СОЦИАЛНО-ПРАВНИ АСПЕКТИ ПРИ РАБОТА С ДАННИ И ГАРАНТИРАНЕ НА СИГУРНОСТ ЗА ЗДРАВНАТА ИНФОРМАЦИЯ

Проф. д.н. Мариела Деливерска [*]

Резюме: *Здравната информация е едновременно правно защитена „специална категория“ лични данни и критичен ресурс за непрекъснатостта на медицинските услуги. Настоящата статия разглежда социално-правните и юридическите предпоставки за законосъобразно обработване на здравни данни и гарантиране на сигурността им, като свързва изискванията на Общия регламент относно защитата на данните (GDPR), националната уредба за „здравна информация“ и секторните режими по киберсигурност в един приложим организационен модел.*

На теоретично ниво се систематизират правните основания, ролите и отговорностите (администратор/обработващ, длъжностно лице по защита на данните, надзорни органи), принципите на обработване, управлението на риска и съотносимите мерки за „поверителност-цялостност-наличност“.

На практико-приложно ниво се предлага рамка за съответствие и информационна сигурност по жизнения цикъл на данните. Акцентът е върху социалната значимост: доверие в системата на здравеопазването, предотвратяване на стигматизация и дискриминация, и гарантиране правата на пациентите при цифровизацията (електронно здравно досие, здравно-информационни системи и свързани услуги).

Ключови думи: *Здравни данни; Медицинска информация; Информационна сигурност; Киберсигурност; Оценка на въздействието.*

SOCIAL AND LEGAL ASPECTS OF DATA PROCESSING AND ENSURING THE SECURITY OF HEALTH INFORMATION

Prof. D.Sc. Mariela Deliverska, PhD [*]

Abstract: *Health information is both a legally protected "special category" of personal data and a critical resource for the continuity of medical services. This article examines the socio-legal and legal prerequisites for the lawful processing of health data and for ensuring its security, by integrating the requirements of the General Data Protection Regulation (GDPR), the national framework governing "health information," and sector-specific cybersecurity regimes into a single, workable organizational model.*

At the theoretical level, the paper systematizes the legal bases, roles and responsibilities (controller/processor, data protection officer, supervisory authorities), the principles of processing, risk management, and the corresponding measures for "confidentiality–integrity–availability."

At the practical and applied level, it proposes a compliance and information security framework across the data lifecycle. The emphasis is on the social significance: trust in the

[*] Проф. д.н. Мариела Деливерска, Университет по застраховане и финанси, mdeliverska@uzf.bg
[*] Prof. D.Sc. Mariela Deliverska, PhD - University of Insurance and Finance, mdeliverska@uzf.bg

healthcare system, prevention of stigmatization and discrimination, and safeguarding patients' rights in the context of digitalization (electronic health record, health information system, and related services).

Key Words: *Health data; medical information; information security; cybersecurity; impact assessment.*

В контекста на бързо напредващата дигитална трансформация в здравеопазването, здравната информация придобива статут на ресурс с особено важна роля и повишена чувствителност. Тя е едновременно необходима основа за диагностично-лечебния процес и гарантиране на непрекъснатостта на медицинските услуги, и обект на засилена правна защита поради потенциално значимите последици при неправомерно обработване. Развитието на електронни здравни досиета, интегрирани регистри, прилагане на телемедицина и интензивен обмен на данни между лечебни заведения, лаборатории, платци и държавни информационни системи увеличава обема, скоростта и сложността на обработването, като разширява рисковия профил и усложнява веригата на отговорност. В тази връзка, гарантирането на сигурността на здравната информация следва да се разглежда не само като задача с която се занимават информационните технологии, а като комплексен социално-правен въпрос, в който се пресичат етични стандарти, обществено доверие, нормативни изисквания и управленски решения.

Социално-правният измерител на работата със здравни данни се проявява в уязвимостта на пациента спрямо неправомерен достъп, разкриване или манипулиране на медицински записи и данни. Нарушенията на поверителността могат да доведат до стигматизация и дискриминация (например при психични разстройства, зависимости, репродуктивно здраве); до отказ от търсене на медицинска помощ; и до ерозия на доверието в здравната система като обществена институция. Ето защо принципът на медицинската тайна и изискванията за законосъобразност и прозрачност при обработването имат не само юридическа, но и ясно изразена обществена функция – да гарантират, че пациентът може да предоставя чувствителна информация без страх от вреди извън лечебния контекст.

- **Социално-прани и юридически аспекти**

Юридическите аспекти се обединяват около статута на здравната информация и медицинските данни като специална категория лични данни, изискваща по-строги условия за обработване, както и около задължението за прилагане на подходящи технически и организационни мерки за сигурност при обработването. В практиката това означава ясна дефиниция на роли (администратор/обработващ), правни основания за обработване (лечение, законови задължения, обществен интерес, научни цели и др.), договорно управление на доставчици и доказуемост при контролна дейност (чрез документация и одитни следи). Едновременно с режима на защита на личните данни, секторът на „здравеопазване“ попада под засилени режим на защита и високи изисквания за киберсигурност, тъй като киберинцидентите могат да нарушат не само поверителността, но и да компрометират функционирането на системи, от които зависи предоставянето на медицинска помощ. В тази връзка, отношението „поверителност - цялостност - наличност“ придобива особено значение е специфична тежест. Прекъсването на болнични информационни системи може да има пряко отражение върху живота и здравето на хората.

Социално-правните аспекти при работа със здравни данни трябва да се разглеждат като единен проблем на регулаторното съответствие и управление на риска, при който правните принципи се „превеждат“ в контролни механизми и организационни практики. Фокусът следва да бъде поставен е върху начинът по който нормативните изисквания се трансформират в реални процеси, включващи контрол на достъпа, разграничаване на роли и контекст на употреба, механизми за защита, политики за съхранение и унищожаване. Въвеждането на подобен подход има ключово значение за устойчивостта на цифровото здравеопазване – то укрепва доверието, защитава правата на пациентите и създава предпоставки за сигурен обмен на информация в полза на общественото здраве.

С оглед постигне на високо ниво на защита, е необходимо да се разработи и приложи цялостен завършен теоретичен и практико-приложен модел за правно съответствие и управление на сигурността при обработването на здравни данни. Използването на подобен модел е в състояние да минимизира правните и репутационните рискове; да намали вероятността от и въздействието при киберинциденти; да повиши доверието на пациентите и устойчивостта на здравните услуги.

Нормативната рамка на Европейския съюз (ЕС) поставя водещ стандарт чрез Общия регламент относно защитата на данните (GDPR), който квалифицира данните, свързани със здравето, като специална категория лични данни и допуска обработването им само при наличие на конкретни правни основания и подходящи гаранции. В теоретико-правен аспект, това изисква ясно разграничаване между правно основание по чл. 6 и изключение (условие) по чл. 9 – т.е. не е достатъчно обработването да е „полезно“ или „удобно“, а трябва да е необходимо и правно обосновано за конкретна легитимна цел.

В здравния сектор съгласието не следва да се използва механично като универсална „разрешителна“ формула, тъй като често съществува зависимост или асиметрия между пациент и доставчик на грижа. Вместо това обработването обичайно се основава на необходимост за медицинска диагностика и лечение, за изпълнение на правно задължение, за обществен интерес в областта на общественото здраве или за управление на системи и услуги в здравеопазването при спазването на принципите на професионална тайна и гаранции на професионална дейност. Ключово значение имат принципите на обработване – законосъобразност, добросъвестност и прозрачност; ограничение на целите; ограничение на съхранението; цялостност и поверителност; и не на последно място – отчетност. Тези принципи и основни начала, гарантиран същността на съответствието и изискват от организациите да демонстрират доказуем контрол върху данните през целия им жизнен цикъл – от събиране и въвеждане в медицинска документация до архивиране, споделяне, вторична употреба (научни/статистически цели) и унищожаване.

Наред с принципите, GDPR въвежда концепцията за защита на данните още при проектирането и по подразбиране, като се взема под внимание и рисково базиран стандарт за сигурност (сигурност на обработването). Теоретично това означава, че сигурността не е фиксиран списък от технологии, а съвкупност от мерки, адекватни на риска и съобразени със състоянието на техниката, разходите за внедряване, естеството, обхвата и целите на обработването. Практическият резултат е изискване за систематични процеси: оценка на риска, избор на контролни механизми, тестване, мониторинг, обучение, управление на инциденти и непрекъснато подобрение.

При високорискови обработки (каквито са мащабните системи за електронно здравеопазване, централизирани платформи, телемедицински услуги, аналитични решения с профилиране) се прилага оценка на въздействието върху защитата на данните – чрез използването на метод за идентифициране на заплахи и за валидиране на мерките още преди стартиране на обработването.

Националната нормативна среда в България конкретизира и допълва европейската рамка чрез Закона за защита на личните данни и секторните актове в здравеопазването, които определят статута на здравната информация, медицинската документация и режима на достъп. Националните правила въвеждат специфични изисквания по отношение на медицинската тайна, ограничаването на достъпа до здравна документация само за лица с правно основание и професионална необходимост, както и регламентация на обмена на данни в рамките на публични системи и регистри. В практиката това означава, че лечебните заведения и администраторите на здравни данни не могат да разчитат единствено на общи политики, а следва да изграждат процеси, съобразени със сектора – правила за водене, съхранение и предоставяне на медицинска документация; протоколи за предоставяне на информация на пациента и на оправомощени трети лица; механизми за удостоверяване на самоличност и правомощия при достъп; както и ясни вътрешни процедури за работа с искания на субектите на данни (достъп, копие, корекция, ограничаване), при съобразяване със специфичните ограничения и изключения, приложими в здравната сфера.

Съществен елемент на „цялостната картина“ е взаимодействието между режима за защита на личните данни и правото на киберсигурност. Здравеопазването е сектор, в който инцидентите засягат едновременно поверителността (изтичане на информация в относима към хода на лечебно-диагностичния процес; лабораторни резултати), цялостността (неоторизирани промени в записи) и наличността (спиране на болнични системи, блокирани лаборатории). Това налага прилагане на изискванията на националното законодателство свързано с киберсигурност и на европейските тенденции за засилване на устойчивостта на критичните и важните субекти, като се гарантира съгласуваност с GDPR. В юридически аспект това е важно поради различните цели на режимите, като GDPR защитава правата на лицата и законността на обработването, докато киберсигурността акцентира върху управлението на риска за мрежите и информационните системи и непрекъснатостта на услугите.

- **Основни роли и отговорност в екосистемата на здравните данни**

В екосистемата на здравните данни ролите и отговорностите не се изчерпват с техническото администриране на информационни системи, а представляват нормативно определена архитектура на задължения, в която се пресичат основни права на пациента, професионалната медицинска тайна, управлението на риска за киберсигурност и многостепенна отговорност за доказуемо съответствие. Здравната информация по българското право е изрично разпозната като лични данни, свързани със здравословното състояние и съдържащи се в медицинска документация, за които се прилагат специални правила за достъп и предоставяне. Тази национална дефиниция и режим се наслагват върху европейския стандарт за защита на личните данни, според който данните, свързани със здравето, са специална категория лични данни и обработването им е допустимо само при наличие на конкретни правни основания и гаранции, включително задължение за сигурност на обработването, съобразено с риска.

Ядрото на отговорността е при субекта, който определя целите и средствата на обработването на здравните данни. Това е администраторът на лични данни, който в здравния сектор най-често е лечебното заведение, медицинският център, лабораторията, държавен орган или публичен оператор на здравни регистри и системи. Отговорността на администратора е едновременно правна и организационна - да обоснове законосъобразността на всяка конкретна обработка, да осигури прозрачност към пациента, да гарантира упражняването на правата на субекта на данни и да може да докаже, че принципите на обработването са превърнати в реални контроли. Тук „доказ-

ването“ не е формалност, а ключова юридическа функция - регистри на дейности по обработване, политики, оценки на риска, протоколи за тестове, и документирани решения за срокове на съхранение трябва да позволят последваща проверка от надзорния орган и съдебен контрол. Европейската съдебна практика последователно затвърждава виждането, че при специалните категории данни е необходимо едновременно да е налице общо правно основание за обработване и отделно приложимо условие за обработване на специална категория данни; това е особено важно при цифрови здравни услуги, където често се смесват клинични и търговски цели. Показателно е делото на Съда на Европейския съюз по казус, свързан с онлайн продажба и маркетинг на лекарствени продукти, при което съдът приема, че определени операции по електронна търговия могат да водят до обработване на данни, разкриващи здравен статус, и подлежат на строгия режим за специалните категории данни, като не може да се разчита на „общо“ основание без специфично условие за тези данни.

Когато два или повече субекта съвместно определят целите и средствата на обработването, те имат статут на съвместни администратори на лични данни и следва прозрачно да разпределят отговорностите си. В здравния сектор това възниква обикновено при интеграции между болнична информационна система и национални платформи, при общи регистри, при консорциуми за телемедицина или при споделени платформи за образна диагностика. Правният риск тук е структурен - ако разпределението на отговорности остане само „договорно“, без да е отразено в реални процеси, пациентът не получава ефективен адресат за правата си, а организацията не може да демонстрира отчетност при инцидент. Практическият стандарт е разпределението да отговаря на действителния контрол върху данните.

Следващата ключова фигура е обработващият лични данни. Това е субектът, който обработва здравни данни по документирани инструкции на администратора: доставчик на облачна инфраструктура, интегратор на софтуер, външна архивна услуга, лабораторен модул, платформа за дистанционни консултации. Нормативно обработващият е длъжен да прилага подходящи мерки за сигурност, да обработва данните само по инструкции и да подпомага администратора при изпълнение на задълженията му, включително при инциденти и при искания на субектите на данни. В здравен контекст, юридическата специфика е, че обработващият много често има фактически контрол върху средата, където се съхраняват и пренасят данни, което означава, че договорната рамка трябва да бъде „инженерно конкретна“ - изисквания за криптиране, управление на ключове, резервни копия, тестове за възстановяване, ограничения за подизпълнители и ясни срокове за уведомяване при инцидент. Тъй като рискът при здравни данни включва не само поверителност, но и наличност на системите, договорите следва да изискват измерими показатели за устойчивост и възстановяване, както и доказуеми процедури за изследване и запазване на следи.

Длъжностното лице по защита на данните има роля на вътрешен независим механизъм за съответствие, но не е „носител“ на отговорността вместо администратора. В здравните организации длъжностното лице по защита на данните изпълнява критична функция свързана с дизайн на процесите – оценява дали целите са легитимни, дали има минимизация и ограничение на достъпа, дали са определени срокове за съхранение и дали проектите на цифровизация отговарят на изискванията за защита на данните още при проектирането и по подразбиране. Практически ефективният модел е длъжностното лице по защита на данните да работи съвместно с отговорника по информационна сигурност и с медицинското ръководство, така че клиничната необходимост да бъде превърната в правилно дефинирани роли на достъп, а юридическата отчетност да бъде подплатена с технически доказателства.

Отговорникът по информационна сигурност и екипите по сигурността са функционалните носители на мерките, но техните задачи имат пряко юридическо значение. Европейската правна рамка за сигурност на обработването изисква „подходящо ниво на сигурност“, определено чрез оценка на риска, и включващо мерки като анонимизиране и криптиране, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите, и процес за редовно тестване и оценяване на ефективността на мерките. За здравните данни това означава, че информационната сигурност трябва да бъде организирана като система за управление.

- **Практика по прилагане на мерки за информационна сигурност и защита на здравна информация**

Съдебната практика на Европейския съд по правата на човека дава особено силна теоретична и практическа рамка за ролите и отговорностите, защото разглежда защитата на медицинските данни като елемент от правото на личен и семеен живот и възлага позитивни задължения на държавата да осигури реална защита. В дело срещу Финландия от 2008 година Европейският съд по правата на човека приема, че защитата на медицинските данни е фундаментална и че не е достатъчно да има законови правила. Необходими са ефективни практически мерки за информационна сигурност и контрол на достъпа, включително предотвратяване на неоторизиран „вътрешен“ достъп в лечебни системи. Това решение е основополагащо, защото превръща сигурността от технически избор в правно изискване, а липсата на адекватни контролни механизми може да доведе до нарушение на правото на личен живот. В друго дело срещу Финландия от 1997 година съдът развива и принципа на баланса: конфиденциалността на медицинската информация е изключително защитена, но в определени ситуации може да бъде ограничена при наличие на законова основа, легитимна цел и пропорционални гаранции, например в контекста на наказателно преследване, при което се изисква внимателно претегляне и ограничаване на разкриването до необходимото. Тези решения имат пряко отражение върху националните роли - когато държавни органи или публични системи обработват здравни данни, те носят засилено задължение да изградят контролни механизми, които реално предотвратяват злоупотреби, а не само да предвидят санкции „след факта“.

В българския контекст надзорът по защита на личните данни се осъществява от Комисията за защита на личните данни, която разглежда жалби, извършва проверки, издава задължителни предписания и налага санкции. Практиката на комисията в областта на здравните данни показва два устойчиви акцента. На първо място, че неправомерното разкриване или предоставяне на здравна информация без правно основание е нарушение, независимо дали е извършено от лечебно заведение или от конкретен медицински специалист. На второ място, че контролът на достъпа и доказуемостта на обработването са централни критерии при оценка на съответствието. Решенията на комисията подлежат на съдебен контрол по административен ред и се формира съдебна практика, която доизяснява границите на правото на достъп до медицинска документация и правилата за предоставяне след смърт на пациента. Показателен е акт на Върховния административен съд от 2008 година, отразен в публичния регистър на комисията, в който съдът приема за законосъобразно предоставянето на достъп до поискана медицинска документация след смъртта на пациента при наличие на правно релевантен интерес и спазване на приложимия ред, което подчертава ролята на администратора да извърши правна преценка и да документира основанията за предоставяне. Националната правна рамка за достъп на пациента до медицинска до-

кументация и възможността за упълномощаване на друго лице, както и условията за предоставяне на здравна информация, са предмет и на тълкувателни позиции и становища на Комисията за защита на личните данни, които в практиката служат като ориентир за лечебните заведения при изграждане на процедури.

Наред с режима за защита на личните данни, екосистемата на здравните данни включва роли и отговорности по киберсигурност, които стават все по-правно значими поради пряката връзка между киберинцидентите и непрекъснатостта на медицинските услуги. На равнище Европейски съюз, Директивата относно мерки за високо общо ниво на киберсигурност въвежда риск-базиран подход и засилена управленска отговорност за определени категории организации, сред които попадат и здравни субекти. В България компетентните структури по режима за сигурност на мрежите и информационните системи включват Държавната агенция „Електронно управление“ като единна точка за контакт по европейската политика за киберсигурност, а националното законодателство урежда задължения за управление на риска, докладване на инциденти и организационни мерки. Европейската комисия официално е отразила статуса на транспониране на тази директива и ролята на Държавната агенция „Електронно управление“ като единна точка за контакт, което е важно за практиката при координация на инциденти, които засягат болници и национални здравни системи.

Отговорността на ръководството на здравната организация е обединяващ елемент между защитата на личните данни и киберсигурността. Ръководството носи задължение да осигури ресурси, да утвърди политики, да въведе контролна среда и да гарантира, че клиничните процеси имат „режим при отказ“, така че при атака или срив да се запази безопасността на пациента. Това е практическото проявление на принципа за наличност и устойчивост – в болничните условия прекъсването на достъп до лабораторни резултати, образна диагностика или лекарствени схеми не е само информационен инцидент, а риск за здравето. Следователно юридическата отговорност на администратора на лични данни и управленската отговорност по киберсигурност се обединяват под едно и също изискване: да се управлява рискът, да се предотвратяват инциденти и да се реагира ефективно, включително чрез вътрешни процедури за откриване, ограничаване, възстановяване и уведомяване.

Надзорните органи и съдилищата изпълняват ролята на външен гарант и коректив. Комисията за защита на личните данни осъществява административен надзор, а административните съдилища и Върховният административен съд осигуряват съдебен контрол върху решенията, като формират стандарти за пропорционалност, законосъобразност на предоставянето на медицинска документация и задължението за мотивирана преценка при конкуриращи се права. Европейският съд по правата на човека допълва рамката чрез доктрината за положителните задължения за защита на медицинските данни и изискването мерките да бъдат ефективни на практика, а не само на хартия. Съдът на Европейския съюз задава тълкуване на европейското право, включително относно квалифицирането на определени данни като здравни и изискването за кумулативни предпоставки за законосъобразно обработване на специални категории данни, което има пряко отражение върху цифровата търговия и платформените модели в здравния сектор.

Практически устойчивата организация на ролите и отговорностите в здравните данни изисква съгласуван модел на управление, при който правните роли се превръщат в технически и процедурни реалности. В този смисъл екосистемата на здравните данни е правно-техническа система на доверие – всяка роля има ясно определени компетентности и отговорности, но ефектът за пациента възниква само когато тези

отговорности са превърнати в конкретни контролни механизми, които предотвратяват неправомерен достъп, ограничават вредите при инцидент и гарантират непрекъснатост на медицинската грижа.

- **Заключение**

Гарантирането на сигурността на здравната информация е системен процес, основан на отчетност, пропорционалност и ефективност на мерките в реална среда. Особено важно е, че в здравеопазването сигурността има и функционално измерение: наличността и устойчивостта на системите са част от защитата на пациента, тъй като прекъсването на ключови информационни потоци може да компрометира терапевтични решения, безопасността на медикаментозната терапия и времето за реакция в спешни състояния. Затова управлението на ролите и отговорностите се утвърждава като ключов инструмент не само за нормативно съответствие, но и за качество и безопасност на медицинската грижа. Чрез него се осигурява минимизация на достъпа, ограничаване на вътрешни злоупотреби, контрол над външни доставчици, и устойчивост срещу киберинциденти. В този смисъл успехът на цифровизацията в здравния сектор зависи от способността на организациите да поддържат единна инфраструктура на доверие – пациентът да разполага с реални гаранции, че данните му се обработват законосъобразно и с необходимата степен на защита, а здравната организация да демонстрира, че сигурността е вградена в ежедневните процеси, измерва се, тества се и се подобрява непрекъснато.

Библиография:

1. Становище на Комисията за защита на личните данни (с рег. № П – 8919/2017 г.) – Становище на КЗЛД относно прилагането на чл. 28б от Закона за здравето
2. Решение на Върховния административен съд № 9702/25.09.2008 г., по адм. дело № 7202/2008.
3. European Court of Human Rights, Judgement of 25.02.1997 on Application no. 22009/93 – Case of Z. vs Finland
4. European Court of Human Rights, Judgement of 17.07.2008 on Application no. 20511/03 – Case of I. vs Finland
5. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, г., стр. 1–88
6. European Court Human Rights, Judgement of the court (Grand Chamber) – 4.10.2024, in Case C-21/23 - ND v DR.
7. Закон за здравето - Обн. ДВ. бр.70 от 10 Август 2004 г.
8. Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните), ОВ L 119, г., стр. 1—88
9. Манева, К. Концептуално-пораждащ модел за оценка на приноса към националната сигурност от чуждестранни икономически субекти в Република България: принципи и постулати., Юридически сборник. Международна научна конференция „100 години от рождението на чл.- кор. проф. д-р Александър Янков". Бургас: БСУ, 2024, Т. XXXI, С. 487- 494. ISSN 1311-3771.