законски основано, неопходно и пропорционално. Во случаи како што се *Z v. Finland*<sup>3</sup> и *Mockutė v. Lithuania*<sup>4</sup>, Судот потврдува дека **откривањето**

---

1 Совет на Европа, Европска конвенција за заштита на човековите права и слободи, во сила од 3 септември 1953, (Член 8), достапна на следниот линк: <https://www.coe.int/mk/web/compass/the-european-convention-on-human-rights-and-its-protocols>.

2 Европска конвенција за заштита на човековите права и слободи (Член 14).

3 Види повеќе: European Court of Human Rights, Case of *Z v. Finland*, App. no. 22009/93, 25 February 1997.

4 Види повеќе: European Court of Human Rights, Case of *Mockutė v. Lithuania*, App.no. 66490/09, 27 May 2018.

здравствени податоци без согласност на пациентот може да претставува нарушување на правото на приватност, особено кога се работи за податоци кои може да имаат сериозни последици врз личниот и социјалниот живот на поединците. Покрај тоа, во случајот *Surikov v. Ukraine*<sup>5</sup>, Судот констатирал дека долговечното чување и откривање на здравствените податоци за цели кои не се поврзани со оригиналната причина за нивното собирање претставува непотребно мешање во правото на приватност.

Судот посветува особено внимание на заштитата на податоците за ХИВ, чија објава може да доведе до стигматизација и исклучување од општествените и професионалните кругови. Во случајот *Z v. Finland*, Судот утврдил дека откривањето на такви податоци без соодветна правна основа претставува несоодветно мешање во правото на приватност, освен ако тоа не е оправдано од јавниот интерес или за заштита на здравјето на поединецот или безбедноста на медицинскиот персонал.

Долунаведените судски одлуки ги нагласуваат важноста на правото на приватност и заштитата на здравствените податоци како суштински дел од човековото достоинство и автономија, кој треба да биде почитуван и заштитен во сите правни системи на земјите членки на Конвенцијата за човекови права.

### 2.1.1.1. L.H. v. LATVIA

Во случајот *L.H. v. Latvia* – 52019/07<sup>6</sup> од 2014 година, Судот донел одлука дека имало повреда на членот 8 (правото на приватен и семеен живот) од Конвенцијата, поради **недостаток на прецизност на домашното право кое дозволува јавниот орган да собира медицински податоци на апликантот**. Во овој случај, апликантката (жалителот) тврдела дека собирањето на нејзините лични медицински податоци од страна на државна агенција – во овој случај, Инспекторатот за контрола на квалитетот за медицинска нега и подготвеност за работа (*Medicīniskās aprūpes un darbspējas ekspertīzes kvalitātes kontroles inspekcija „MADEKKI“*) во Латвија – без нејзина согласност, го повредило нејзиното право на почитување на нејзиниот приватен живот.

Судот особено забележа дека **латвискиот закон на никаков начин не го ограничува опсегот на приватните податоци што може да ги собере MADEKKI**, што резултирало со собирање медицински податоци за апликантот неселективно и **без претходна проценка за нивната релевантност или важност**. Поконкретно, истрагата започнала седум години по стерилизацијата на апликантот, што довело до сомневање дали собирањето на податоците било навистина „неопходно за целите на медицински третман или администрација на здравствени услуги“, како што бара законот. Во оваа пресуда, Судот потсетил на важноста на заштитата на медицинските податоци за уживањето на правото на почитување на приватниот живот на една личност.

5 Види повеќе: European Court of Human Rights, Case of *Surikov v. Ukraine*, App.no. 42788/06, 26 April 2017.

6 Види повеќе: European Court of Human Rights, Case of *L.H. v. Latvia*, App.no. 52019/07, 29 April 2014.

### 2.1.1.2. Y.G. v. RUSSIA

Во случајот Y.G. v. Russia – 8647/12 од 2022 година<sup>7</sup>, Судот, исто така, донел пресуда дека постои прекршување на членот 8 од Конвенцијата. Овој случај се однесува на собирање здравствени податоци, вклучително и на апликантот, кој бил пациент со ХИВ и боледувал од хепатит, во база на податоци што била достапна за продажба на пазар. Апликантот изјавил дека органите на прогонот незаконски ги собрале, ги складираше и ги внесле неговите здравствени податоци во база на податоци и дека не успеале да обезбедат доверливост на неговите податоци и да спроведат ефикасна истрага за нивното откривање. Државните органи, кои имале пристап до медицинските податоци, не успеале да спречат нарушување на доверливоста. Како резултат на тоа, тие податоци станале јавно достапни, за што била одговорна тужената држава. Во овој поглед, неспорно е дека само властите имале пристап до повеќето од податоците во базата на податоци, затоа **Судот потсетил дека постојано ја нагласува важноста на соодветните заштитни мерки за да се спречи неовластен трансфер и обелоденување на здравствените податоци.**

## 2.2. ПОВЕЛБА ЗА ОСНОВНИТЕ ПРАВА ВО ЕУ (CHARTER OF FUNDAMENTAL RIGHTS OF THE EUROPEAN UNION, 2012/C 326/02)

Оваа Повелба ги реafirмира правата такви какви што произлегуваат од уставните традиции и меѓународните обврски на државите членки на ЕУ, од Спогодбата на Европската Унија, од Спогодбите на ЕЕЗ, од Европската конвенција за заштита на човековите права и слободи, од Социјалните спогодби усвоени од страна на ЕЕЗ и Советот на Европа, од судската пракса на Судот на правдата на европските заедници и на Европскиот суд за човекови права.

Одредбите од оваа Повелба се применуваат од страна на институциите, телата, канцелариите и агенциите на ЕУ и на земјите членки, во сите нивни активности кога го спроведуваат правото на ЕУ. Преку оваа Повелба, физичките и правните лица може да се заштитат од дејствијата на институциите и на агенциите на ЕУ кои ги нарушуваат основните права.

Повелбата, во член 8, предвидува дека личните податоци мора да се обработуваат само за конкретни легитимни цели и со согласност на засегнатото лице. Исто така, и дека секој има право на пристап до личните податоци.

Повелбата за основните права во ЕУ (член 8) и Европската конвенција за заштита на човековите права (член 8) се меѓусебно поврзани во заштитата на правото на приватност и на личните податоци, вклучително и медицинските податоци. Двата инструмента ја обврзуваат ЕУ и земјите членки да го почитуваат правото на приватност и да ги заштитат личните податоци во согласност со високите стандарди на човекови права.

---

7 Види повеќе: European Court of Human Rights, Case of Y.G. v. Russia, App.no. 8647/12, 30 August 2022, достапно на <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22002-13761%22%7D>.

## 2.3. ДОГОВОР ЗА ФУНКЦИОНИРАЊЕ НА ЕВРОПСКАТА УНИЈА

Договорот за функционирање на ЕУ, како и претходните акти, ја следи потребата од утврдување на правилата и од систематизирање на одредбите за заштитата на личните податоци. Поточно, консолидираната верзија на Договорот за функционирање на ЕУ<sup>8</sup> одредбите за заштита на личните податоци ги сместува во одредби со општа примена, при што член 16 (поранешен член 286 од Договорот за основање на Европската заедница) го потенцира правото на заштита на личните податоци како основно право и упатува на усогласени правила при примена на ова право низ целата Унија и земјите членки. Со ова се поставува основното право на заштита на личните податоци во ЕУ, се создава правна рамка за обработка на овие податоци, која вклучува механизми за контрола и надзор, за да се осигури усогласеност со правилата на Унијата и со правото на поединците на приватност.

### 2.3.1. РЕГУЛАТИВА ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО ЕУ (GDPR РЕГУЛАТИВАТА)<sup>9</sup>

Регулативата е крстопатот и правен акт кој системски ја уредува заштитата и обработката на личните податоци. Една од главните цели поради кои е донесена Регулативата е да даде придонес во унапредувањето на благосостојбата на физичките лица. Оваа Регулатива влезе во сила 2016 година и стана директно применлива во сите земји членки на Европската Унија на 25 мај 2018 година.

Една од целите на Регулативата е **физичките лица да имаат „контрола“ над своите лични податоци, а особено над посебните категории на личните податоци, генетските и биометриските податоци**. Член 5 од Регулативата ги уредува начелата кои се однесуваат на обработката на личните податоци. Такви начела се: законитост, правичност, транспарентност, ограничување на целите, минимизирање на податоците, точност, ограничување на складирањето, интегритет и доверливост, и отчетност.

За потребите на оваа анализа, особено се важни начелата на **„ограничување на целите“**, кои предвидуваат дека податоците ќе се собираат за конкретни и јасни цели; **„минимален обем на податоци“**, односно да се собираат релевантни податоци само во обемот што е неопходен за целите за кои се собираат; **„ограничување на рокот на чување на податоците“**, кој предвидува податоците да се чуваат не подолго од она што е потребно за целите за кои се обработуваат; како и **„интегритет и доверливост“** – податоците е потребно да бидат обработени на соодветно ниво на безбедност и да бидат соодветно заштитени од неовластена и незаконска обработка.

8 European Union, Treaty on European Union, 2010/C 83/01)EN, 30 March 2010.

9 Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119, 04.05.2016)

### 2.3.1.1. ОБРАБОТКА НА ПОСЕБНИТЕ КАТЕГОРИИ ПОДАТОЦИ

Регулативата ја нормира обработката на посебните категории податоци и ја забранува обработката на посебните категории на податоци кои откриваат расно или етничко потекло, политички ставови, религиозни или филозофски убедувања или членства во синдикални организации, обработката на генетски податоци, биометриски податоци за целите на уникатно идентификување на физичкото лице, **податоци кои се однесуваат на здравјето** или на сексуалниот живот или ориентација на физичкото лице<sup>10</sup>.

Секако, исклучоци од ова правно правило постојат и се сметаат за законски во ситуации кога субјектот дал изречна согласност за обработка на неговите податоци, ако тоа го налагаат посебни закони, обработката е неопходна за извршување работи од јавен интерес, за заштита на суштинските интереси на субјектот на личните податоци, податоци кои очигледно се објавени јавно од субјектот на личните податоци и други ситуации наведени во член 9 став 2 од Регулативата.

### 2.3.1.2. ИНФОРМАЦИИ И ПРИСТАП ДО ЛИЧНИТЕ ПОДАТОЦИ

Дел 2 од Регулативата е посветен на информации и пристап до личните податоци нормирани во неколку членови, регулирајќи прашања како право на пристап на субјектот на личните податоци, правото да се биде избришан, правото на ограничување, обврската за известување или за бришење на личните податоци и правото на преносливост на податоци. Од интерес за оваа анализа е правото на ограничување на обработката, содржано во членот 18. Член 18 од Општата регулатива за заштита на податоци (GDPR) поставува важен механизам кој гарантира дека субјектите на податоците имаат можност да побараат ограничување на обработката на нивните лични податоци во одредени ситуации. Овој член обезбедува правна заштита и ги дефинира околностите под кои може да се побара ограничување на обработката. Според член 18, субјектите на податоците можат да побараат ограничување на обработката кога е исполнет барем еден од следниве услови:

- Точноста на податоците е оспорена од страна на субјектот на податоците. Во ваков случај, ограничувањето на обработката трае за период кој е потребен за да се потврди нивната точност.
- Обработката е незаконска, а субјектот на податоците се противи на бришење на податоците и бара ограничување на нивната обработка.
- На контролорот повеќе не му се потребни податоците за целите на обработката, но тие се потребни за субјектот на податоците заради утврдување, остварување или одбрана од правни барања.
- Субјектот на податоците се спротивставил на обработката во согласност со член 21(1), во текот на проверката дали легитимните основи на контролорот ги надминуваат (се посилен од) основите на субјектот на податоците.

Кога обработката е ограничена во согласност со став 1 од членот 18, таквите лични податоци, со исклучок на складирањето, може да се обработуваат само со согласност на субјектот на податоците или за воспоставување, остварување или одбрана на правни

---

10 Чл. 9 од GDPR регулативата.

побарувања, во случај на заштита на правата на друго физичко или правно лице, или поради важен јавен интерес на Унијата или на земјата членка. Кога ќе се применат мерките за ограничување на обработката на лични податоци, лицето на кое се однесуваат податоците ќе биде информирано од страна на контролорот пред да се отстрани ограничувањето на обработката. Овој процес на известување е важен бидејќи го осигурува правото на субјектот на податоците да биде свесен за сите промени во статусот на неговите податоци, особено кога тие се обработуваат под ограничени услови. Контролорот има обврска да ги обезбеди сите потребни информации пред да го продолжи или да го укине ограничувањето на обработката на податоците, како и да го задржи транспарентниот процес.

Европската јуриспруденција ја смета заштитата на личните податоци за основно човеково право воспоставено со потпишувањето на Лисабонскиот договор од 2007 година, и ова право е препознатливо во гореспоменатите акти (Договорот за функционирање на ЕУ и Европската повелба за човекови права). Медицинските податоци се сметаат за посебна категорија на лични податоци, поради чија сензибилност се донесува цел сет на акти и правила во кој централна позиција зазема заштитата на личните, односно медицинските податоци. Со ваквото толкување, фокусот се става врз давањето контрола на пациентот сам да ги контролира сопствените медицински податоци.

## 2.4. ЗАКОН ЗА ПОДАТОЦИ НА ЕУ И ЕВРОПСКИ ПРОСТОР ЗА ЗДРАВСТВЕНИ ПОДАТОЦИ (EUROPEAN HEALTH DATA SPACE- EHDS)

Во 2020 година беше донесена Европската стратегија за податоци<sup>11</sup>, чии цели во суштина беа базирани врз 2 важни акта, а тоа е Законот за управување со податоци и Законот за медицински податоци (Health Data Act). Овој ЕУ-акт стапи на сила во јануари 2024 година и тој е столб на европската стратегија за податоци. Неговата главна цел е да ја направи Европа лидер во економијата на податоци преку искористување на потенцијалот на постојано зголемување на количината индустриски податоци, со цел да има корист за европската економија и општество. Европскиот простор за здравствени податоци ќе биде клучен столб на силната Европска здравствена Унија. Во пролетта 2024 година, Европскиот парламент и Советот постигнаа политички договор за Предлогот на Комисијата за EHDS. Ова има за цел:

- » да им овозможи на поединците да преземат контрола врз своите здравствени податоци и да ја олеснат размената на податоци за испорака на здравствена заштита низ ЕУ (примарна употреба на податоци),
- » поттикнување вистински единствен пазар за системи за електронска здравствена евиденција, и
- » да обезбеди конзистентен, доверлив и ефикасен систем за повторна

11 [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_20\\_273](https://ec.europa.eu/commission/presscorner/detail/en/ip_20_273), последен пат пристапено 10.11.2024.

употреба на здравствените податоци за истражување, иновации, креирање политики и регулаторни активности (секундарна употреба на податоци).

Оттука, довербата е основен услов за успехот на Европскиот простор за здравствени податоци. EHDS ќе обезбеди доверлива поставка за безбеден пристап и за обработка на широк опсег од здравствени податоци низ целата Унија.

За целите на оваа анализа, треба да се земе предвид дека станува збор за електронски здравствени податоци, односно предмет на анализа не се здравствените податоци и евиденции во хартиена форма.



# 3

## РЕГУЛАЦИЈА НА МЕДИЦИНСКИТЕ ПОДАТОЦИ ВО ЕСТОНИЈА

*“I should have called the Estonians when we were setting up our health care website.”*

- Barack Obama<sup>12</sup>

Анализа објавена во 2013 година покажува дека естонските решенија во е-здравството се меѓу водечките во Европа. Во септември 2008 година започнува да функционира нивниот систем за е-здравство, т.н. Естонски национален здравствен информативен систем (Estonian National Health Information System – ENHIS). ENHIS е национална централна електронска база на податоци за обработка на здравствени досиеја на сите пациенти кои примаат здравствени услуги од кој било естонски давател на здравствени услуги<sup>13</sup>. На овој начин се воведува обврска за **сите официјално признати даватели на здравствени услуги да ги прикачат електронските здравствени картони ЕЗК (EHR) на своите пациенти на ENHIS, а пациентите можат да ги видат своите ЕЗК складирани на ENHIS на платформата за пациенти „Моето е-здравје“.**

Во декември 2023, естонскиот Фонд за здравствено осигурување и Центарот за информациски системи за здравје и благосостојба (TEHIK) го лансираат новиот Здравствен портал. Со ова стартува новиот портал за пациентите, а стариот портал Digilugu бил затворен<sup>14</sup>. Новиот портал е значително технолошки унапреден,

12 <https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf>

13 Milieu Ltd and Time.lex: Overview of the national laws on electronic health records in the EU Member States – National Report for the Republic of Estonia, 13 мај 2014, а во врска со измените и дополнувањата на Законот за организирање на здравствените услуги од 2008 година, Глава 5, членовите 59<sup>1</sup> – 59<sup>4</sup>.

14 Информацијата е достапна на следниот веб-линк: <https://www.tehik.ee/en/uudis/new->

со нови е-здравствени алатки. Имено, на Здравствениот портал, преку алатката „Моја контролна табла“, се прикажуваат претстојни состаноци, рецепти, прегледи, тестови и состаноци во последните шест месеци, како и препораките за вакцинација.

Како нова функција, луѓето имаат пристап до „Мојата здравствена историја“, што ќе им овозможи детално да филтрираат информации за состаноци, тестови, прегледи, вакцини и информации поврзани со итна медицинска помош, хоспитализација или операции. Во 2024 година се работи на нови ИТ-решенија додадени на здравствениот портал, со што целта е да се зголеми личното учество и одговорност на луѓето во донесувањето одлуки поврзани со здравјето и со ова се креира пристап фокусиран на пациентот. Во етапите на имплементирање и ажурирање на здравствениот портал, креаторите укажуваа дека една од карактеристиките што најмногу ја бараат корисниците е можноста да се добиваат известувања за работи како што се рецепти, вакцини и посети на лекар<sup>15</sup>.

Оваа платформа во иднина може постојано да се ажурира со нови и неопходни функции, без да се заменува со нова. Она што му дава посебна важност при креирањето на овој портал е дека на луѓето им е овозможено да дадат повратни информации за новиот здравствен портал преку копчето „Повратни информации“ или директно преку е-поштата за помош на ТЕНИК. Додадена е и можност за пополнување здравствени податоци за себе и за најблиските и пополнување прашалници за здравствена проценка пред термините. Со ова ќе се овозможи непречено движење на здравствените податоци во рамките на здравствениот систем, максимизирајќи ја користа на пациентите во следењето и управувањето со нивното здравје. Откако ќе се интегрира и оваа алатка, на пациентите ќе им се овозможи да закажуваат термини или да ги променуваат и да ги откажуваат овие термини.

Специјален закон кој го уредува основањето на EHNIS, го регулира функционирањето на овој национален интегриран здравствен систем и ја регулира заштитата и обработката на здравствените податоци е Законот за организација на здравствените услуги (Health Service Organization Act) и Уредбата (Статутот) на Здравствено-информатичкиот систем, како и Регулативата за содржината на податоци на документите проследени до здравствениот информативен систем и условите и аранжманите за чување на овие документи од 18 септември 2008 година (Regulation of 18 September 2008 on Data Content of Documents Forwarded to Health Information System and the Conditions and Arrangements for Retention of these Documents)<sup>16</sup>.

Денес Естонија користи КСИ блокчејн (KSI Blockchain) технологија во здравствениот систем. KSI е блокчејн технологија дизајнирана во Естонија и се користи на глобално ниво за да се осигури дека мрежите, системите и податоците не се компромитирани, задржувајќи 100 приватност на податоците<sup>17</sup>.

Оваа технологија се користи за да се обезбеди интегритет на преземените електронски медицински досиеја, како и евиденции/записи (logs) за пристап до системот. Естонскиот

---

[health-portal-has-replaced-digilugu](#)

15 Информацијата е достапна на следниот веб-линк: <https://www.tehik.ee/en/uudis/new-health-portal-brings-peoples-health-information-together>

16 Overview of the national laws on electronic health records in the EU Member States - National Report for the Republic of Estonia,/iii [https://health.ec.europa.eu/system/files/2016-11/laws\\_estonia\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/laws_estonia_en_0.pdf) . Пристапено 30.9.2024.

17 Информацијата е достапна на следниот линк: <https://e-estonia.com/solutions/cyber-security/ksi-blockchain/>

државен здравствен регистар е поддржан од КСИ блокчејн технологијата<sup>18</sup>.

### 3.1. ПРАВНА РАМКА – КРАТОК ОСВРТ

Правната рамка може да се сведе на неколку важни акти:

- » **Општа Регулатива за заштита на податоци во ЕУ**, донесена 2016 година. Повеќе детали за ова, видете supra 2.3.1.
- » **Закон за заштита на личните податоци на Естонија** ([Personal Data Protection Act–Riigi Teataja](#)), донесен 2018 година.
- » **Закон за јавна здравствена заштита** ([Public Health Act–Riigi Teataja](#)), донесен 1995 година, а неколкупати изменет и дополнет до 2023 година. Целта на овој закон е заштита на здравјето на луѓето, спречување на болести и унапредување на здравјето, што треба да се постигне преку извршување на должностите на државата, на локалната самоуправа, на правните лица од јавното право, на правните лица од приватното право и на физичките лица, како и преку системот на национални и локални мерки.
- » **Закон за организација на здравствените услуги** ([Health Services Organisation Act–Riigi Teataja](#)), донесен во 2002 година, стапува на сила 2003 година и до денес има многубројни измени и дополнувања. Овој закон ја обезбедува организацијата и условите за давање здравствени услуги и постапката за управување, финансирање и надзор на здравствената заштита. Во 2008 година, со овој закон се воведува Информатичкиот здравствен систем во Естонија. Во 2013 година се воведуваат одредби за прекуграничните здравствени услуги, со што се организираат содржините и начините на поврзување со давањето здравствени услуги во рамките на ЕУ, и за ограничување на пристапот за прием на прекугранични здравствени услуги во Естонија. Во 2018 година е воведена Платформата за размена на прекугранични здравствени евиденции, а во 2022 година, националниот Здравствено-административен информатички систем (под глава 1, член 26<sup>4</sup>). Со овој закон се прави сеопфатна рамка за давањето, пристапот, преносот на медицинските услуги и податоци, како и правата и обврските на сите чинители во овој комплексен „екосистем“.

**Уредба за информатичкиот здравствен систем** ([Statutes of the Health Information System – Riigi Teataja](#)). Станува збор за подзаконски акт кој произлегува од Законот за организација на здравствените услуги, во кој се дефинира рамката за функционирање на националниот здравствен информативен систем, вклучувајќи ја и употребата на електронска здравствена евиденција и е-порталот за пациенти, правата и обврските на давателите на услугите и на пациентите. Со овој акт се гарантира дека сите трансфери (пренос) на податоци се безбедни и дека пациентите можат да пристапат до своите здравствени податоци преку е-порталот со користење на своите електронски лични карти.

---

18 Информацијата е достапна на следниот линк: <https://www.pwc.com/gx/en/services/legal/tech/assets/estonia-the-digital-republic-secured-by-blockchain.pdf>, стр. 7.  
Последен пат пристапено 1.11.2024.

### 3.2. ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ НА ЕСТОНИЈА (PERSONAL DATA PROTECTION ACT – RIIGI TEATAJA)

Овој закон е донесен во 2018 година, а стапи на сила во 2019 година<sup>19</sup>. Се однесува на заштита на физички лица при обработка на лични податоци и ги доуредува и ги дополнува одредбите содржани во GDPR-регулативата. Со овој национален закон се воспоставуваат стандардите за спроведување на GDPR-регулативата и стандардите за транспонирање на Директивата за заштита на физичките лица во однос на обработката на личните податоци од страна на надлежните органи за целите на превенција, истрага, откривање или гонење кривични дела или извршување кривични казни и за слободно движење на таквите податоци; односно се воспоставува постапка за вршење државен надзор над почитувањето на условите за обработка на личните податоци и одговорност за повреда на условите за обработка на лични податоци<sup>20</sup>. Законот за заштита на личните податоци се применува врз сите чувствителни прашања за заштита на личните податоци, помеѓу кои се и здравствените податоци, иако никаде во законот не се опфатени како посебни одредби, туку нивната примена упатува на одредбите од GDPR-регулативата. Во овој закон, регулирани се и специфичните основи за обработка на личните податоци кои се однесуваат на обработка на лични податоци, како, на пример, за новинарски цели.

### 3.3. ЗАКОН ЗА ЈАВНА ЗДРАВСТВЕНА ЗАШТИТА (PUBLIC HEALTH ACT – RIIGI TEATAJA)

Целта на овој закон е заштита на здравјето на луѓето, спречување на болести и унапредување на здравјето, што треба да се постигне преку извршување на должностите на државата, на локалните самоуправи, на правните лица од јавното право, на правните лица од приватното право и на физичките лица и преку системот на национални и локални мерки. Во **член 2** од овој закон се дефинирани основните поими кои се однесуваат на јавно здравје, здравствена заштита, промоција на здравјето, здравјето на населението, превенција на зарази итн.

Во интерес на нашето истражување се следните членови:

- » **Член 8 став 1 точка 12**, каде што се укажува на надлежноста на Министерството за социјални работи да собира информации за здравјето на населението и да обработува лични податоци за развој и спроведување на националните здравствени и здравствени политики во согласност со Законот за заштита на личните податоци и со Законот за информации од јавен карактер.
- » **Член 11**, каде што се прикажани општи податоци за жителите на управната единица или регион и преглед на здравствената состојба и на благосостојбата на населението и детерминанти на здравјето на управната единица или регион.

---

19 Претходниот закон беше донесен 15.2.2007, влегува на сила на 1.1.2008 година, ревидиран и влезен во сила 16.1.2016 година со важност до 14.1.2019. <https://www.riigiteataja.ee/akt/106012016010>, последен пат пристапено 28.10.2024. Сега актуелен, донесен 2018 год., на сила од 2019 год. <https://www.riigiteataja.ee/en/eli/ee/523012019001/consolide/current>

20 Чл.1 Закон за заштита на личните податоци, <https://www.riigiteataja.ee/en/eli/ee/523012019001/consolide/current>

- » **Член 14<sup>1</sup>**, каде што се регулираат државните бази на податоци/регистри. Податоците од базата на податоци или информацискиот систем кои содржат здравствени податоци (како што се регистарот за рак, регистарот за туберкулоза, информацискиот систем за бременост) се издаваат во неперсонализирана форма. Персонализираните податоци се издаваат со согласност на субјектот на податоците или за научни и историски истражувања, за статистика или за утврдување на вистината во кривична постапка.

### 3.4. ЗАКОН ЗА ОРГАНИЗАЦИЈА НА ЗДРАВСТВЕНИТЕ УСЛУГИ

Овој закон ја обезбедува организацијата и условите за давање здравствени услуги и постапката за управување, финансирање и надзор на здравствената заштита. Ги уредува правата и обврските на пациентите и на давателите на здравствените услуги, обработката, пристапот и трансферот до медицинските податоци на пациентите. Содржината на овој закон опфаќа повеќе чинители со различни права, статус и надлежности.

Имајќи ја предвид сложената структура и поврзаност на различни чинители во е-здравството, а со цел воспоставување стабилна врска помеѓу различните учесници во здравствениот систем и спроведување на националните закони и ЕУ-регулативи и стандарди, ќе се споменат дел од круцијалните правни субјекти, односно контролори и овластени копроцесори на медицинските податоци: Министерството за социјални работи (Ministry for Social Affairs), Фондот за здравствено осигурување (Estonian Health Insurance Fund- Tervisekassa)<sup>21</sup>, Естонската банка за дигитални дијагностички слики (The Estonian Health-care Picture Bank – SA Eesti Tervishoiu Pildipank), Одборот за здравство (Health Board), Центарот за информациски системи за здравје и благосостојба (the Center for Health and Welfare Information Systems- HWISC), Естонскиот национален здравствен информативен систем (Estonian National Health Information System – ENHIS), Етичкиот комитет за истражување, Инспекторатот за заштита на личните податоци (Estonian Data Protection Inspectorate) и други.

Со овој закон се регулира пристапот до медицинските податоци од Националниот здравствен систем и се гарантира правото на пристап до личните податоци на пациентот.

#### 3.4.1. ПРАВА И ОБВРСКИ НА ДАВАТЕЛИТЕ НА ЗДРАВСТВЕНИТЕ УСЛУГИ

Со измените и дополнувањата од март 2019 година на Законот за организација на здравствените услуги, давателите на здравствена заштита, кои имаат законска обврска да ја обезбедат доверливост, **имаат право да обработуваат лични податоци потребни за давање здравствена услуга, вклучително и лични податоци од посебни категории, без дозвола на субјектот на податоците.**

21 <https://www.tervisekassa.ee/en/people/my-data-health-portal-state-portal>

Со измените и дополнувањата од 2023 година, „правото на обработка на податоци за планирање на давањето здравствени услуги“ делумно се проширува и на матичниот лекар и на здравствените услуги во училиштата, давателите на специјализирана медицинска нега, независна физиотерапија, говорна терапија, психолошки третман, нега и акушерска нега, само по постоење претходно склучен договор за здравствени услуги.

Естонското право содржи специфични барања кога станува збор за регулирање на безбедносното ниво на EHR во ENHIS системот. Нивото на заштита на овој систем е категоризирано како „високо“ и подлежи на ревизија секои две години<sup>22</sup>. Во принцип, ова се однесува на безбедносните нивоа утврдени за сите информациски системи управувани од јавни субјекти. **Во здравствениот сектор им се овозможува на пациентите да се откажат од споделување на податоците од ENHIS: пациентот може да ги направи сите или одредени EHR недостапни во ENHIS.** За да се повика на тоа право, пациентот мора да поднесе барање до неговиот или нејзиниот давател на здравствени услуги (ефективни за податоците на ENHIS создадени од тој давател) или до Министерството за социјални работи (применливо за сите податоци на ENHIS).

### 3.4.2. ПРАВА И ОБВРСКИ НА ПАЦИЕНТИТЕ

Секој човек во Естонија што посетил лекар има е-здравствено досие (e-Health record) и за него се води е-здравствена евиденција. Имено, 100% од пациентите во Естонија имаат дигитално досие. Е-здравствената евиденција всушност ги повлекува податоците по потреба од различни даватели на здравствени услуги, кои можеби користат различни системи, и ги прикажува во стандарден формат преку порталот Е-пациент. Оваа дигитална алатка функционира како централизирана, национална база на податоци. Податоците се видливи за сите лекари кои лекуваат пациенти и пациентите можат да ги видат сопствените податоци и да видат кој пристапил до нивните податоци.

Пациентите имаат обврска да дадат точни податоци и да ги информираат лекарите и здравствените работници за каков било здравствен индикатор кој би можел да биде релевантен за препишување на соодветниот третман. Меѓутоа, согласноста на пациентот не е неопходна за да се креира ЕЗК или да се сподели ЕЗК со цел да се обезбеди здравствена заштита на пациентот. Понатаму, пациентите имаат пристап до нивните е-здравствени картони (ЕЗК) и имаат пристап до безбедна и висококвалитетна здравствена заштита во друга земја на ЕУ. Исто така, **естонското право им овозможува на пациентите да се откажат од споделување на податоците од ENHIS: пациентот може да ги направи сите или одредени е-здравствени евиденции (EHR) недостапни во ENHIS.** За да се повика на тоа право, пациентот мора да поднесе барање до неговиот или нејзиниот давател на здравствени услуги (ефективни за податоците на ENHIS создадени од тој давател) или до Министерството за социјални работи (применливо за сите податоци на ENHIS).

Со Директивата 2011/24/ЕУ на Европскиот парламент и на Советот од 9 март 2011 година за примена на правата на пациентите во прекуграничната здравствена заштита, овозможено е да се добие медицински третман во друга земја држава на ЕУ. За таа цел, потребна е прекугранична соработка на давателите на здравствените услуги и на здравствените установи и ова усогласување претставува еден од главните предизвици на поголем дел од земјите членки на Унијата. Според извештајот од 2014 година, за анализираниот период од 2013 година, Естонија е земја членка на ЕУ која за исполнување на овие услуги во тој

---

22 Член 2<sup>2</sup>, Уредба (Статут) на здравствено-информацискиот систем.

период се соочувала само со неколку правни и технички бариери за нивниот ENHIS-систем да споделува здравствени податоци со другите земји членки на ЕУ, особено со земјите каде што има многу Естонци, а тоа се Финска и Ирска и, надвор од Европа, Австралија. Пациентите имаат право да го ограничат или да го забранат пристапот до нивните податоци со соодветен поднесок.

### 3.4.2.1. ОГРАНИЧУВАЊЕ (РЕСТРИКЦИЈА) НА ПРИСТАПОТ ЗА ПРИЕМ НА ПРЕКУГРАНИЧНИ ЗДРАВСТВЕНИ УСЛУГИ

На предлог на надзорниот одбор на Фондот за здравствено осигурување, надлежниот министер може со пропис да утврди ограничување на пристапот за пациентите опфатени со здравствено осигурување во друга земја членка на Европската Унија за добивање прекугранични здравствени услуги во Естонија.

### 3.4.2.2. ДАВАЊЕ ПРИСТАП ДО ПОДАТОЦИ ВО ЗДРАВСТВЕНИОТ ИНФОРМАТИВЕН СИСТЕМ (ПРАВОТО НА ПАЦИЕНТОТ ДА ГО ОГРАНИЧИ ПРИСТАПОТ)

Со член 59<sup>3</sup> од Законот за организација на здравствените услуги, на пациентот му се овозможува да ги испита неговите/нејзините лични податоци преку овластено лице (здравствен професионалец), а за таа цел, давателот на здравствена заштита може да постави временско ограничување за препраќање податоци до здравствениот информацискиот систем (ЗИС)<sup>23</sup>. Пристап до податоците во ЗИС имаат давателите на здравствените услуги кои имаат лиценца и на кои во посебни ситуации со закон им е дозволен пристап. Освен на овие лица, дозволен е пристап до личните податоци во Здравствениот информациски систем за учество во давањето здравствени услуги и на следниве лица:

- студент кој е на медицинска обука и кој ги завршил задолжителните предмети од наставната програма на IV година,
- професионален терапевт,
- оптометрист,
- радиолошки техничар и
- регистрирани лица кои стекнале квалификации во други странски држави.

Дополнително, оваа листа може да се прошири со одобрување од страна на ресорниот министер.

Сепак, Законот дозволува пациентот да го забрани правото на пристап на лицата набројани погоре<sup>24</sup>. Во ваква ситуација, давателот на здравствената услуга веднаш ќе забрани пристап до податоците на пациентот во ЗИС.

23 Член 59<sup>3</sup> ст. 1 од Законот за организација на здравствените услуги.

24 Чл. 59<sup>3</sup> ст. 3 Закон за организација на здравствените услуги.

### 3.4.3. ЭСТОНСКИ НАЦИОНАЛЕН ЗДРАВСТВЕН ИНФОРМАЦИСКИ СИСТЕМ (ESTONIAN NATIONAL HEALTH INFORMATION SYSTEM - ENHIS)

Эстонскиот национален здравствен информациски систем (Health Information System) е воспоставен врз основа на член 59<sup>3</sup> од Законот за организација на здравствените услуги во 2008 година. Информацискиот систем е составен од 3 бази: 1. централната база на податоци на информацискиот систем, 2. базата на податоци за медицинска евиденција и 3. базата за складирање податоци.

**Централната база на податоци на информацискиот систем** се состои од следните збирки на податоци: база на податоци обезбедена од субјектот на податоците, здравствени податоци обезбедени од давателите на здравствени услуги и други лица, база на податоци на националниот дигитален регистар и база на податоци за усогласеност. **Базата на податоци за медицинска евиденција** се состои од медицинска евиденција која се однесува на субјектот на податоците. **Базата на податоци за складирање**, пак, се состои од псевдонимизирани лични податоци обезбедени од централната база на податоци и од давателите на податоци, што не дозволува идентификација. Овие податоци се обработени на таков начин што медицинските податоци повеќе не можат да се поврзат со одреден субјект/пациент (псевдонимизирани), поради што и не можат да се третираат како сензитивни податоци<sup>25</sup>.

#### 3.4.3.1. КОНТРОЛА И БЕЗБЕДНОСТ НА ИНФОРМАТИЧКИОТ ЗДРАВСТВЕН СИСТЕМ

Во согласност со Законот за организација на здравствените услуги, Здравствениот одбор е орган кој го контролира Информатичкиот здравствен систем. Во согласност со Уредбата, безбедноста на податоците во овој систем е категоризирана и поделена во безбедносни класи: доверливост, интегритет, достапност. Безбедноста на информатичкиот систем е класифицирана како „висока“. Исто така, Здравствениот одбор ги објавува податоците за квалификацијата и лиценцата за дејност на здравствените работници регистрирани во информативниот систем на здравствената управа за јавна употреба, во обем предвиден во Уредбата на информатичкиот систем на здравствената управа.

Како контролори и овластени обработувачи на податоците законски се јавуваат неколку субјекти, кои се носители на одговорноста. Имено, заедничката одговорност за Информатичкиот здравствен систем ја имаат Министерството за социјални работи и Фондот за здравствено осигурување. Овластен обработувач на информацискиот систем е Центарот за информациски системи за здравје и благосостојба (Health and Welfare Information Systems Centre – HWISC), кој го одржува, го управува и го развива информацискиот систем, ги обработува податоците и ги исполнува другите обврски наметнати од одговорниот обработувач (процесор).

Исто така, како овластен обработувач (процесор) на здравствениот информацискиот систем е Picture Bank – Eesti Tervishoiu Pildipank, која ги управува, ги обработува и ги архивира медицинските податоци и евиденција, и ги исполнува обврските наложени од одговорниот обработувач врз основа на законската регулатива и според пропишаните

---

25 Чл.2<sup>1</sup> од Уредбата (Статутот) на ЗИС.



барања. Исто така, како овластен процесор се јавува Одборот за социјално осигурување, кој обезбедува објавување на податоците на сертификатите за биде во согласност со законските барања, односно му помага на субјектот на податоците при пополнување на апликацијата, при издавањето сертификати, потврди за усогласеност поврзани со ширењето на коронавирусот SARS-CoV-2, кој ја предизвикува болеста КОВИД-19. На овој начин, естонското законодавство пристапило кон директно законско решение како последица од последната светска здравствена криза, која на глобално ниво создаде простор за кумулирање, пренос и обработка на голем обем на електронски здравствени податоци кај различни овластени субјекти и други даватели на здравствени услуги.

### 3.4.3.2. ПРИСТАП ДО ЕКЗ, Е-РЕЦЕПТИ (ДИГИТАЛНИ РЕЦЕПТИ)

**До податоците на ENHIS мора да се пристапи само заради обезбедување здравствени услуги. Секој здравствен работник може да пристапи до податоците на ENHIS за секој пациент, доколку давателот на здравствена заштита што го вработува здравствениот работник има важечка лиценца за вршење активност во Естонија и доколку пациентот не забранил пристап до неговите или нејзините податоци ENHIS.** Здравствените работници имаат законска обврска да го ажурираат ENHIS кога обезбедуваат здравствена услуга на пациентот. Пред да се добие пристап до податоците на ENHIS, се проверува валидноста на лиценцата за активност на давателот на здравствена заштита и регистрацијата на здравствениот работник.

Понатаму, **пациентите се сопственици на своите здравствени податоци и можат да го видат дневникот за пристап до нивните податоци ENHIS на платформата за пациенти „Мое е-здравје“.** Пациентите по правило имаат целосен пристап до сите нивни податоци од ENHIS, но во одредени ситуации, во согласност со законот, давателот на здравствените услуги може временски да го лимитира пристапот до податоците на пациентот. Со цел да се заштити животот или здравјето на пациентот, давателот на здравствена заштита може да постави временско ограничување при препраќање податоци до Информацискиот систем во текот на кое пациентот може прво да ги испита своите лични податоци само преку здравствен работник<sup>26</sup>.

### 3.4.4. ЦЕНТАР ЗА ИНФОРМАЦИСКИ СИСТЕМИ ЗА ЗДРАВЈЕ И БЛАГОСОСТОЈБА (HEALTH AND WELFARE INFORMATION SYSTEMS CENTRE–HWISC)

Центарот за информациски системи за здравје и благосостојба е ИКТ компетентен центар основан на 1 јануари 2017 година и тој ги консолидира улогите и одговорностите на поранешното одделение за ИКТ на Министерството за социјални работи и естонското е-здравство (Estonian eHealth Foundation). Веб-

26

Чл. 59<sup>3</sup> ст.1, Закон за организација на здравствените услуги.

страницата „Здравствен портал“ (Terviseportaal.ee)<sup>27</sup> е дел од HWISC и користи одредени технолошки алатки и принципи за креирање содржина, со цел да овозможи полесен пристап до содржината на здравствениот портал за лица со оштетен вид, слепи, глуви или когнитивно оштетени лица. Дополнително, можно е да се подобри пристапноста до информациите со конфигурирање на компјутерот на ниво на прелистувач и оперативен систем<sup>28</sup>.

### **3.4.5. ЕСТОНСКА БАНКА ЗА ДИГИТАЛНИ ДИЈАГНОСТИЧКИ СЛИКИ (THE ESTONIAN HEALTHCARE PICTURE BANK – SA EESTI TERVISHOIU PILDIPANK)**

Естонската банка за дигитални дијагностички слики од областа на здравствена заштита е основана од Регионалната болница во Северна Естонија и од Универзитетската болница Тарту во 2006 година. На почетокот од основањето, целта на оваа институција е да им понуди на давателите на здравствени услуги можност да архивираат и да прикажуваат дигитални дијагностички слики. Давателите на здравствена заштита се обврзани да ги задржат дијагностичките снимки направени за време на давањето здравствени услуги 30 години, а Банката (Picture Bank) ја нуди услугата за архивирање и прикажување за исполнување на оваа обврска. Податоците архивирани во Банката на слики се на давателот на здравствена заштита кој ги испратил податоците на архивирање. Како давател на услуги за архивирање, Банката на слики е овластен процесор на сликите испратени за архивирање и на други лични податоци поврзани со нив.

Од 1.9.2014 година, Банката е и овластен процесор на здравствениот информативен систем и сите даватели на здравствени услуги се обврзани да испраќаат слики во формат DICOM направени за време на давањето здравствени услуги.

### **3.4.6. ФОНД ЗА ЗДРАВСТВЕНО ОСИГУРУВАЊЕ (ESTONIAN HEALTH INSURANCE FUND - TERVISEKASSA)**

Естонскиот фонд за здравствено осигурување нуди многубројни дигитални алатки за здравствената заштита на пациентите<sup>29</sup>. За целите на ова истражување, ќе го споменеме е-порталот „Мое здравје“, составен од портал Здравје: Здравствен портал – Health portal и Државен портал – State portal<sup>30</sup>. Пристапот до содржините на двата портали се овозможени со лична идентификација (ID card) или мобилна лична идентификација (mobile ID-card). Во здравствениот портал сите може да ги видат своите здравствени информации и осигурениците имаат увид во фактурите за лекување кои Фондот ги платил до медицинските установи. Исто така, преку овој портал може:

- » Да се направи увид во медицинските документи подготвени и испратени до здравствениот информативен систем од лекари,

---

27 Повеќе за ова *infra*

28 <https://www.terviseportaal.ee/en/ligipaasetavus/>, последен пат пристапено на 16.12.2024.

29 <https://www.tervisekassa.ee/en>

30 <https://www.tervisekassa.ee/en/people/my-data-health-portal-state-portal>

- » Да се провери валидноста на здравствен сертификат,
- » Да се назначи лице кое во име на пациентот ќе извршува различни активности (на пример, купување препишан лек),
- » Да се поднесе изјава за волја, и
- » Да се провери кога и од кого се прегледани здравствените информации на пациентот.

### **3.5. УРЕДБА НА ЗДРАВСТВЕНИОТ ИНФОРМАЦИСКИ СИСТЕМ**

Овој подзаконски акт го воспоставува и го структурира целиот ЗИС, ја определува улогата, овластувањата и обврските на контролорите, на давателите на здравствени услуги како даватели на податоци, го уредува трансферот на податоци до ЗИС, го одржува системот и го нормира пристапот и измената на податоците до/во ЗИС.

Министерството за социјални работи и Фондот за здравствено осигурување, како коодговорни обработувачи, во соработка со овластениот процесор (Центар за информациски системи за здравје и благосостојба – HWISC, Picture Bank - – Eesti Tervishoiu Pildipank и Одборот за социјално осигурување) организираат креирање е-услуги, развој на системот и електронска размена на податоци на информацискиот систем со други бази на податоци и вршат други задачи специфични за одговорниот процесор.

#### **3.5.1. ТРАНСФЕР (ПРЕНЕСУВАЊЕ) НА ПОДАТОЦИТЕ ВО ИНФОРМАЦИСКИОТ СИСТЕМ**

Преносот на податоци (овластените субјекти и начинот на пренос на податоците) во информацискиот систем се утврдени во Глава 2 (член 5 и член 6) од Уредбата. Овластени субјекти кои може да прават трансфер на личите податоци се давателите на здравствените услуги и други лица (контролорот надлежен за регистарот на населението, контролорот задолжен за управување со здравствената заштита, Фондот за здравствено осигурување, Процесорот задолжен за центарот за рецепти, Естонскиот фонд за осигурување за невработеност, Агенцијата за одбрана и други субјекти таксативно наброени во Уредбата).

#### **3.5.2. ПРИСТАП ДО ПОДАТОЦИТЕ НА ИНФОРМАЦИСКИОТ СИСТЕМ И ДО ОБЈАВУВАЊЕТО ПОДАТОЦИ**

Член 10 од Уредбата ги содржи општите барања и услови за директен пристап до информатичкиот систем. Овластениот обработувач на информацискиот систем води евиденција за времето на издавање на податоците од информацискиот систем, составот на издадените податоци, примателите на податоците и начинот

на издавање на податоците. Овластениот обработувач на информацискиот систем има право да го ограничи или да го забрани пристапот до податоците доколку, поради размена на податоци, може да настане или настанал ризик за доверливоста или интегритетот на информацискиот систем.

**Давателот на здравствена заштита има пристап до личните податоци во информацискиот систем заради планирање на давањето здравствени услуги, склучувањето и извршувањето на договорот за давање услуги.** Член 12 овозможува пристап и на трети лица кои имаат законско право на пристап до личните податоци во информацискиот систем. На овие лица може да им се издаваат податоци од информацискиот систем само до степен што е предвиден со закон.

### 3.5.3. ПРАВА НА СУБЈЕКТОТ НА ПОДАТОЦИТЕ

Уредбата, односно членовите 15-20 им ги овозможуваат следниве права на субјектите на податоците:

- » да добиваат информации и лични податоци за себе,
- » да добиваат информации и лични податоци за себе во согласност со постапката утврдена со закон,
- » да вршат дејствија, да поднесуваат и да менуваат податоци,
- » да бараат корекција на неточни лични податоци,
- » да одбијат пристап до личните податоци,
- » да дозволат на трети лица пристап до личните податоци.

### 3.6. КРАТКО РЕЗИМЕ

Естонија се смета за најнапредното дигитално општество во светот. Приватноста и сопственоста на податоците се централни начела на е-владеењето на Естонија и се длабоко вкоренети во системот за е-здравство уште од 2008 година. Според овие принципи, здравствените податоци во основа му припаѓаат на засегнатото лице. Сите даватели на здравствени услуги се обврзани да доставуваат податоци до EHIS, но пристапот до овие информации е строго контролиран. Сите официјално признати даватели на здравствени услуги имаат законска обврска да ги прикачат електронските здравствени картони ЕЗК (EHR) на своите пациенти на ENHIS. **Само лиценцирани медицински професионалци можат да пристапат до системот, а пациентите имаат право да ја видат (прегледаат) сопствената здравствена евиденција зачувана во централната база на податоци. Покрај тоа, пациентите имаат можност да го ограничат пристапот до нивните податоци и имаат увид кога и од кого биле видени нивните здравствени информации.**

Собирањето, обработката, пристапот до и трансферот на медицинските податоци се опфатени со поголем број правни акти и легислатива со кои естонскиот законодавец и релевантните чинители во креирањето на правната рамка успеале да ги регулираат/ да предвидат решенија кои произлегуваат од дигитализацијата на медицинските услуги и податоци. Посебен закон што го уредува основањето на ENHIS и го регулира функционирањето на овој национален интегриран здравствен систем и ја регулира

заштитата и обработката на здравствените податоци е Законот за организација на здравствените услуги (Health Service Organization Act) и Уредбата на здравствено-информатичкиот систем. Структурата на информатичкиот систем, контролорите и овластените лица таксативно се набројани и јасно се дефинирани нивните овластувања и надлежности, а нивните обврски и одговорности прецизно се утврдени и регулирани. Архитектурата на естонскиот здравствен информатички систем внимателно е конструирана и континуирано се надоградува и усовршува. Последователно, интероперабилноста помеѓу учесниците во системот на здравствена заштита е основна алатка која обезбедува сигурен и безбеден и контролиран трансфер и обработка на податоците. Со ова се избегнува дуплирање на здравствените податоци на пациентите при примарната употреба на здравствените податоци за дијагноза, третман и рехабилитација, и се овозможува координирано и брзо донесување одлуки.

Естонскиот државен здравствен регистар е поддржан од KSI Blockchain. Оваа технологија исто така се користи од НАТО и од САД, од Одделот за одбрана. Податоците никогаш не го напуштаат системот и тие не се складираат во KSI блокчејнот, туку само се испраќа хаш „порака“ до блокчејнот.



## 4

## РЕГУЛАЦИЈА НА МЕДИЦИНСКИТЕ ПОДАТОЦИ ВО СЛОВЕНИЈА

Во правната литература се среќаваме со мислењето на теоретичарите дека Словенија одржува детална и ригорозна правна рамка за обработка на здравствени податоци, која ја приоритизира приватноста на пациентите, овозможува неопходен проток на податоци во рамките на здравствениот систем, но и често го ограничува пристапот што е неопходен за обезбедување квалитетна здравствена нега.

Анализата за оваа држава е базирана врз два темелни акти:

- Законот за заштита на лични податоци и
- Законот за бази на податоци од областа на здравството.

Темелните акти на оваа рамка се поддржани од специфични правила кои го уредуваат пристапот и обработката на податоците на пациентите<sup>31</sup>.

---

31 Tepej Jočić L. Impact of data protection regulation on Slovenian eHealth. J Glob Health 2021;11:03063. doi: 10.7189/jogh.11.03063.

## 4.1. ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ<sup>32</sup>

Одредбата од членот 1 од овој закон јасно го дефинира односот помеѓу националниот закон и Регулативата (ЕУ) 2016/679, позната како Општа регулатива за заштита на податоците (GDPR). Актуелниот национален закон е донесен во декември 2022 година, а стапи на сила во јануари 2023 година, и е во функција на спроведување и обезбедување усогласеност со оваа регулатива на Европската Унија. Меѓутоа, Законот доуредува и одредени аспекти кои не се регулирани во GDPR, како што е, на пример, обработката на лични податоци на починати лица, обработката на лични податоци во врска со извршување активности надвор од опсегот на правото на ЕУ, обработката на лични податоци од страна на властите на Словенија при дејствување во областите на безбедносната и одбранбената политика и носење надвор од разузнавачките и безбедносните активности.

Тоа значи дека овој закон не само што ги поставува основните правила и процедури за заштита на личните податоци, туку исто така ги надополнува и ги деталзира одредбите на GDPR во рамките на националниот правен систем. Со други зборови, националниот закон ги утврдува принципите, обврските и мерките кои се потребни за да се осигури дека обработката на личните податоци во државата е во согласност со барањата на GDPR, кој претставува наднационална регулатива. Тоа подразбира дека за сите прашања што се регулирани од GDPR, националниот закон мора да биде во согласност со него и да обезбеди дополнителни мерки каде што е потребно.

### 4.1.1. ПРЕГЛЕД НА ДЕФИНИЦИЈАТА ЗА МЕДИЦИНСКИ ПОДАТОЦИ

Законот не дава експлицитна дефиниција за „медицински податоци“; сепак, опфаќа специфични одредби во врска со обработката на лични податоци поврзани со здравјето.

Клучни одредби поврзани со медицински податоци се:

- **Биометриски податоци:** Законот ја забранува обработката на биометриски лични податоци, освен ако друг закон не предвиди поинаку, кој мора да ги утврди условите за нивна употреба.
- **Генетски податоци:** Генетските податоци можат да се обработуваат само ако е тоа дозволено со специфични законски одредби, особено за обезбедување здравствена заштита или врз основа на договорни обврски.
- **Обработка во здравствениот и јавниот сектор:** Законот предвидува дека обработката на лични податоци поврзани со здравствената заштита мора да ги следи строгите критериуми за обработка, осигурувајќи безбедност и усогласеност со регулаторните рамки.
- **Права на пациентите:** Постојат одредби за управување со медицинската

32 Словенечкиот текст е достапен на [Zakon o varstvu osebnih podatkov \(ZVOP-1\) \(PISRS\)](#) – вон сила и во сила на [Zakon o varstvu osebnih podatkov \(ZVOP-2\) https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2022-01-4187](#) . (Personal Data Protection Act



документација, при што се истакнува заштитата на професионалната тајна и правата на пациентите во специфични правни контексти.

- **Согласност за истражувања:** Физичките лица имаат право да го ограничат обработувањето на нивните податоци, вклучително и за истражувачки цели. Истражувачите мора да обезбедат писмена согласност за обработка на лични податоци, со цел да се обезбеди етичка усогласеност.
- **Правна основа за обработка:** Обработката на медицински податоци мора да биде во согласност со утврдените правни основи, кои вклучуваат добивање согласност или исполнување законски обврски.
- **Недискриминациска клаузула:** Законот забранува дискриминација врз основа на здравствена состојба, осигурувајќи дека обработката на податоците не резултира со нефер третман на индивидуите.
- **Обем на примената:** Одредбите се однесуваат на автоматизирано обработување податоци и на податоци наменети за системи за евиденција, осигурувајќи сеопфатна регулација на личните податоци.

## 4.1.2. АНАЛИЗА И РЕЗИМЕ НА ЧЛЕНОВИТЕ ОД ЗАКОНОТ ВО ВРСКА СО ПРИСТАПОТ ДО МЕДИЦИНСКИ ПОДАТОЦИ

Законот за заштита на личните податоци и неговите одредби поврзани со пристапот до медицински податоци покажуваат балансиран пристап преку внимателно регулирање на обработката, пристапот и заштитата на овие чувствителни податоци. Одредбите можат да се категоризираат во две главни групи: општи и посебни одредби, кои заедно создаваат сеопфатна рамка за заштита на личните и на медицинските податоци.

Општите одредби се фокусираат врз транспарентноста, законитоста и правичноста на обработката на лични податоци, додека посебните одредби се однесуваат на заштитата на чувствителни категории на податоци (биометрија, генетски податоци) и на специфични групи лица (малолетници, починати лица). Ова овозможува добро балансиран систем кој ги штити индивидуалните права, приватноста и сигурноста на медицинските податоци, истовремено обезбедувајќи соодветен пристап кога е потребно, под строго регулирани услови.

### 4.1.2.1. ОПШТИ ОДРЕДБИ

#### 4.1.2.1.1. ПРАВНИ ОСНОВИ ЗА ОБРАБОТКА НА ЛИЧНИ ПОДАТОЦИ

Личните податоци може да ги обработува или „контролор“ или „процесор“, по различни правни основи наведени во ZVOP-2 и GDPR (член 6 ZVOP-2 и во врска со член 6 и член 9 од GDPR).

Имајќи ги предвид дефинираните поими во законите, неминовно е да споменеме дека „**субјектот на податоците**“ е живо, физичко лице чии лични податоци ги

обработува или контролор или обработувач. **Контролорот** е одлучувачот, субјектот кој „сам или заедно со други ги определува целите и средствата за обработка на личните податоци“. **Обработувачот** „обработува лични податоци во име на контролорот“, постапувајќи по инструкции на контролорот. За разлика од претходниот закон, ZVOP-2, заедно со GDPR, наметнува директни обврски на контролорот и на процесорот, иако на процесорот му се наметнуваат помалку обврски.

Овој член го поставува основниот принцип дека обработката на лични податоци, вклучувајќи ги и медицинските податоци, може да биде законска само ако е заснована врз конкретни правни основи. Ова обезбедува транспарентност и правична обработка, така што поединците се информирани за целите, за видовите податоци и за времетраењето на чувањето. На овој начин се осигурува дека обработката на податоците е ограничена на неопходното, без прекумерно собирање или злоупотреба на лични податоци.

#### 4.1.2.1.2. ДНЕВНИК ЗА ОБРАБОТКА НА ПОДАТОЦИ (DATA PROCESSING LOG)

Дневникот за обработка на податоци е една од позначајните промени кои се донесени со ZVOP-2 и се однесува на безбедноста на заштитата на податоците и на проценката на влијанието. Со таа новина, од контролорите се бара да водат дневник за обработка на податоци (dnevnik obdelave) за одредени категории на обработка на податоци, вклучувајќи ги собирањето, промената и откривањето. Оваа обврска се применува: 1. кога се користат автоматизирани системи за податоци од големи размери а се однесуваат на посебни категории на лични податоци, 2. каде што има систематско и редовно следење на поединци, 3. кога анализата на влијанието врз заштитата на податоците (Data protection impact analyses – DPIA) покажала ризик што може да биде ефикасно управуван со водење дневник за обработка на податоците, или 4. кога поинаку се бара со закон (на пр., за видеонадзор), во врска со следниве дејствија кои произлегуваат од/за обработка на лични податоци: собирање; менување; увид; обелоденување, вклучително и трансфери; бришење; и други дејствија за обработка на податоците определени со закон.

**Дневникот за обработка содржи детали за дејствијата за обработка на податоците, а контролорот може да определи дополнителни содржини на дневникот за обработка, земајќи ја предвид проценката на влијанието. Дневникот за обработка се користи само за да се докаже законитоста на обработката и да се спроведе внатрешна контрола, да се вршат контроли или други законски проверки од надзорниот орган или од други надлежни органи, за да се обезбеди интегритетот и безбедноста на личните податоци и да се поправат грешките во работењето на информацискиот систем или обработката на податоците.** По правило, дневниците за обработка мора да се чуваат две години по истекот на календарската година кога е евидентирана соодветната обработка. Ова, во некои случаи, може да се продолжи до пет години.

#### 4.1.2.1.3. БЕЗБЕДНОСТ НА ЛИЧНИТЕ ПОДАТОЦИ ВО ОБЛАСТА НА ПОСЕБНА (СПЕЦИЈАЛНА) КАТЕГОРИЈА НА ПОДАТОЦИ ЗА ОБРАБОТКА (SECURITY OF PERSONAL DATA IN THE FIELD OF SPECIAL PROCEEDING)

Со ова се воведуваат дополнителни безбедносни барања за „специјална обработка“ (posebne obdelave). ЗВОП-2 воведува нова категорија на обработка на податоци, категоризирана како „специјална обработка“, која опфаќа специфична обработка на податоци од големи размери во рамките на информациските системи. Ова вклучува системи за обработка на лични податоци на повеќе од 100.000 поединци, врз основа на статутот, или обработка на посебни категории на лични податоци на повеќе од 10.000 поединци, како и случаи кога обработката се заснова врз специјалните закони (како што се законите за здравствена

заштита или задолжително здравствено осигурување). Покрај барањата за GDPR, специјалната обработка е предмет на зголемена безбедност и барања за известување за инциденти утврдени во законодавството, што ја регулира безбедноста на информациите. Во некои случаи, овие системи со такви податоци не смеат да се чуваат надвор од Словенија.

#### **4.1.2.1.4. КОРИСТЕЊЕ ЗНАЦИ (СИМБОЛИ) ЗА ПОВРЗУВАЊЕ (USING HYPHENS)**

Законот дава насоки за добивање лични податоци од базите на податоци, особено во чувствителни области како што е здравството. Овде се истакнува правната оправданост на обработката, односно дека пристапот до личните податоци мора да биде строго регулиран и поврзан со легитимна цел. Символи за поврзување може да се користат во специфични случаи за идентификување на сторител или за кривично гонење, особено кога е потребно за заштита на животот или телото на поединец. Оваа употреба мора веднаш да се документира за подоцна да се потврди неопходноста од употребата на симболот за поврзување.

#### **4.1.2.2. ПОСЕБНИ ОДРЕДБИ (ЗА СПЕЦИФИЧНИ КАТЕГОРИИ ЛИЦА И ПОДАТОЦИ)**

##### **4.1.2.2.1. СПЕЦИЈАЛНА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ НА ПОЧИНАТИ ЛИЦА**

Оваа одредба ја регулира обработката на лични податоци на починати лица, што е особено важно во контекст на медицински податоци. Само овластени корисници или оние кои имаат правен интерес можат да пристапат до овие податоци. Со ова, законот обезбедува контролиран пристап и заштита на приватноста на починатите лица, истовремено дозволувајќи ги неопходните правни постапки. Одредбите се применуваат врз личните податоци на починати лица 20 години по нивната смрт, освен ако друг закон не предвидува поинаку.

##### **4.1.2.2.2. ИСКЛУЧОК ОД БАРАЊЕТО НА ЛИЦЕТО ПРЕКУ ЗАКОНСКИ ПРЕТСТАВНИК**

Законот предвидува исклучок при пристапот до податоци кога е во прашање заштитата на ранливи категории, како малолетници или други заштитени лица. Контролорот може да одбие пристап до медицински податоци ако тоа влијае врз правата на овие лица. Ова е значаен принцип кој дава приоритет на интересите на ранливите групи над барањата на законските застапници.

##### **4.1.2.2.3. ОГРАНИЧУВАЊЕ ВО ОБРАБОТКАТА НА БИОМЕТРИСКИТЕ И ГЕНЕТСКИТЕ ПОДАТОЦИ**

Биометриските и генетските податоци се особено чувствителни, а нивната обработка е строго ограничена, освен ако не е предвидено поинаку со друг закон. Ова ја одразува важноста на специфичната правна основа за обработка на вакви типови податоци и осигурува висока заштита на поединците чија биометрија или генетика може да биде предмет на обработка.

#### 4.1.2.2.4. БИОМЕТРИЈА ВО ЈАВНИОТ СЕКТОР

Во јавниот сектор, обработката на биометриски податоци е дозволена само под точно дефинирани услови. Обработката на биометриски лични податоци во јавниот сектор е дозволена исклучиво и под услов дејствијата за обработка и користењето на овие податоци да се потврдат во согласност со овластувањата на надзорниот орган, на начин што обезбедува обработка и користење на овие податоци на поединецот под негова ексклузивна контрола или власт и му дозволува изречно да дозволи обработка на овие податоци од други обработувачи и менаџери со цел да се докаже точноста на неговиот идентитет. Ова го отсликува настојувањето на законот да ја лимитира и да ја контролира обработката на чувствителни податоци во јавните установи.

## 4.2. ЗАКОН ЗА БАЗИ НА ПОДАТОЦИ ОД ОБЛАСТА НА ЗДРАВСТВЕНАТА ЗАШТИТА

Предмет на анализа од правната регулатива на Словенија беше неофицијалната пречистена верзија на Законот за бази на податоци од областа на здравствената заштита, која ги опфаќа:

- » Законот за бази на податоци од областа на здравствената заштита (Службен весник на Република Словенија, бр. 65/00 од 21 јули 2000 година)<sup>33</sup>,
- » Законот за изменување и дополнување на Законот за бази на податоци од областа на здравствената заштита (Службен весник на Република Словенија бр. 47/15 од 30 јуни 2015 година)<sup>34</sup> и
- » Законот за изменување и дополнување на Законот за бази на податоци од областа на здравствената заштита – ZZPPZ-B (Службен весник на Република Словенија бр. 31/18 од 4 мај 2018 година)<sup>35</sup>.

### 4.2.1. КРАТОК ПРЕГЛЕД НА ЗАКОНОТ

Законот за бази на податоци од областа на здравството (ZZPPZ) има за цел да ги регулира обработката и чувањето на медицинските и личните податоци на пациентите. Овој закон е дизајниран да обезбеди заштита на приватноста на пациентите и да постави јасни правила за пристап до овие податоци. Регулацијата за пристап до медицински податоци во Словенија е утврдена со овој закон. Тој ги задолжува сите здравствени установи да испраќаат податоци за пациентите во Централниот регистар на податоци за пациенти (CRPP).

Оваа регулација овозможува централизирано собирање на здравствени информации, што ја подобрува транспарентноста и ангажираноста на пациентите преку порталот zVEM (подетално објаснет *infra* во текстот). Иако се олеснува пристапот до медицински податоци

---

33 Zakon o zbirkah podatkov s področja zdravstvenega varstva – ZZPPZ (Uradni list RS, št. 65/00 z dne 21. 7. 2000),

34 Zakon o spremembah in dopolnitvah Zakona o zbirkah podatkov s področja zdravstvenega varstva – ZZPPZ-A (Uradni list RS, št. 47/15 z dne 30. 6. 2015)

35 Zakon o spremembah in dopolnitvah Zakona o zbirkah podatkov s področja zdravstvenega varstva – ZZPPZ-B (Uradni list RS, št. 31/18 z dne 4. 5. 2018).

за здравствените работници, истовремено се наметнуваат ограничувања за заштита на приватноста на пациентите. **Ограничувањата вклучуваат услови за пристап до податоците, обврска за доверливост, обука за дигитална писменост и мониторинг на пристапот, со цел да се осигури етичко и одговорно управување со чувствителните информации.** Оваа рамка има за цел да ја балансира потребата за достапност на податоците во здравствената грижа со заштитата на приватноста на индивидуите<sup>36</sup>.

## 4.2.2. ЗАШТИТА НА МЕДИЦИНСКИТЕ И НА ЛИЧНИТЕ ПОДАТОЦИ

### 4.2.2.1. ВРЕМЕ НА ЧУВАЊЕ НА ПОДАТОЦИТЕ

Член 14.b предвидува дека податоците за пациентите се чуваат до нивната смрт. По смртта, одредени податоци се чуваат уште една година. Ова создава основа за заштита на податоците дури и по смртта на пациентот, спречувајќи неконтролирано обработување на чувствителни информации.

### 4.2.2.2 БЛОКИРАЊЕ НА ПОДАТОЦИТЕ

По истекот на времето на чување, податоците се блокираат, што спречува нивно понатамошно обработување. Ова е важен механизам за заштита на приватноста на пациентите, осигурувајќи дека нивните податоци не се користат без согласност по завршувањето на законскиот рок.

## 4.2.3. ПРИСТАП ДО МЕДИЦИНСКИТЕ ПОДАТОЦИ

### 4.2.3.1. КОЈ ИМА ПРИСТАП ДО ПОДАТОЦИТЕ?

Член 14.c поставува правила за тоа кои субјекти можат да имаат пристап до медицинските податоци. **Пристапот е строго ограничен на овластени лица во рамките на здравствените институции и органи, а неовластен пристап е забранет.**

### 4.2.3.2. УСЛОВИ ЗА ПРИСТАП

Член 14.c, став 1 предвидува дека обработката на податоците може да се изврши само во согласност со законите и со пропишаните процедури. Ова значи дека само овластени медицински работници и организации можат да имаат пристап до податоците, под услов тие да го почитуваат законот и правилата за приватност. Законските одредби водат до заклучокот дека условите за пристап до медицински податоци се засноваат врз принципот на овластени корисници и принципот на пристап базиран на улоги:

**Овластени корисници: Само одредени здравствени професионалци, како**

36 Rant, Ž., Janet, J., & Stanimirović, D. (). Functionalities and use of the zVEM Patient Portal and the Central Registry of Patient Data. 35th Bled eConference Digital Restructuring and Human (Re)Action, 65–79. <https://doi.org/10./UM.FOV.4.2022.4>.

лекари и медицински сестри, можат да пристапат до здравствените податоци на пациентите. Овие лица обично треба да поседуваат соодветни квалификации и обука за ракување (работење) со податоците.

**Пристап базиран на улоги:** Пристапот до информациите често е специфичен за улогата, што значи дека здравствените работници можат да пристапат само до податоци кои се потребни за нивните задачи. Ова го минимизира неовластениот пристап и ја штити доверливоста на пациентите<sup>37</sup>.

Следствено, следните субјекти имаат пристап до здравствените податоци:

- 1. Здравствени установи:** Сите здравствени установи се обврзани да ги доставуваат податоците до Централниот регистар на здравствени податоци (CRPP) како дел од системот за е-здравство.
- 2. Даватели на концесии:** Субјектите кои работат под концесија во здравството се должни да ги споделуваат релевантните податоци.
- 3. Приватни оператори:** Дури и оние без концесии мораат да доставуваат податоци до CRPP.
- 4. Пациенти:** Самите пациенти имаат пристап до своите лични здравствени податоци преку Порталот за пациенти zVEM.
- 5. Јавни здравствени власти:** Овие власти имаат пристап до податоците за јавно здравје и за следење на здравствените состојби.
- 6. Истражувачи:** Според специфични регулативи, истражувачите можат да пристапат до анонимизирани податоци за спроведување на студии.
- 7. Осигурителни компании:** Тие може да пристапат до одредени податоци за обработка на побарувања и за спроведување здравствени проценки.
- 8. Итни служби:** Првите реагирачи (првата интервенција) може да пристапат до потребните здравствени информации за време на итни случаи.

Пристап до здравствените податоци е дозволен во следниве околности:

- 1. Давање медицинска нега:** Пристапот е неопходен за здравствените работници за да овозможат соодветна медицинска услуга.
- 2. Јавно-здравствени иницијативи:** Податоците се споделуваат за да се олеснат мерките за јавно здравје, особено за време на здравствени кризи како пандемиите.
- 3. Согласност на пациентот:** Пациентите можат да дадат согласност за специфична употреба на нивните податоци, како, на пример, за истражувања или споделување со осигурителни компании.
- 4. Законски барања:** Ускладувањето со законите може да бара споделување на податоци со властите за истраги или за правни постапки.

---

37 Rant, Živa, Dalibor Stanimirović, and Jure Janet. 2021. „Portal za paciente zVEM in centralni register podatkov o pacientu.“ In Dnevi slovenske informatike 2021, 1-5. National Institute of Public Health Slovenia.

5. **Итни ситуации:** Брз пристап до здравствените податоци е клучен за итните служби да обезбедат навремена нега.
6. **Административни цели:** Пристапот е потребен за управување со здравствените побарувања и за регистрирање пациенти.
7. **Обработка на податоци за здравствени апликации:** Апликации како електронско препишување лекови и системи за закажување прегледи бараат пристап до податоците на пациентите.
8. **Статутарно известување:** Здравствените установи мораат да ги известуваат националните здравствени власти за ускладување и за следење<sup>38</sup>.

#### 4.2.3.3. ОБЕМ И ВРЕМЕНСКИ ПЕРИОД

Пристапот до податоците е ограничен на минималниот обем потребен за исполнување на медицинските обврски. **Ова значи дека само оние информации кои се релевантни за конкретниот случај можат да се обработуваат.** Временскиот период за чување на податоците е до смртта на пациентот или, во некои случаи, 30 години по последната промена на медицинските податоци.

#### 4.2.4. ПРАВО НА ПАЦИЕНТОТ ДА ГО ОГРАНИЧИ ПРИСТАПОТ

Член 18, Пациентот има право да биде информиран за обработката на своите податоци и може да побара ограничување на пристапот во одредени ситуации. Ова право е клучно за одржување на приватноста и довербата во здравствениот систем.

### 4.3. ПРАВИЛНИК ЗА ЗАБРАНА ЗА ПРЕГЛЕД НА ИЗВОДОТ ОД ПОДАТОЦИТЕ ЗА ПАЦИЕНТОТ ВО ЦЕНТРАЛНИОТ РЕГИСТАР НА ПОДАТОЦИ ЗА ПАЦИЕНТИ

Овој правилник<sup>39</sup> ги уредува деталите за давање и повлекување на забраната за преглед на податоците на пациентот во Централниот регистар на податоци за пациенти (CRPP), со фокус врз правата на пациентите и процедурите за заштита на нивната приватност. Тој е донесен врз основа на третата алинеја од четвртиот став од член 14.d од Законот за бази на податоци од областа на здравствената

---

38 Rant, Ž., Janet, J., & Stanimirović, D. (). Functionalities and use of the zVEM Patient Portal and the Central Registry of Patient Data. 35th Bled eConference Digital Restructuring and Human (Re)Action, 65–79. <https://doi.org/10./UM.FOV.4.2022.4>

39 Pravilnik o prepovedi vpogleda v povzetek podatkov o pacientu v Centralnem registru podatkov o pacientih, Uradni list RS, št. [84/15](#) (Rules prohibiting access to the summary of patient data in the Central Register of Patient Data, Official Gazette of the Republic of Slovenia, No. [84/15](#)), Достапен на [Pravilnik o prepovedi vpogleda v povzetek podatkov o pacientu v Centralnem registru podatkov o pacientih \(PISRS\)](#), пристапено на 10.10.2024 година.

заштита (Службен весник на РС, бр. 65/00 и 47/15). Тоа значи дека правилникот се заснова врз специфична одредба од законот која овластува детална регулација на забраната за пристап до податоците на пациентите.

Овој правилник претставува добро структуриран и балансиран документ кој обезбедува високо ниво на заштита на личните податоци на пациентите. Тој ги дефинира принципите за управување со здравствените бази на податоци и поставува темели за правилата кои регулираат пристап и обработка на податоците. Одредбите овозможуваат флексибилност и контрола од страна на пациентите, притоа осигурувајќи дека нивните права се почитуваат. Воедно, процедуралните аспекти на правилникот гарантираат брза реакција и ефикасност при ажурирањето на податоците, што е од клучна важност за заштита на приватноста.

Тој оди понатаму од законот, овозможувајќи детална процедура за пациентите да ја остварат својата контрола врз личните медицински податоци, како и да ги знаат методите за поднесување и повлекување на забраната.

Правилникот детално ја уредува процедурата за давање забрана за пристап до податоците во Централниот регистар за податоци на пациентите (CRPP). Анализата на одредбите покажува дека овој документ се заснова врз принципите на „правото на приватност“ и „автономија на пациентите“, кои се клучни во модерното здравствено право.

### **4.3.1. ПРЕДМЕТ НА ПРАВИЛНИКОТ**

Член 1 го утврдува главниот предмет на регулирање – процедурите и условите под кои пациентите можат да забранат преглед на нивните податоци. „Правото на ограничување на пристапот до здравствени податоци“ е јасно дефинирано и претставува важен механизам за заштита на приватноста на пациентите. Овој член го воспоставува основниот рамковен контекст за целиот правилник, што овозможува јасно и транспарентно управување со чувствителните податоци.

### **4.3.2. ПРАВО НА ДАВАЊЕ ЗАБРАНА**

Правото на пациентите да дадат забрана за пристап до изводот од податоците за пациентот во Централниот регистар на податоци за пациенти во секое време укажува на високото ниво на заштита на „информатичката самоопределба“ (правото самостојно да одлучуваат за своите податоци). Одредбата од член 2 е усогласена со принципите на заштита на лични податоци, вклучувајќи ја и Европската регулатива (GDPR). Дополнително, дозволата на овластен претставник или на законски застапник да дејствува во име на пациентите кои не можат да одлучуваат за себе обезбедува дека приватноста на пациентите е заштитена и во случаи на неспособност. Со ова, правилникот го заштитува правото на достоинство и приватност, особено кај ранливи групи како што се малолетници и неспособни лица.

### **4.3.3. ОБЕМ НА ЗАБРАНАТА И ПОТРЕБНИ ПОДАТОЦИ**

Членот 3 дава флексибилност на пациентите да изберат кон кого ќе биде насочена забраната (кон конкретен давател на здравствени услуги или на пошироко државно ниво). Оваа одредба е важна, бидејќи им овозможува на пациентите да го контролираат степенот на пристап до нивните податоци, што е во согласност со принципите на пропорционалност



и за непотребна обработка на лични податоци. Побарувањето за точни податоци, како што се името и матичниот број, гарантира административна точност и правна заштита при поднесувањето на забраната.

#### **4.3.4. ПОДНЕСУВАЊЕ И ВРЕМЕТРАЕЊЕ НА ЗАБРАНАТА**

Член 4 е значаен заради обезбедувањето брзина и достапност во поднесувањето на забраната преку дигиталната платформа zVEM или преку личен лекар. Двоканалниот пристап ги поедноставува процедурите за пациентите, што е особено важно за ефикасна заштита на податоците. Обврската забраната да биде доставена до крајот на работниот ден гарантира дека податоците ќе бидат брзо ажурирани, што претставува клучен аспект за заштита на информациската безбедност.

#### **4.3.5. ПОВЛЕКУВАЊЕ НА ЗАБРАНАТА**

Можноста за повлекување на забраната е во согласност со правото на ревизија и на контролирана промена на одлуките за личните податоци. Процедурите за повлекување се идентични како и за поднесувањето на забраната, што обезбедува конзистентност и следливост во процесот. Со ова се гарантира дека промените во одлуките на пациентите ќе бидат брзо и лесно процесирани.

#### **4.3.6. ОБРАСЦИ ЗА ЗАБРАНА И ПОВЛЕКУВАЊЕ**

Стандардираните обрасци гарантираат единственост во процесирањето на забраните и повлекувањата. Ова ја олеснува работата на здравствените институции и обезбедува правна сигурност за сите засегнати страни. Употребата на стандардирани документи го прави процесот транспарентен и лесно разбирлив за корисниците.

### **4.4. ПОРТАЛ ЗА ЗДРАВСТВЕНИ УСЛУГИ zVEM И ЦЕНТРАЛЕН РЕГИСТАР ЗА ПОДАТОЦИ НА ПАЦИЕНТИТЕ (CRPP) ВО СЛОВЕНИЈА**

Системот zVEM (Централен пациентски портал) е воспоставен како дел од проект за еЗдравство (2008 – 2015), а неговата целосна функционалност станува достапна од почетокот на 2017 година. Системот zVEM, заедно со CRPP, претставува значаен напредок во е-здравството во Словенија, овозможувајќи им на пациентите сигурен пристап до нивните медицински податоци, додека истовремено воспоставува јасни протоколи и ограничувања за здравствените работници. Овој систем има за цел да го подобри квалитетот на здравствената заштита, истовремено зачувувајќи ја приватноста и безбедноста на податоците на пациентите. Значајните напредоци во дигиталното здравство настанале

особено за време на пандемијата со COVID-19<sup>40</sup>.

Пациентите добија значително подобрен пристап до нивните медицински податоци преку системот **zVEM**, кој овозможува безбеден и ефикасен пристап до различни медицински документи и услуги. Овој систем им овозможува на пациентите да:

- Пристапуваат до упати,
- Гледаат рецепти,
- Читаат извештаи од специјалисти,
- Закажуваат прегледи онлајн,
- Проверуваат периоди на чекање за услуги,
- Преземаат статус на вакцинација и резултати од тестирање за COVID,
- Преземаат Европски дигитален COVID сертификат,
- Дадат согласност за споделување на податоци и да резервираат термини за вакцинација<sup>41</sup>.

#### 4.4.1. КЛУЧНИ КАРАКТЕРИСТИКИ НА ПОРТАЛОТ zVEM<sup>42</sup>

Овој портал овозможува:

**Пристап за пациенти:** Пациентите можат да ги прегледуваат своите здравствени документи, вклучувајќи ги отпусните писма од болниците и резултатите од тестовите за COVID-19.

**Пристап за здравствени работници:** Здравствените работници можат да пристапуваат до податоците на пациентите, овозможувајќи подобро здравствено згрижување без потреба пациентите да пренесуваат документи меѓу различни здравствени установи.

**Резиме на пациентот (PPoP):** Структуриран запис на основните здравствени податоци е достапен за пациентите и нивните старатели, што обезбедува здравствените работници да имаат потребни информации за квалитетно лекување.

**Податоци за рецепти:** Пациентите можат да ја прегледуваат својата историја на издадени рецепти, вклучувајќи детали за препишаните лекови и надополнувања.

**Онлајн термини и листи на чекање:** Порталот нуди информации за времето на чекање и за достапните термини кај здравствените установи.

---

40 Živa Rant, Dalibor Stanimirović, Jure Janet „The Development of zVEM Portal and the Central Register of Patients Data“, DOI link <https://doi.org/um.fov.3.2022.63>

41 Rant, Ž., Janet, J., & Stanimirović, D. (). Functionalities and use of the zVEM Patient Portal and the Central Registry of Patient Data. 35th Bled eConference Digital Restructuring and Human (Re)Action, 65–79. <https://doi.org/10./UM.FOV.4.2022.4>

42 Ibid

#### 4.4.2. ЛИЦА СО ПРИСТАП

Пристапот до медицинските податоци е структурирано организиран на следниов начин:

1. **Пациенти:** Имаат директен пристап до своите здравствени записи и можат да управуваат со различни податоци за своето здравје.
2. **Здравствени работници:** Лекарите и овластените здравствени лица можат да пристапуваат до податоците на пациентите за да обезбедат давање здравствена услуга.

#### 4.4.3. ОГРАНИЧУВАЊА И ОДГОВОРНОСТИ

Пациентите мора да дадат согласност за пристап и за споделување на нивните податоци меѓу здравствените работници. Пациентите можат да постават ограничувања на тоа кој може да ги прегледува нивните податоци, со што се обезбедува приватност и контрола врз личните информации.

Постојат строги мерки за заштита на податоците на пациентите од неовластен пристап (нарушување на безбедноста на податоците), што осигурува усогласеност со прописите за приватност на здравствените информации.

Обработката на личните здравствени податоци е регулирана со конкретни закони кои пропишуваат како се собираат, како се чуваат и како се пристапува до податоците.

#### 4.4.4. ЦЕНТРАЛЕН РЕГИСТАР НА ПОДАТОЦИ НА ПАЦИЕНТИ (CRPP)<sup>43</sup>

Централниот регистар на податоци на пациенти (CRPP) е клучна платформа во словенечкиот систем за е-здравство. Овој регистар овозможува споделување електронски здравствени записи на национално ниво и содржи голем број неструктурирани медицински документи и резимеа за здравјето на пациентите. До денес, CRPP има повеќе од 50 милиони записи, кои опфаќаат повеќе од 90 % од словенечкото население. Негова цел е да го подобри процесирањето на податоците во здравствениот систем, додека обезбедува усогласеност со строгите регулативи за заштита на податоци.

CRPP е функционален од 2015 година. Неговото основање имаше за цел да создаде сеопфатен и пристапен систем на електронски здравствени записи за Словенија, со што ќе се обезбеди ефикасна испорака на здравствени услуги низ целата земја.

CRPP работи под регулаторната рамка поставена со Законот за заштита на лични податоци, кој стапи на сила во 2004 година. Овој закон е усогласен со Општата регулатива за заштита на податоци (GDPR), но наметнува уште построги регулативи за ракување со податоците во јавниот здравствен систем. Правното управување

43 Податоци според Tepej Jočić L. Impact of data protection regulation on Slovenian eHealth. J Glob Health 2021;11:03063. doi: 10.7189/jogh.11.03063.

со CRPP е доделено на Националниот институт за јавно здравје, кој го спроведува Законот за бази на податоци од областа на здравството. Овој закон ги дефинира спецификациите за содржината, целта и обемот на обработката на здравствените податоци.

Клучни акти кои го уредуваат CRPP:

1. Закон за заштита на лични податоци (2004);
2. Закон за бази на податоци од областа на здравството;
3. Правилник за овластувања за обработка на податоци.

Оваа структурирана регулатива обезбедува дека личните здравствени податоци се управувани сигурно и одговорно, додека се задржува пристапот за овластените здравствени работници.

## 4.5. ПРАВИЛНИК ЗА ОВЛАСТУВАЊА ЗА ОБРАБОТКА НА ПОДАТОЦИ

Предмет на нашата анализа беше неофицијален консолидиран текст на Правилникот за овластувања за обработка на податоци во Централниот регистар на податоци на пациенти, кој ги вклучува следните акти:

- Правилник за овластувања за обработка на податоци во Централниот регистар на податоци на пациенти (Службен весник на Република Словенија, бр. 51/16 од 22/07/2016 година) и Правилник за изменување и дополнување на Правилникот за овластувања за обработка на податоци во Централниот регистар на податоци на пациенти (Службен весник на Република Словенија, бр. 95/21 од 15 јуни 2021 година). Овие акти беа во примена во Словенија до 31 август 2024 година<sup>44</sup>.
- Предмет на анализа беше и новиот Правилник за овластувања за обработка на податоци во Централниот регистар на податоци за пациенти (CRPP) во Словенија, кој почна да се применува од 1 септември 2024 година (Службен весник на Република Словенија, бр. 35/24 од 19 април 2024 година).

Овие подзаконски акти ја уредуваат процедурата и овластувањата за обработка на податоци во рамките на Централниот регистар на податоци на пациенти (CRPP), вклучувајќи ги измените и дополнувањата што овозможуваат ажурирање и усогласување со поновите регулативи. Претходниот Правилник, како и Правилникот кој денес е во сила, содржи и Прилог за пристап до медицински податоци. Прилогот ги утврдува правилата за пристап до медицинската документација во Централниот регистар на податоци за пациенти (CRPP) во Словенија, во зависност од видот на здравствената дејност и условите кои треба да бидат исполнети за обработка на документацијата<sup>45</sup>.

---

44 Текстот е достапен на [Rules on authorisations to process data in the Central Register of Patient Data \(PISRS\)](#), пристапено на 19.10.2024 година.

45 Текстот на прилогот е достапен на [RS\\_-2024-035-01084-OB~P001-0000.PDF](#), пристапено на 09.12.2024 година.

#### 4.5.1. ПРЕГЛЕД НА ПРАВИЛНИКОТ ЗА ОВЛАСТУВАЊА ЗА ОБРАБОТКА НА ПОДАТОЦИ ОД 2016 ГОДИНА СО ИЗМЕНИТЕ ОД 2021 ГОДИНА<sup>46</sup>

Правилникот за овластувања за обработка на податоци во Централниот регистар на податоци на пациенти (CRPP) воспоставува строги протоколи за здравствените работници во однос на пристапот до информациите на пациентите. Овие правила се клучни за осигурување дека само овластени лица можат да пристапат до чувствителни податоци на пациенти, што ја штити нивната приватност и безбедноста на податоците.

#### 4.5.2. КЛУЧНИ ПОЕНТИ НА ПРАВИЛНИКОТ

1. Услови за пристап: Здравствените работници мора да имаат валидни упати, согласност од пациентот или да бидат дел од итна служба за да добијат целосен пристап до податоците на пациентот.
2. Назначување на лекар: Пристапот се одобрува само ако идентификацискиот број на лекарот што бара пристап се совпаѓа со претходно регистрираниот ИД број на избраниот лекар во Регистарот на пациенти.
3. Процес на верификација: Системот го проверува идентификацискиот број на здравствениот работник со индексот на пациенти, тековните упати и која било регистрирана согласност од пациентот пред да одобри пристап.
4. Итен пристап: Во итни ситуации, лекарите можат привремено да ги заобиколат ограничувањата за пристап до 8 часа, со соодветна документација.
5. Дигитални сертификати: Корисниците мора да се регистрираат во базата на податоци на корисници на е-здравство користејќи лични дигитални сертификати, кои овозможуваат безбеден пристап до податоците на пациентот.
6. Процес на ревизија: Секое барање за пристап поминува низ повеќе фактори на ревизија за да се осигури усогласеност со правилата за овластувања.
7. Евалуација на метаподатоци: Системот ги евалуира метаподатоците на достапните документи за да утврди дали е дозволен пристап врз основа на работното место на лекарот.
8. Улога на контролор на податоци: Националниот институт за јавно здравје ја извршува улогата на контролор на податоците, надгледувајќи го пристапот на крајните корисници, независно од информациските системи на здравствените установи.
9. Модел на имплементација: CRPP е модел-пример за вградување на заштитата на податоците, со минимални промени во постоечките информатички системи на болниците.

46 Според Tepej Jočić L. Impact of data protection regulation on Slovenian eHealth. J Glob Health 2021;11:03063. doi: 10.7189/jogh.11.03063.

10. Повратни информации од засегнатите страни: Од почетокот на имплементацијата, најголемиот дел од повратните информации од засегнатите страни се однесуваат на комплексноста на овластувањата за пристап за здравствените работници.

Правила за пристап до медицински податоци се сложени и тешки за разбирање за здравствените работници, што создава проблеми со достапноста и дополнително административно оптоварување. За да се подобри ефикасноста, се препорачуваше пофлексибилна правна рамка, воспоставување сеопфатни ревизорски механизми, меѓусебен дијалог и континуирани обуки на овластените лица кои ќе осигурат одговорност и заштита на приватноста<sup>47</sup>. Со новиот правилник од 2024 година се прави голем исчекор во надминување на овие предизвици.

#### **4.5.2.1. ИЗМЕНИТЕ ОД СЕПТЕМВРИ 2024 ГОДИНА**

Со измените од овој правилник, во здравствената евиденција се воведува:

Подобрување на транспарентноста: Новиот правилник воведо појасни критериуми за овластувања и дефинираше подобро структурирани категории на податоци.

Поширока интероперабилност: Обезбеден е пофлексибилен пристап до податоците преку националните и регионалните платформи за е-здравство, вклучително и системот zVEM.

Проширување на овластувањата: Овластувањата се проширени за различни видови здравствени дејности, како што се патронажна грижа, клиничка генетика и итна медицинска помош.

Построги механизми за контрола: Усовершени се ревизорските механизми за следење на пристапот, а дозволите за обработка на податоци се условени од конкретни околности, како изјави на пациенти или итни здравствени потреби.

Целосно дигитализирање: Сите упати и пристапи сега се евидентираат во дигитални системи, овозможувајќи следливост и минимизирање грешки.

Посебно истакнуваме три клучни придобивки од новиот правилник:

1. Автономија на пациентот: Пациентите имаат поголема контрола врз своите податоци преку можноста за изјави за дозвола или забрана за пристап.
2. Ефикасност и достапност: Обработката на податоците сега е олеснета, со посебен акцент врз итните случаи и дигитализацијата.
3. Јасност на улогите: Дефинирани се прецизни улоги и одговорности на здравствените работници и институции.

#### **4.5.3. ПРИЛОГ ЗА ПРИСТАП ДО МЕДИЦИНСКА ЕВИДЕНЦИЈА**

Прилогот го систематизира пристапот до медицинските податоци во Централниот регистар на податоци за пациенти (CRPP), со јасно дефинирани правила кои ги балансираат потребите на здравствените работници за пристап со правото на приватност

---

47 Ибид.

на пациентите. Оваа систематизација вклучува разграничување помеѓу различни здравствени дејности, овластувања и нивоа на пристап, врз основа на природата на медицинската документација и улогата на здравствените работници.

Прилогот од Правилникот систематизира **три вида пристап** до медицинската документација во Централниот регистар на податоци за пациенти (CRPP), врз основа на природата на документацијата и условите за нејзина обработка:

### 1. Пристап без ограничувања:

- Овој пристап е дозволен без изречна согласност од пациентот. Се однесува на случаи каде што обработката на податоците е од суштинско значење за обезбедување здравствена нега, како што се итна медицинска помош или активности на диспечерските служби.
- *Пример:* При итна медицинска состојба, медицинските лица можат директно да пристапат до документацијата за да го спасат животот на пациентот.

### 2. Пристап со изречна согласност:

- Овој вид пристап се дозволува само доколку пациентот даде изречна писмена согласност.
- *Пример:* Во стоматологијата, лекарот може да пристапи до медицинската документација само доколку пациентот даде дозвола, што ги рефлектира строгиот акцент на приватност и ограничената итност во оваа гранка.

### 3. Пристап врз основа на претходна изјава на пациентот:

- Во некои здравствени области, пристапот е можен доколку пациентот веќе има поднесено изјава за дозвола за обработка на документацијата поврзана со неговата здравствена состојба.
- *Пример:* Ова се однесува на документацијата од области како патронажната нега или трудовата медицина, каде што континуитетот на грижата често бара претходно дадена согласност.

Видот на пристап до медицинската евиденција ќе зависи од два фактори:

- » **Од видот на специјализација на здравствените работници** (прилогот прави разлика меѓу семејна медицина, стоматологија, гинекологија и акушерство, итна медицинска помош, ментално здравје и неврологија, клиничка генетика и онкологија, медицина на трудот, друга здравствена заштита, судска медицина и вештак. Според видот на специјализација, секој здравствен работник има различен степен на пристап до медицинските податоци) и
- » **Од видот на медицинската евиденција, односно од активноста при која е создадена медицинската евиденција** (евиденцијата може да настанала во рамки на семејната медицина и педијатријата, при постапување на итната медицинска помош, во рамки на стоматологијата, во рамки на гинекологијата и акушерството, при грижа за ментално здравје, во рамки на клиничката генетика, при лабораториски активности и дијагностика во рамки на медицината на трудот и при други здравствени активности).

## 4.6. КРАТКО РЕЗИМЕ

Словенија ја поставува регулацијата на медицинските податоци на високо ниво, претставувајќи модел за балансирање на приватноста со функционалноста на здравствениот систем. Основните принципи врз кои се заснова пристапот се транспарентност, минимална обработка на податоци, согласност на пациентите и овластен пристап. Овие принципи се уредени преку Законот за заштита на личните податоци и подзаконските акти, како Правилникот за овластувања за обработка на податоци. Овие норми не само што ја обезбедуваат приватноста на пациентите, туку и гарантираат функционалност и ефикасност во работењето на здравствениот систем.

Пристапот до медицинските податоци е организиран преку детална правна и институционална рамка која ги балансира приватноста на пациентите и функционалните потреби на здравствениот систем. Оваа рамка го почитува европското законодавство, како GDPR, но истовремено вклучува специфични национални решенија за да обезбеди усогласеност и заштита на личните податоци во контекст на здравството. Оваа структура служи како пример за интегрирано управување со здравствени податоци преку ефикасно комбинирање на националните закони и европските регулативи.

Словенија има два основни закони кои ја регулираат обработката на медицински податоци: Законот за заштита на лични податоци (ZVOP-2) и Законот за бази на податоци од областа на здравството (ZZPPZ). Главни карактеристики на Законот за заштита на лични податоци се чување на податоците до смртта на пациентот и една година по смртта, воведување дневник за обработка на податоците за евиденција и надзор, строга регулација за обработка на биометриски и генетски податоци. Законот за бази на податоци од областа на здравството поставува строги критериуми за тоа кои лица и институции можат да имаат пристап. Само овластени здравствени работници и организации можат да ги користат податоците, и тоа исклучиво во согласност со улогата и целта на обработката. Приватноста на пациентите е заштитена преку принципот на овластен пристап, кој го лимитира пристапот според професионалната потреба и функцијата на корисникот. Овој закон ги обврзува здравствените установи да испраќаат податоци до Централниот регистар на податоци за пациенти (CRPP).

Дополнително, се применуваат подзаконски акти како Правилникот за овластувања за обработка на податоци, кој ги деталзира процедурите за пристап до CRPP; Правилникот за забрана за преглед на изводот од податоците за пациентот во Централниот регистар на податоци за пациенти, кој регулира детални процедури за давање и за повлекување на забраната за пристап до податоците во Централниот регистар за податоци на пациенти (CRPP); Правилникот за овластувања за обработка на податоци, кој ги регулира и условите под кои здравствените работници можат да пристапат до податоците, како и процесот на верификација на овие услови, што обезбедува соодветна и контролирана обработка на чувствителни податоци.

Заедно, овие правилници создаваат систем во кој правата на пациентите се заштитени, но истовремено овозможуваат ефикасен пристап за здравствените работници кога е тоа неопходно за обезбедување соодветна медицинска нега. Тие ја обезбедуваат флексибилноста и пропорционалноста на обработката на податоците, што е клучно за постигнување баланс помеѓу заштитата на приватноста и потребата од пристап до медицински податоци.

Во однос на институционалната рамка, во Словенија постојат три основни столбови на оваа рамка: Централниот регистар за податоци на пациенти (CRPP) – централна



платформа за електронски здравствени податоци, овозможувајќи споделување и заштита на чувствителните информации, управуван од Националниот институт за јавно здравје; Порталот zVEM – електронски систем за пациенти и здравствени работници, кој нуди: пристап до медицински документи, рецепти и прегледи, управување со дозволи за пристап до податоци, сигурен и транспарентен процес за пациентите, преглед на здравствени записи на пациентите, можност да закажуваат прегледи и да ги следат своите медицински информации, и Националниот институт за јавно здравје, кој ги надгледува и ги контролира активностите поврзани со заштита и обработка на здравствените податоци.



## 5

## РЕГУЛАЦИЈА НА МЕДИЦИНСКИТЕ ПОДАТОЦИ ВО ПОРТУГАЛИЈА

Португалската Национална платформа за медицински податоци е лансирана во 2012 година. На ова претходеле многубројни активности и конкретни владини заложби, меѓу кои и осигурувањето дека секој граѓанин има електронски здравствен картон (EHR) до крајот на 2012 година. Со донесувањето на Основниот закон за здравство од 2019 година, следи цел процес на реформи во португалското здравство кој сè уште е во тек. Ова се случува особено со усвојувањето на владиното упатство<sup>48</sup> од 2023 година, со кое се бара јасно утврдување на механизмите за меѓусебна соработка на Централната управа на здравствениот систем, Извршната дирекција на Националната здравствена служба и Заедничките услуги на Министерството за здравство и други релевантни институции.

### 5.1. ПРАВНА РАМКА

Имајќи го предвид законскиот систем на Португалија, истражувањето и направената анализа се базира врз три закони:

1. Општа регулатива за заштита на податоци (GDPR). Закон за заштита на личните податоци, обработката и преносот на лични податоци од 2019 година<sup>49</sup>.

48 <https://diariodarepublica.pt/dr/en/detail/order/7985-2023-216643611>

49 Донесен на 8 август 2019 година, Закон бр. 58/2019.

2. Основен Закон за здравство од 2019 година<sup>50</sup>.

3. Закон за лични генетски информации и здравствени информации од 2005 година<sup>51</sup>.

## 5.2. ЗАКОН ЗА ЗАШТИТА НА ЛИЧНИТЕ ПОДАТОЦИ ВО СОГЛАСНОСТ СО РЕГУЛАТИВАТА (ЕУ) 2016/679 НА ПАРЛАМЕНТОТ И НА СОВЕТОТ ОД 2016 ГОДИНА (GDPR)

Законот за заштита на личните податоци содржи одредби кои се однесуваат на заштита на физички лица во однос на обработката на лични податоци и слободна циркулација на тие податоци и е во согласност со Општата регулатива на ЕУ за заштита на личните податоци. Законот е донесен во август 2019 година.

Во согласност со европската Општа регулатива за заштита на податоци (GDPR), португалското законодавство воведува клучни механизми за заштита на личните податоци, со акцент врз транспарентноста, техничката и организациска безбедност, како и отчетност на контролорите.

- **Транспарентност:** Обврската за известување на субјектот за секој пристап до неговите медицински податоци. Оваа обврска, при нејзиното практично реализирање, бара контролорот на податоци да воведо механизам за автоматско известување на пациентите за секој пристап до нивните податоци.
- **Техничка и организациска безбедност:** Категоризација на пристапите и уредување на пристапите со примена на безбедносни мерки како што се автентикација, регистрирање на пристапите и обврска за чување електронска трага од пристапот.
- **Отчетност на контролорите:** Контролорите на податоци се одговорни за обезбедување механизми за следливост и известување.

Законот за заштита на личните податоци има широка територијална и вонтериторијална применливост, со цел да ги заштити правата на физичките лица во сите области каде што обработката може да ги засегне. Но постојат и исклучоци од неговата применливост. Имено, според чл. 2 ст. 3 од овој закон: *Овој закон не се применува на дајтошеките со лични податоци создадени и чувани под одговорност на Информацискиот систем на Република Португалија. (Sistema de Informações da República Portuguesa).* Овие обработки се регулирани со посебни правни акти.

Со донесувањето на овој закон, предвидени се специфични ситуации за обработка на личните податоци<sup>52</sup>, меѓу кои се обработката на здравствените податоци и генетските податоци.

**Во согласност со член 29 став 1 од овој Закон, „при обработка на здравствени и генетски податоци, пристапот до личните податоци се раководи по принципот ’треба да се знае’**

---

50 Службен весник на Републиката, 1° серија, Бр. 169 од 4 септември 2019 година, со што се укинува Законот бр. 48/90 од 24 август и Уредбата со законска сила бр. 185/2002, од 20 август.

51 <https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2005-106603593>

52 Поглавје VI, Закон за заштита на личните податоци на Португалија.

**информацијата.** Обработката и пристапот на електронските медицинските податоци е доверена исклучиво на стручно лице или на друго лице обврзано со должност за тајност и доверливост. Сите лица (раководителите на тела, работниците и давателите на услуги на лицето одговорно за обработка на здравствените податоци и генетските податоци, службеникот за заштита на податоците, студентите и истражувачите од областа на здравството и генетиката и сите здравствени работници) кои имаат пристап до здравствените податоци се обврзани на тајност/доверливост и заштита на податоците<sup>53</sup>.

Португалското законодавство го уредува пристапот до сопствените медицински податоци со обврзувачка норма „субјектот на податоците мора да биде известен за каков било пристап до неговите лични податоци“<sup>54</sup>, додека обработувачот на податоците, односно контролорот е должен да обезбеди достапност до овој механизам за следење, известување и техничка безбедност. Дополнително, со одлуки на владата, односно на ресорните министерства, се определуваат дозволите за пристап, условите за претходна автентикација за оној кој пристапува и електронска евиденција на пристапите и податоците кон кои се пристапува<sup>55</sup>.

Членовите 6 и 7 од португалскиот закон претставуваат основа за транспарентна и безбедна обработка на медицинските податоци.

### Табеларен приказ за пристапот до здравствени податоци

СУБЈЕКТ	НИВО НА ПРИСТАП	ОБВРСКИ
Професионалци обврзани со тајност	Обработка според принципот „треба да се знае“	Должност за тајност; примена на соодветни безбедносни мерки
Вработени и даватели на услуги	Ограничен пристап	Обврска за тајност
Студенти и истражувачи	Ограничен пристап	Обврска за тајност; дозвола за обработка
Регулатори и надзорни органи	Ограничен пристап	Обврска за тајност; електронска евиденција за пристап

Здравствените податоци може да бидат организирани во регистри или централизиран бази на податоци, засновани врз единечни платформи.

53 Ст. 4 Чл. 29.

54 Ст. 6 Чл. 29.

55 Ст. 7 Чл.29.

Националната платформа за здравствени податоци на Португалија е лансирана во мај 2012 година и се состои од два различни портали:

- Портал за здравствени работници кои работат во Националната здравствена служба (Portal do Profissional de Saúde – The Health Professionals’ Portal) и
- Портал на пациентот/корисниците на Националниот здравствен систем (Portal do Utente – The Patient’s Porta)<sup>56</sup>.

Идејата е платформата постепено да биде поврзана и со давателите на здравствени услуги кои не се дел од Националната здравствена служба. Имајќи ги предвид резултатите<sup>57</sup> од едно проектно истражување спроведено за 12 земји членки на ЕУ (TEHDAS – Towards European Health Data space) за периодот од 2021-2022, Електронската здравствена евиденција (EHR) е дигитализирана и централизирана во Националниот клинички регистар на SClínico. Во Португалија, освен SClínico, има околу 80 регистри на податоци, или системи<sup>58</sup>. Исто така, имајќи го предвид ова истражување, приватните болници немаат законска обврска да ги споделат своите податоци со Националниот здравствен систем (NHS)<sup>59</sup>.

Овие позиции се поместуваат, имајќи го предвид сетот од акти на ниво на ЕУ, а тоа се Европската стратегија за податоци 2020 и Актот за управување со податоци (Data Governance Act). Ова имаше влијание за целокупна промена и формирање нов екосистем за трансфер и размена на електронски податоци во рамките на ЕУ. Белата книга за Португалија за European Health Data Space (EHDS), објавена од LabToMarket, април 2024 година<sup>60</sup>, дава посеопфатен приказ на актуелниот статус на Португалија и нејзината подготвеност, и некои тековни иницијативи усогласени со целите на EHDS:

Националниот EHR-систем и високата дигитализација и нивото на дигитализација во здравството ја прави Португалија една од најподготвените земји за интегрирање на EHDS. Понатаму, постои национална иницијатива која се состои од регулирање на универзален EHR со информации од јавни и од приватни болници.

SPMS имплементира широк обем на здравствени податоци и портал за управување со апликации за пристап до податоци.

### 5.3. ОСНОВЕН ЗАКОН ЗА ЗДРАВСТВО ОД 2019 ГОДИНА

Законот за здравство е основен закон во кој се содржани правните основи на португалскиот здравствен систем. Овој закон ги поставува постулатите за усвојување на неопходните дополнителни закони во областа на јавното здравје, здравствената заштита, здравствената политика, здравствениот систем, институционалната рамка, улогата и одговорноста на државата, правата и должностите на луѓето, на здравствените работници, здравствената

---

56 Стр. 7 [https://health.ec.europa.eu/system/files/2016-11/laws\\_portugal\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/laws_portugal_en_0.pdf), пристапено 29.11.2024.

57 Резултатите се објавени во март 2023.

58 Country visit Portugal, стр. 2, <https://tehdas.eu/app/uploads/2023/03/portugal-country-visit-factsheet-03-2023.pdf> пристапено 30.11.2024

59 Country visit Portugal, стр. 2, <https://tehdas.eu/app/uploads/2023/03/portugal-country-visit-factsheet-03-2023.pdf> пристапено на 30.11.2024.

60 <https://eithealth.eu/wp-content/uploads/2024/06/EHDS-white-paper-Portugal.pdf>

писменост, менталното здравје, здравствените информации, ИКТ во здравството, и останато.

Во согласност со основниот закон за здравството, правото на здравствена заштита, како основно право за сите луѓе и граѓани на Португалија, е загарантирано право преку Националната здравствена служба – Serviço Nacional de Saúde, (SNS). Законот го регулира правото на здравствена заштита како право на сите луѓе да уживаат во најдобра физичка, ментална и социјална здравствена состојба, што претпоставува создавање и развој на економски, социјални, културни и еколошки услови кои гарантираат доволно и здрави животни стандарди, работа и слободно време. Правото на здравствена заштита претставува заедничка одговорност на луѓето, општеството и државата и опфаќа пристап, унапредување, превенција, третман и здравствена рехабилитација, континуирана грижа и палијативна нега. Истовремено, државата го унапредува и го гарантира правото на здравствена заштита преку Националната здравствена служба, регионалните здравствени служби и другите јавни, централни, регионални и локални институции.

Во одделот „**Права и должности на луѓето**“, законот ја дава правната рамка за правата, должностите и слободите на луѓето при користењето на правото на здравствена заштита, со почитување на принципите на еднаквост, недискриминација, доверливост и приватност. Понатаму, секој има право на:

- а) **Пристап до здравствена заштита приспособена на неговата состојба**, брзо и во временска рамка која се смета за клинички прифатлива, на достоинствен начин, во согласност со најдобрите достапни научни достигнувања и следејќи ги практиките за добар квалитет и здравствена безбедност;
- б) **Да добива информации** за времето на одговор за здравствената заштита што му е потребна;
- в) **Да биде информиран на адекватен, достапен, објективен, целосен и разбирлив начин за неговата состојба**, целта, природата, можните алтернативи, придобивките и ризиците од предложените интервенции и веројатниот напредок на неговата здравствена состојба, во зависност од здравствениот план што треба да се усвои квалитет и здравствена безбедност;
- г) **На слободен пристап до информациите што го засегаат**, без потреба од посредување од здравствен работник, освен ако тоа не го побара;
- д) **Да ја унапредува благосостојбата и квалитетот на животот** за време на стареењето, од инклузивна и активна перспектива, што ја фаворизира способноста за донесување одлуки и контрола на неговиот живот, преку создавањето адаптивни механизми на прифаќање, автономија и независност, при што детерминантите се социоекономски, еколошки, социјални и здравствени одговори.

Со овој закон се опфатени и постулатите на здравствената политика (законска основа 4), меѓу кои еднаквост и недискриминација во пристапот до квалитетна и навремена здравствена заштита, обезбедување еднаквост во распределбата на ресурсите и користењето на услугите и усвојување мерки за позитивно

разграничување на луѓето и на групите во ситуации на поголема ранливост<sup>61</sup>. Исто така, со оваа секција, португалската влада ја опфаќа потребата од „унапредување на здравственото образование и здравствената писменост, овозможувајќи реализација на слободен и доброволен избор за усвојување здрави животни стилови“<sup>62</sup>. Но, упатува и на креирање партиципативни здравствени политики преку поттикнување „учество на луѓето, заедниците, стручните лица и општинските органи во дефинирањето, следењето и евалуацијата на здравствените политики“<sup>63</sup>.

Во делот „Здравје и геномика“, државата ја препознава важноста на геномиката во областа на јавното здравје, во согласност со принципите:

- а) Достоинство и права на сите луѓе, без оглед на нивните генетски карактеристики;
- б) Бесплатна и доброволна согласност во врска со предвидливите геномски тестови, спроведени во здравствен контекст и на кои им претходи суштинско генетско советување;
- в) Доверливост на геномските податоци поврзани со лице кое може да се идентификува;
- г) Нема неоправдана дискриминација, врз основа на генетските карактеристики на лицето, особено ако е поврзана со болест или инвалидитет, и друго<sup>64</sup>.

Во согласност со **Законската основа 13**, се дефинира статусот на здравствените информации; имено, **здравствените информации се сопственост на лицето** и мора да се обезбеди циркулација на здравствени информации, притоа со почитување на безбедноста и заштитата на личните податоци и здравствените информации, преку интероперабилност и меѓусебна поврзаност на системите во рамки на Националната здравствена служба и принципот на минимална интервенција<sup>65</sup>.

Со цел да се подобри обезбедувањето на здравствената заштита во дигиталното општество, од суштинско значење е примената на ИКТ во обезбедувањето здравствена заштита, пристап до квалитетни здравствени услуги и ефикасно управување со ресурсите<sup>66</sup>.

### 5.3.1. ПРАВА И ОБВРСКИ НА ЗДРАВСТВЕНИТЕ РАБОТНИЦИ

Здравствените работници, поради значајната општествена улога што ја имаат во служба на луѓето и заедницата, подлежат на зголемени етички и деонтолошки должности, особено да ја чуваат професионална тајна во однос на информациите до кои доаѓаат во текот на нивните активности<sup>67</sup>. Здравствените работници имаат право и должност, во рамките на професионалната кариера, да ја вршат својата дејност во согласност со *legis artis* и етичките

---

61 Законска основа 4, г)

62 Законска основа 4, д)

63 Законска основа 4, ф)

64 База 11

65 База 15 т.1 и т.2

66 Види База 16

67 База 28, т.2



правила, со почитување на правата на лицето на кое му даваат нега<sup>68</sup>. Граѓаните имаат пристап до своите здравствени податоци преку веб-портал и можат да се откажат од нивното користење за примарна употреба, но не за секундарна употреба.

### 5.3.2. НАЦИОНАЛНА ЗДРАВСТВЕНА СЛУЖБА

Националната здравствена служба е организиран и артикулиран збир на јавни установи и услуги кои обезбедуваат здравствена заштита, раководен од надлежното министерство за здравствената област, кое ја спроведува одговорноста на државата за заштита на здравјето. Основањето на организацијата и функционирањето на Националната здравствена служба се определени во Основниот закон за здравствена заштита. Своето работење го заснова врз принципите: универзалност, општост, солидарност, економичност, еднаквост, квалитет, транспарентност, интероперабилност, доволност<sup>69</sup>. Сите португалски граѓани се корисници на Националната здравствена служба. Корисници на службата се и лицата со постојано живеалиште или во ситуација на привремен престој или престој во Португалија, кои се државјани на земјите членки на Европската Унија, државјани на трети земји или лица без државјанство, баратели на меѓународна заштита и мигранти со или без соодветен легализиран статус, во согласност со важечкиот правен режим.

SClinico Hospitalar е еволутивен информациски систем, развиен од SPMS, кој е креиран од огромното искуство со две претходни апликации користени од илјадници лекари, медицински сестри и други здравствени техничари: SAM (Sistema de Apoio ao Médico), систем за поддршка на лекар, и SAPE (Sistema de Apoio à Prática de Enfermagem), систем за поддршка за медицинска сестра. Таа прерасна во единствена апликација, заедничка за сите даватели на здравствени услуги, и фокусирана на пациентите. Оваа алатка е присутна во 50 субјекти во здравствениот сектор и ја користат околу 75 % од болничкиот тим, што одговара на повеќе од 66.500 корисници на системот од различни области. SClinico е дел од стратегијата дефинирана од Министерството за здравство за областа на клиничката компјутеризација на SNS (Serviço Nacional de Saúde), која предвидува стандардизација на процедурите за медицински досиеја, со цел да се гарантира стандардизација на информациите.

Пристапот до разновидните клинички информации на корисникот, употребата и споделувањето податоци со здравствените работници од различни области и нивната систематизација ќе овозможи хомогенизација на практиките и на информациите собрани на национално ниво, со што работата на здравствените работници ќе биде поефикасна, овозможувајќи им подобро да ја извршуваат својата улога во мултидисциплинарниот тим, да обезбедат подобра поддршка, помош и следење на корисникот<sup>70</sup>.

68 База 28, т.4

69 База 20, т.2

70 <https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/>

### 5.3.3. ЕЛЕКТРОНСКИ ЗДРАВСТВЕН СИСТЕМ

Националната комисија за електронски здравствени евиденции беше формирана на почетокот од 2011 година, но многу бргу заменета како Комисија за клиничка дигитализација (Comissão para a Informatização Clínica), функционира под директен надзор на државниот секретар за здравство. Комисијата за клиничка дигитализација беше основана со конкретна цел за спроведување платформа за здравствени податоци (Plataforma de Dados de Saúde) и создавање единствено клиничко резиме за корисниците на Националниот здравствен систем – RCU2 (Resumo Clínico Único do Utente – RCU2). Откако беа лансирани платформата за здравствени податоци и RCU2, Комисија за клиничка дигитализација беше заменета со Комисијата за следење на клиничката дигитализација (CAIC – Comissão de Acompanhamento da Informatização Clínica)<sup>71</sup>. Треба да се напомене дека информациите вклучени во овој извештај за функционирањето на Платформата за здравствени податоци, и особено на RCU2, се заснова исклучиво врз десктоп истражување, особено на одлуката на Националната комисија за заштита на податоците која го одобри формирањето Платформа за здравствени податоци и создавањето на RCU2.

## 5.4. ЗАКОН ЗА ЛИЧНИ ГЕНЕТСКИ ИНФОРМАЦИИ И ЗДРАВСТВЕНИ ИНФОРМАЦИИ ОД 2005 ГОДИНА<sup>72</sup>

Овој закон го дефинира поимот на здравствени и генетски информации, циркулацијата на информации и интервенцијата на човечкиот геном во здравствениот систем, како и правилата за собирање и складирање биолошки производи за целите на генетско тестирање или истражување. Португалското законодавство определува кои податоци се здравствени податоци/информации (чл.2), медицински податоци/ информации (чл.5) и генетски податоци/ информации (чл.6). Овој Закон опфаќа материја која се однесува на директните и индиректните информации за здравјето на поединецот:

### 5.4.1. ЧЛЕН 2 – ЗДРАВСТВЕНИ ИНФОРМАЦИИ

За целите на овој закон, поимот ‘здравствени информации’ ги опфаќа сите видови директни или индиректни информации тесно поврзани со здравјето, постојни или идни, на едно лице, без оглед дали е живо или починато, и неговата клиничка и семејна историја.

### 5.4.2. ЧЛЕН 3 – СОПСТВЕНОСТ НА ЗДРАВСТВЕНИТЕ ИНФОРМАЦИИ

**Здравствените информации, вклучително и евидентираниите клинички податоци, резултатите од анализи и други дополнителни испитувања, интервенции и дијагностика се во сопственост на лицето, а единиците на здравствениот систем се депозитари на информациите, кои не можат да се користат за други цели освен за обезбедување нега и здравствени истражувања и други цели утврдени со закон.**

71 [https://health.ec.europa.eu/system/files/2016-11/laws\\_portugal\\_en\\_0.pdf](https://health.ec.europa.eu/system/files/2016-11/laws_portugal_en_0.pdf) стр. 7

72 Службен весник на Републиката – I серија-а, бр. 18 од 26 јануари 2005 година.

Имателот на здравствена информација има право, доколку сака, да биде запознат со целата клиничка ситуација што се однесува на него, освен во исклучителни оправдани околности и во кои недвосмислено се покажува дека тоа може да биде штетно за него, или да му биде соопштено некому посочен од него.

### 5.4.3. Член 4 – ПРИСТАП ДО ЗДРАВСТВЕНИТЕ ПОДАТОЦИ

Пристап до здравствена информација од страна на нејзиниот имател или трети лица со негова согласност, се врши преку лекар, со соодветни квалификации, избран од страна на имателот на информацијата. Здравствените информации може да ги користи само здравствениот систем под условите содржани во овластување дадено од нивниот имател или од неговиот застапник.

### 5.4.4. Член 5 – МЕДИЦИНСКИ ИНФОРМАЦИИ

Медицински информации се здравствени информации наменети да се користат за обезбедување здравствена заштита или здравствени третмани, се внесуваат во клиничкото досие од страна на лекарот кој го лечел лицето или, под негов надзор, компјутеризирани од друго стручно лице кое исто така е обврзано на тајност и заштита на податоците, во рамките на специфичните вештини на секоја професија и со почитување на соодветните етички стандарди. Здравствените податоци, дигитални или во физичка форма, се внесуваат во вид на запис, т.е. клиничко досие. Секое клиничко досие треба да ги содржи сите достапни медицински информации кои се однесуваат на лицето, освен законските ограничувања. **До клиничкото досие пристап има само лекарот одговорен за обезбедување здравствени услуги во корист на лицето на кое се однесува или, под негов надзор, друг здравствен работник обврзан со должност за тајност и до степен кој е строго потребен за извршување на истото, без да се влијае врз епидемиолошките, клиничките или генетските истражувања за човечкиот геном (каде што се гарантира слободен пристап на научната заедница до податоците кои произлегуваат од истражувањето на човечкиот геном, по претходно одобрение од релевантни етички комитети).**

Судската практика покажала дека медицинските досиеја се третираат како административни документи и не секогаш се во сопственост на имателот<sup>73</sup>. Имено, првиот португалски случај што се однесувал на правото на пристап до медицинската документација бил пресуден од Апелациониот суд во Порто (Трибуналот Relacao do Porto). Тужителот учествувал во сообраќајна несреќа во која бил повреден и се здобил со делумен инвалидитет, а за повредите сакал да добие отштета од локална осигурителна компанија. Тој ја побарал својата клиничка евиденција од болницата (неименувана во извештајот) како доказ, но бил одбиен. Бидејќи имал намера да ги користи своите медицински досиеја како доказ за судење, тој се обратил до Судот, барајќи судски налог да

73 V. v. European Parliament, Case F-46/09, Judgment of 5 July 2011, para 110 – onward. Anatoliy A. Lytvynenko: Right to Access to Medical Records in the Case Law of the Portuguese Courts: Possible Guidelines for future European Court of Human Rights Case Law, Athens Journal of Law 2020, 6: 1-18, стр.9

ја принуди болницата да ги приложи овие документи. Судот потврдил дека тужителот има право да изврши увид во евиденцијата и побарал од тужителот да назначи лекар на кого треба да му бидат испратени записите (во подоцнежната судска пракса се смета дека ова не е строго неопходно). Имено, во конкретниов случај судот се согласил дека одредбите од чл. 2-3 од Законот бр. 12/2005 гарантираат дека информациите поврзани со здравјето се навистина сопственост на засегнатото лице, но, во исто време, не се поседувани од него, туку се во сопственост на здравствените установи<sup>74</sup>.

Не постојат специфични национални правила кои пропишуваат различни категории здравствени податоци со различни нивоа на доверливост; сепак, член 3(5) од Законот за лична генетика и здравствени информации вели дека „управувањето на системите за здравствени податоци на организацијата мора да обезбеди поделба помеѓу здравствени и генетски податоци и преостанатите лични податоци, преку воспоставување различни нивоа на пристап.“

#### **5.4.5. Член 6 – ГЕНЕТСКИ ИНФОРМАЦИИ**

Генетските информации се здравствени информации кои се однесуваат на наследни карактеристики на едно или повеќе лица, меѓусебно поврзани или со заеднички карактеристики од овој вид. Употребата на генетска информација е чин помеѓу нејзиниот носител и лекарот, што подлежи на деонтолошки правила за професионална тајна на лекарите и на другите здравствени работници. Граѓаните имаат право да знаат дали некое клиничко досие, архивски или медицински или истражувачки запис содржи генетски информации за нив и за нивното семејство и да ги знаат целите и употребата на тие информации, начинот на којшто се чуваат и роковите на нивното зачувување. Пристапот, доверливоста и безбедноста на генетските информации е предмет на законски и административни засилени мерки. Запис, дигитален или не, кој содржи генетски информации за група луѓе или семејства се определува како „Генетска база на податоци“. Генетските бази на податоци што содржат семејни информации и генетски записи кои овозможуваат идентификација на членовите на семејството треба да се чуваат и да бидат под надзор на лекар специјалист по генетика или, во негово отсуство, на друг лекар. Правилата за создавање, одржување, управување и безбедност на генетските бази на податоци за обезбедување здравствена заштита и здравствени истражувања се уредуваат во согласност со законската регулатива за заштита на личните податоци. Секое лице може да бара пристап до информациите што се однесуваат на него, а кои се содржани во досиејата со лични податоци.

### **5.5. КРАТКО РЕЗИМЕ**

Во согласност со европската Општа регулатива за заштита на податоци (GDPR), португалското законодавство воведува клучни механизми за заштита на личните податоци, со акцент врз транспарентноста, техничката и организациска безбедност и отчетност на контролорите.

Португалскиот здравствен информативен систем е дигитализиран со централизирано управување со ЕЗК. Електронската здравствена евиденција (EHRs) е дигитализирана и

---

74 See. *B. c. C.*, Acordao do Tribunal da Relacao do Porto, 08.09.2019, Processo No. 2147 /18.T8AGD.P1, Sec. II. стр.10.

централизирана во Националниот клинички регистар на SClinico. Во Португалија, освен SClinico, има околу 80 регистри на податоци или системи.

Многубројни институционални чинители се инволвирани во процесот на дигитализација, управување и заштита на здравствените и медицинските податоци. Министерството за здравство е составено од управа која го опфаќа јавното здравство, агенции, индиректна администрација составена од лаборатории и национални институти и јавен бизнис-сектор составен од јавни претпријатија, национални болници и заеднички услуги (SPMS). SPMS е давател на ИКТ на Националната здравствена служба (NHS). Повеќето здравствени податоци се чуваат на структуриран начин на изворот. Националниот институт за здравје „Доктор Рикардо Хорхе“ (ИНСА) е национален институт за здравје и национална лабораторија за здравје. Ја има единствената биобанка за примероци базирана на население. Во моментот<sup>75</sup>, нема централизиран каталог на метаподатоци што обезбедува општ преглед на податоците поврзани со здравјето, збирки и процедури за пристап.

Порталот за транспарентност има каталог на метаподатоци заснован врз DCAT-AP стандард, но само за отворените податоци до кои дава пристап. Тоа е портал за транспарентност со најмалку 150 структурирани, отворени податоци од анонимизирани збирки на податоци, збирни податоци и податоци добиени од различни извори (на пр., INSA, ACSS, DGS).

Овие механизми не само што ги штитат правата на пациентите, туку и ја зголемуваат довербата во здравствените системи, што е предуслов за успешна имплементација на дигитализирани здравствени услуги. Концептот за **автоматизирано известување за пристап до податоците** обезбедува транспарентност и доверба, додека деталното уредување на **техничките стандарди** гарантира безбедност и функционалност.



# 6

## ПРЕПОРАКИ И ПРЕДИЗВИЦИ ЗА СЕВЕРНА МАКЕДОНИЈА

Врз основа на направената анализа за Северна Македонија, како и направената компаративна анализа за одредени европски држави, се доаѓа до заклучокот дека потребно е дорегулирање на прашањето за заштита на медицинските податоци, особено во однос на пристапот до медицинските податоци. Во таа насока, во продолжение ќе се идентификува фактичката состојба во Северна Македонија во однос на одредени прашања околу заштитата на медицинските податоци, конкретни препораки за преземање одредени решенија од анализираните практики на горенаведените земји, како и предизвиците со кои може да се соочи земјата при нивната имплементација.

### 6.1. ПРЕПОРАКИ ЗА ЗАКОНСКИ ИЗМЕНИ И ТЕХНИЧКИ РЕШЕНИЈА

#### 1. ДА СЕ ИМПЛЕМЕНТИРА ЕСТОНСКИОТ МОДЕЛ ЗА НАЦИОНАЛЕН ЗДРАВСТВЕН ИНФОРМАТИВЕН СИСТЕМ (ENNIS)

- **Фактичка состојба во Македонија:** Северна Македонија сè уште нема целосна дигитализација на досиејата на пациентите и има незадоволително ниво на поврзаност и размена на медицински податоци со приватните здравствени болници и даватели на здравствени услуги, со што се јавува дуплирање на медицински податоци (досиеја, третмани, дијагнози, снимања) за еден пациент.
- **Практика:** Во Естонија, сите даватели на здравствени услуги имаат обврска да

ги внесат електронските здравствени досиеја (EHR) на национално ниво, овозможувајќи централизирана контрола и пристап за пациентите преку порталот „Моето е-здравје“. Естонија користи KSI блокчејн (Keyless Signature Infrastructure) за осигурување на интегритетот на медицинските податоци и следливост на пристапите, што ја зголемува довербата и безбедноста.

- **Примена во Македонија:**

- » Да се ревидира „Законот за евиденции во областа на здравството“, со цел воведување задолжителен електронски запис,
- » Да се централизираат сите бази на е-податоци,
- » Да се воведат обврска за интероперабилност помеѓу државните и приватните даватели на здравствени услуги,
- » Да се обезбеди систем сличен на естонскиот, каде што пациентите ќе имаат централен пристап до своите податоци. Да му се овозможи на секој пациент да може:
  - Да контролира кој има пристап до нивните податоци, и
  - Да биде известен/ добива нотификации за секој пристап или промена во неговото е- здравствено досие во реално време (in real time).
- » Да се воведат блокчејн технологија за дополнителна безбедност.

- **Предизвици за Македонија**

- » Недостаток на ИКТ инфраструктура и поддршка на интегрираниот здравствен систем.
- » Високи финансиски издатоци за унапредување на моделите и платформите за безбеден трансфер и обработка на податоците помеѓу многубројните релевантни институции во целокупниот процес.

## 2. ДА СЕ ВОВЕДАТ ПРИНЦИПИТЕ ЗА ТРАНСПАРЕНТНОСТ И ОГРАНИЧЕН ПРИСТАП ОД СЛОВЕНЕЧКИОТ МОДЕЛ

- **Фактичка состојба во Македонија:** Корисникот на јавните здравствени услуги (субјектот) нема директна можност, ниту механизам (алатка) за контрола на сопствените медицински податоци, кога трето лице пристапува, обработува или ги менува неговите медицински податоци.
- **Практика:** Словенија го користи „ZZPPZ“ како основен закон за ограничување на пристапот до медицински податоци и употреба на „CRPP“ како централен регистар.
- **Примена во Македонија:**
  - » Законот за заштита на личните податоци и Законот за евиденции во областа на здравството треба да се дополнат со одредби за строги услови за пристап до медицински податоци, со дефинирани улоги и овластувања.
  - » Создавање централен регистар на здравствени податоци со јасно дефинирани услови за пристап и употреба.
- **Предизвици за Македонија:**



- » Потреба од основање еден независен субјект заради архивирање на медицинските податоци, со строго контролиран пристап (Банка чувар на медицински податоци) и
- » Дополнителни постапки и процедури за основање, определување надлежности и овластување на новооснованиот субјект.

### 3. ИНТЕГРИРАЊЕ НА ПОРТУГАЛСКИОТ ПРИСТАП ЗА СЕКУНДАРНА УПОТРЕБА НА ЗДРАВСТВЕНИТЕ ПОДАТОЦИ

- **Фактичка состојба во Македонија:** Законодавецот не прави јасна разлика помеѓу примарна и секундарна употреба на здравствените податоци. Не постои ефикасен систем на контрола при трансфер на посебните податоци кон трети лица и нарушување на безбедноста на личните податоци.
- **Практика:** Португалија има јасно регулирани услови за примарна и за секундарна употреба и пристап до медицински податоци преку националниот клинички регистар „SClinico“.
- **Примена во Македонија:**
  - » Да се создаде правна рамка за секундарна употреба на здравствените податоци за истражување, во согласност со GDPR.
  - » Ова може да се регулира преку дополнителен правилник или измена на Законот за заштита на правата на пациентите.
- **Предизвик за Македонија:**
  - » Потреба од усогласен пристап на сите донесувачи на одлуки за пристапот до медицинските податоци од примарна и од секундарна употреба. Потребно е дополнување на Законот за заштита на личните податоци.

## 6.2. ПРЕПОРАКА ЗА ПРИМЕНА НА ПРИНЦИПИ ЗА ТРАНСПАРЕНТНОСТ И ОГРАНИЧЕН ПРИСТАП ОД СЛОВЕНЕЧКИОТ МОДЕЛ

Имајќи ги предвид анализите од трите земји, како и нивното државно-правно уредување (административно-територијална организација), општествено-економски, социјален развој и животен стил, во однос на прашањата на транспарентност и ограничен пристап до медицински податоци, Република Северна Македонија може да го имплементира моделот на Р Словенија.

Во словенечкиот модел, Законот за бази на податоци од областа на здравствената заштита (ZZPPZ) и Законот за заштита на личните податоци (ZVOP-2) ја регулираат транспарентноста и ограничувањето на пристапот до здравствените податоци. Ова се постигнува преку детално уредување на улогите и правата на пристап во однос на видот на евиденцијата и специјализацијата на корисникот.

### 1. КАТЕГОРИЗАЦИЈА НА ПРИСТАПОТ СПОРЕД ВИДОТ НА ЕВИДЕНЦИЈА:

- **Основна медицинска документација:**

» Пристап дозволен само на матичниот лекар на пациентот и на лекари специјалисти директно вклучени во третманот.

» Пример: анамнеза, лабораториски тестови, дијагностички извештаи.

- **Специјализирани евиденции:**

» Пристап дозволен само на специјалисти со релевантна специјализација.

» Пример: Психијатриски извештаи достапни само за психијатри.

- **Истражувачки податоци:**

» Пристап дозволен само по анонимизација, за научни цели, со претходна согласност од регулаторен орган.

» Пример: Епидемиолошки податоци за анализи.

## 2. ДЕФИНИЦИЈА НА КОРИСНИЧКИ УЛОГИ:

- **Општи корисници:** Матични лекари со пристап до целосната историја на пациентите кои ги третираат.

- **Специјалисти:** Ограничен пристап до евиденцијата поврзана со нивната специјализација.

- **Администратори:** Ограничен пристап до технички податоци, без право на увид во содржината.

- **Истражувачи:** Пристап само до анонимизирани податоци.

## 3. ВОВЕДУВАЊЕ ТРИ ВИДА НА ПРИСТАП:

- **Примарен пристап:**

» Лекари и медицински персонал кои се во директен контакт со пациентот.

» Услов: Врска помеѓу пациентот и здравствената установа.

- **Секундарен пристап:**

» За специјалисти кои добиле барање за консултација од матичниот лекар.

» Услов: Пристап до специфични податоци кои се релевантни за консултацијата.

- **Рестриктивен пристап:**

» За администратори и истражувачи.

» Услов: Анонимизација на податоците и документ со дозвола за пристап.

## 4. ТЕХНИЧКА ИМПЛЕМЕНТАЦИЈА:

- **Регистар на улоги и пристап:** Развивање систем за управување со пристап базиран на улоги (Role-Based Access Control – RBAC).

- **Контролен механизам:** Секој пристап автоматски да се евидентира (audit log), со цел следливост и спречување злоупотреба.

- Промоција и зајакнување на улогата на Агенцијата за заштита на личните податоци од

областа на здравството.

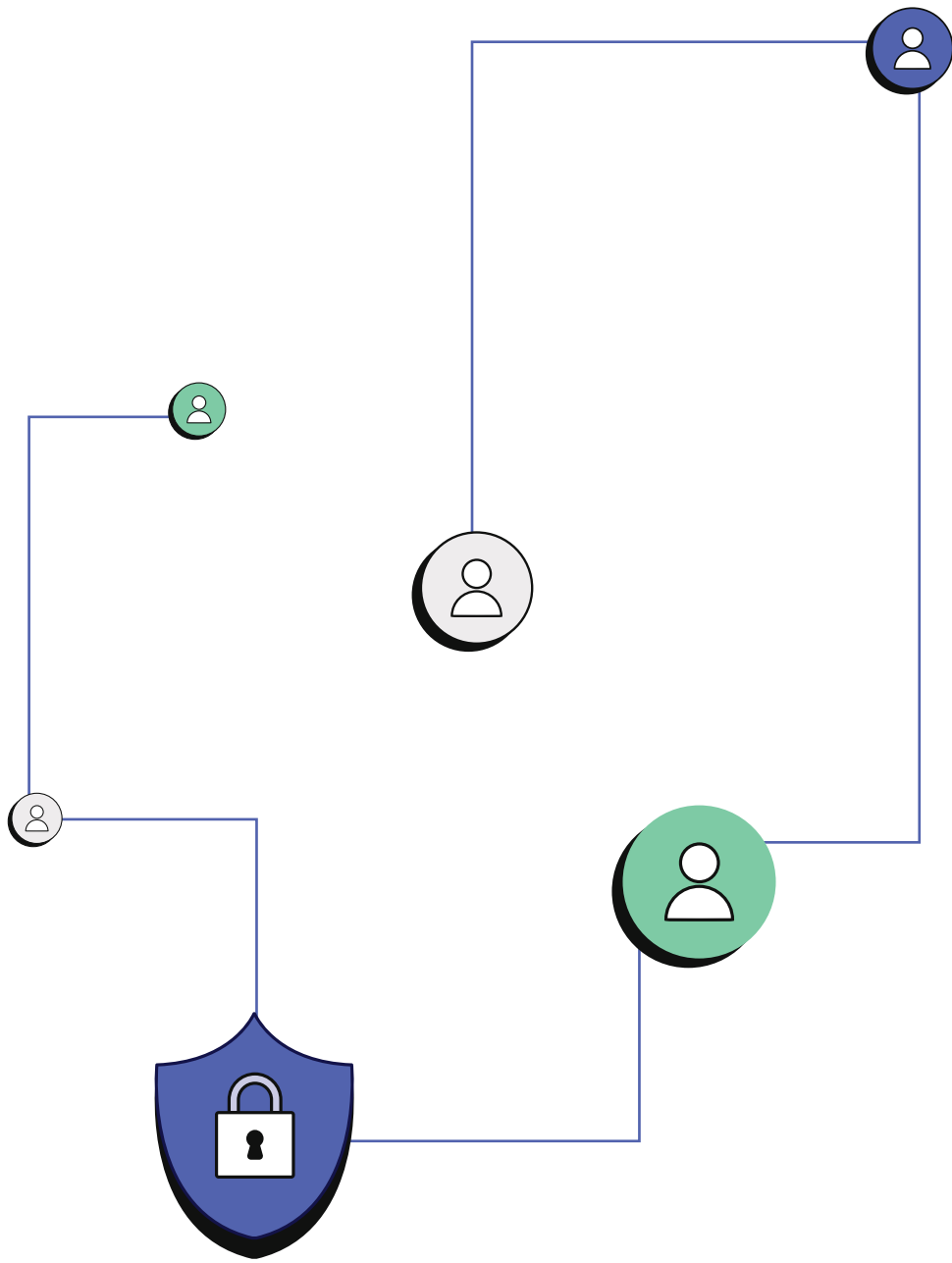
- Унапредување на системот за контрола и безбедност на дигиталните податоци.

#### 5. ПРИМЕНА ВО ПРАКТИКА:

- **Изменување на постоечкиот Правилник за начинот на пристап, дистрибуција, издавање, користење, чување и заштита на податоците од интегрираниот здравствен информатички систем:**
  - » Усвојување анекс со дефиниција на трите вида пристап и видот на специјалист, по примерот на Словенија.
  - » Опис на типот на евиденција, кој може да пристапи и во кои околности, по примерот на Словенија.
- **Едукација на персоналот:** Обуки за разликите во пристапот и имплементацијата на новите правила и континуирана едукација.
- **Информатичка платформа:** Интеграција на новите правила во електронскиот систем за здравствени податоци.

#### Правна основа за измените:

- **Закон за заштита на правата на пациентите:** Да се прошири со нови одредби за дефинирање пристап.
- **Закон за евиденциите во областа на здравството:** Дополнување со посебни членови за ограничување и контролирање на пристапот според улогата и потребата.



# 7

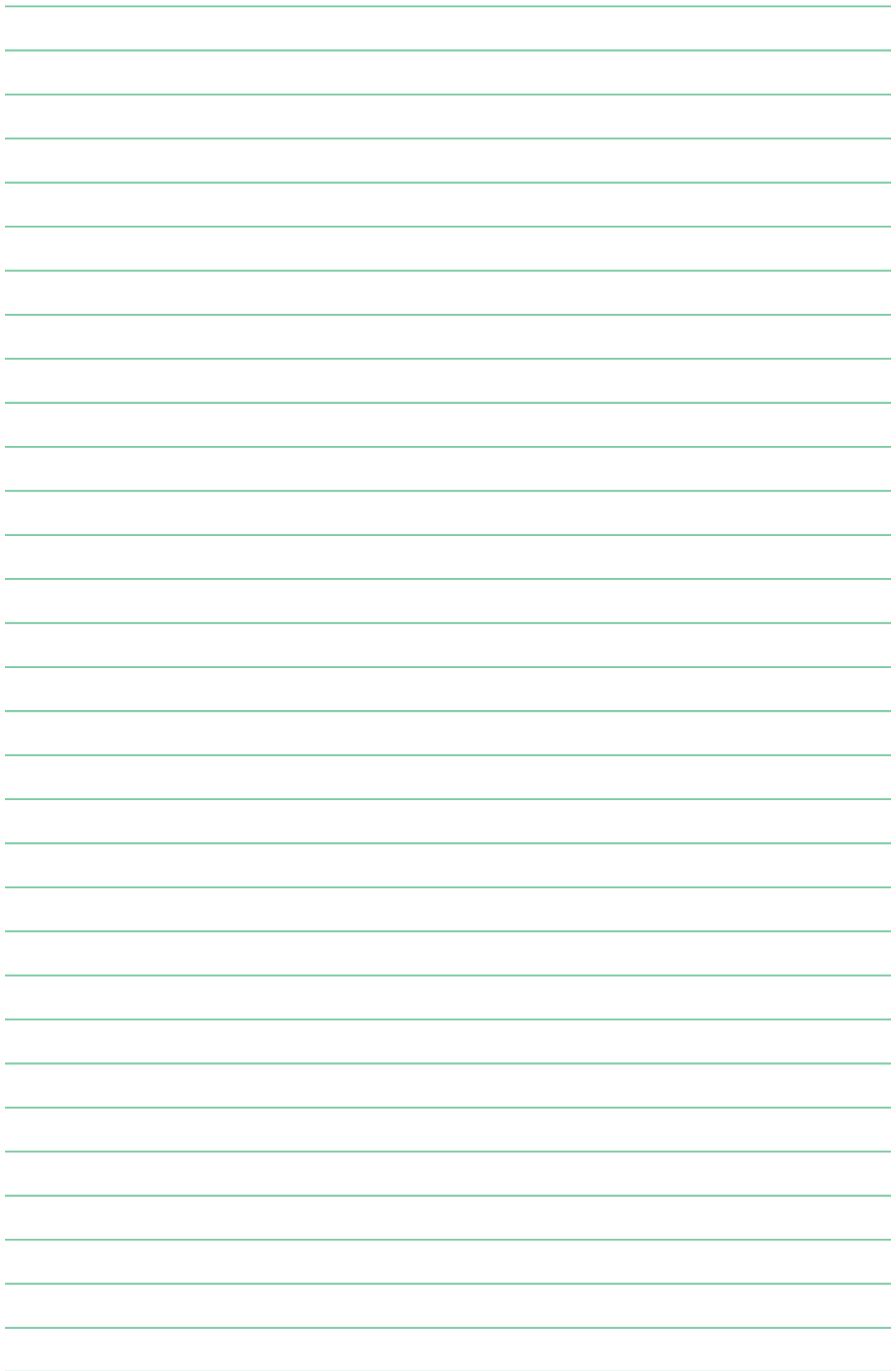
## ЗАКЛУЧОК

И покрај софистицираниот пристап и континуираната надоградба на ИТК здравствените системи во насока на подобрување на здравствените услуги и заштита на податоците, генерално, секоја држава има предизвици кои произлегуваат од дилеми поврзани со пристапот до медицинските податоци, како и до нивната обработка и трансфер. Медицинските податоци, како посебна категорија податоци, можат да бидат обработени и достапни само доколку постои правна основа за тоа (изјава на волја, договор, законска основа, оправдан интерес). Без разлика на степенот на развој и ефикасниот пристап кон примена на законските и подзаконските решенија, сите држави се соочуваат со дилемата за балансиран пристап до медицинските податоци која произлегува од конфликтот помеѓу желбата за пристап до медицинските податоци и потребата да се заштитат посебните категории на лични податоци. Меѓутоа, сите се држат до императивот за заштита на медицинските податоци и за зголемување на сигурноста при трансферот на податоците, а притоа да не се скрати правото на давање ефикасна и квалитетна здравствена услуга на поединецот.

Државата не заостанува многу при имплементирањето на законските и практичните решенија, но од анализите може да се заклучи и дека не е доволно спремна за да може да ги следи добрите практики, технички реченија и сигурносни механизми од европските земји во однос на здравствената дигитализација. Неопходно е да се посвети внимание во воспоставувањето заеднички стандарди за електронска размена на здравствени податоци и навремено стратешко вклучување на ИТ решенија за автоматско известување и следење на податоците. Од друга страна, од направената

анализа и споредувањето на законодавствата на Словенија, Португалија и Естонија, произлегува дека Северна Македонија треба подетално да го регулира прашањето на транспарентност и пропорционалност во пристап до медицински податоци, со што ќе се осигури дека контролата врз употребата на податоците е во рацете на самиот субјект или, во случајот, пациентот.







Издавач: Здружение за поддршка на луѓето што живеат со ХИВ – ЗАЕДНО ПОСИЛНИ Скопје

Уредник: Атанас Аврамов

Автори: Кристина Мишева, Марија Амповска

Лектура: Татјана Б. Ефтимоска

Графички дизајн: Александра Софрониевска

Година на издавање: Скопје, 2025

Печати: Полиестердеј - Скопје

Тираж: 100

Овој материјал е изработен во рамки на проектот „Безбедноста на медицинските податоци на пациентите во Северна Македонија и нејзината поврзаност со дискриминацијата“ финансиски поддржан од Digital Freedom Fund, а е дел од работната програма на ЗАЕДНО ПОСИЛНИ за 2024 година, која е поддржана од Европската Унија. Содржината е единствена одговорност на Здружението ЗАЕДНО ПОСИЛНИ Скопје и не ги одразува ставовите на Европската унија или на Digital Freedom Fund.

Овој материјал може слободно да се репродуцира, во целост или делумно, при што е потребно да се наведе изворот.

CIP - Каталогизација во публикација

Национална и универзитетска библиотека "Св. Климент Охридски", Скопје

342.728 : 61(4-672 ЕУ)

342.738:616-052(4-672 ЕУ)

342.738:61(497.7)

342.726:616-052(497.7)

МИШЕВА, Кристина

Процеси и предизвици во уредувањето на пристап до медицински податоци : европски искуства и примена во Северна Македонија / Кристина Мишева, Марија Ампова. - Скопје : Здружение за поддршка на луѓето што живеат со ХИВ - Заедно посилни, 2025. - 69 стр. ; 21 см

Тираж 100. - Фусноти кон текстот

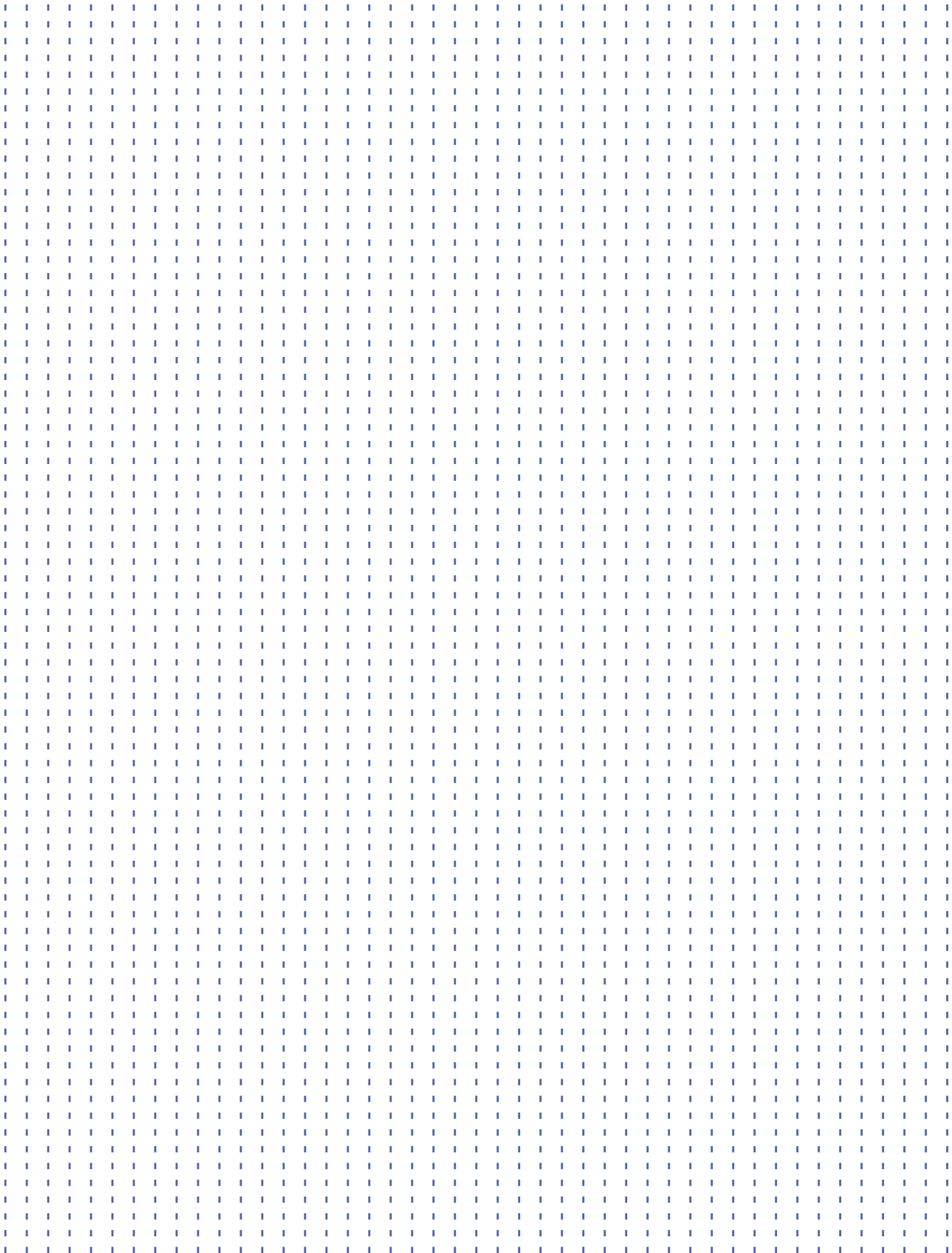
ISBN 978-608-66936-5-7

1. Ампова, Марија [автор]

а) Пристап до медицински податоци -- Уредување -- Европска Унија б)

Пристап до медицински податоци -- Уредување -- Македонија

COBISS.MK-ID 65207045



Годишна работна  
ПРОГРАМА ФИНАНСИРАНА  
ОД ЕВРОПСКАТА УНИЈА



Digital  
Freedom Fund

ЗАЕДНО  
ПОСИЛНИ