ЗА ЕЛЕКТРОННИТЕ ЗДРАВНИ ЗАПИСИ В КОНТЕКСТА НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ

доц. д-р Галина Йолова
Икономически университет – Варна

FOR ELECTRONIC HEALTH RECORDS IN CONTEXT FOR PROTECTION ON PERSONAL DATA

Assoc. Prof. Galina Yolova, PhD
University of Economics - Varna, Bulgaria

Резюме: Разработката анализира същността и принципите при използване на електронните здравни записи в контекста на изискванията за защита на личните данни, установени в Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни, и предвид нуждата от адекватни механизми за тяхната поверителност с оглед охрана интересите и правата на пациентите и осигурените лица. Извежда се същността на електроните здравни записи като цифрови инструменти за съхраняване и споделяне на данни, изясняват се принципите за създаване, ползване, съхранение и споделяне на записите в контекста на принципите на защита на личните данни, както и се систематизират обобщения за нуждата от гарантиране на поверителност, адекватна и ефективна правна защита.

Ключови думи: *електронен здравен запис, защита на личните данни, принципи за защита на личните данни*

Abstract: The development analyzes the nature and principles of the use of electronic health records in the context of the data protection requirements set out in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data, personal data and on the free movement of such data, and given the need for adequate mechanisms for their confidentiality in order to protect the interests and rights of patients and insured persons. The essence of electronic health

records as digital tools for data storage and sharing is presented, the principles for creation, use, storage and sharing of records in the context of the principles of personal data protection are clarified, as well as summaries of the need to ensure confidentiality, adequate and effective legal protection.

***Key words:** electronic health record, personal data protection, principles of personal data protection*

DOI: <https://doi.org/10.36997/PPDD2021.76>

Въведение

Като важна част от инструментите на електронното здравеопазване електронните здравни записи са компонент от цялостната система на цифровизация на здравните услуги, предвидена като поетапно изграждане в Националната здравна стратегия 2014 – 2020, Програмата за развитие на електронното здравеопазване (2014), Пътната карта към програмата за развитие на електронното здравеопазване (2014), Националната здравна стратегия 2020 (Политика 2.6 „Развитие на електронно здравеопазване“). Базисни в тази система са понятията „електронно здравно досие“, „пациентски здравен запис“ (Electronic Patient Records – EPR), eGenomics, PACS (архивна система за образната диагностика), e-Health Portal, „е-рецепта“, „е – доставка“, „е-аптека“, „телемедицина“, „мобилно здравеопазване“ и др. (Йолова 2020).

От друга страна, те са свързани пряко и с процесите по надграждане и доразвитие на Националната здравноинформационна система, в аспектите на възможността за централизиран достъп до здравните услуги чрез Националния електронен здравен портал като част от e-Health инициативите на ЕС за болничната помощ и общо-практикуващите лекари.

В тези насоки **цел на разработката** е анализиране същността и принципите при използване на електронните здравни записи в контекста на изискванията на защита на личните данни, установени в Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и предвид нуждата от адекватни механизми за тяхната

поверителност с оглед охрана на интересите и правата на пациентите и осигурените лица. В изпълнение на целта са и следните изследователски задачи:

1. Анализиране същността на електронните здравни записи като цифрови инструменти за съхраняване и споделяне на данни.
2. Принципи за създаване, ползване, съхранение и споделяне на записите в контекста на принципите на защита на личните данни.
3. Извеждане на обобщения за гарантиране на поверителност и адекватна и ефективна правна защита.

За постигане на заложената цел и свързаните с нея изследователски задачи се използват индуктивен и дедуктивен подход, формално-юридически, нормативен и сравнителноправен анализ.

Докладът е съобразен с регламентацията на разглежданите отношения в законодателството на Р България и Европейския съюз (ЕС) към 30.09.2021 г.

Изложение

1. Същност и съдържание на електронните здравни записи като елемент на електронното здравеопазване

Инфраструктурата на здравните данни като общоевропейска политика е част от Европейската стратегия за данните (19 февруари 2020 г.), чрез която следва да се доразвият цифровите услуги и политики в европейските референтни мрежи и в частност – проектът „Геномика“. В тази връзка общото европейско пространство на здравни данни е приоритетна политика за периода 2019 г. – 2025 г., която е предвидено да се базира на стълбовете – стабилна система за управление на данните и правила за обмена на данни, качество на данните, стабилна инфраструктура и оперативна съвместимост, както и на принципите на прозрачност и защита в ползването и преносимостта на данните съгласно чл. 20 от Общия регламент относно защитата на данните. В тази връзка се очаква то да осигури качествен обмен и достъп до здравни данни и използването им с цел ефективно и качествено здравно обслужване, както и за целите на здравните изследвания, разработването на здравни политики и подкрепяне на иновациите в прилагането на общите здравни стратегии.

Електронният здравен запис (ЕЗЗ) като интернет базиран интерактивен запис е механизъм, чрез който съгласно чл. 28г., ал.3 от За-

кона за здравето (33) Националната здравноинформационна система събира, обработва и съхранява информация за здравното състояние на населението. В този смисъл като способ за улесняване обменът на медицинските документи и интегрирането им в множество доставчици, терминът „електронен здравен запис“ се прилага за интегриране на процесите на съхраняване на данни и едновременно с това – за осигуряване на достъп до електронния медицински регистър на пациента. Изграждането му е част от процесите по създаване на връзка между разработени към момента системи в различни организации в сферата на здравеопазването, в това число НЗОК, доброволни дружества, национални центрове и изпълнителни агенции и лечебни заведения. Целта на тази интеграция е обединяване на процесите в здравеопазването в единна система с възможност за обмен и контрол на информацията в реално време, включваща, освен електронен пациентски запис, още и електронна автентификация, регистри на основните участници в системата на здравеопазването и обвързаност между тях.

Съгласно дефиницията, дадена от Европейския съюз, ЕЗЗ е „изчерпателен медицински запис или проста документация на минало и настоящо физическо и умствено здравно състояние на индивида, в електронна форма, предоставящ лесен достъп до тази информация за медицинско лечение и други, свързани с това цели“. Като обединяваща система от първични медицински, здравни, персонални и административни данни за пациента е предвидено той да съдържа базисна и минимална систематика от данни в следните насоки:

- Данни на пациента – лични данни, данни за контакт, данни за здравно осигуряване (задължително и доброволно), антропометрични данни (ръст тегло, и др.).

- Лични и професионални данни за общопрактикуващите лекари, при които лицето е било или е записано – лични и професионални данни: имена, адреси, УИН, специалности, лечебни заведения, в които работят.

- Контакти при спешност (име, роднинска връзка, адрес, телефон).

- Кръвна група, резус фактор.

- HLA типизиране.

- Кръвопреливане и кръводаряване – на коя дата е имало кръвопреливане, с какъв кръвен продукт.

- Рискови фактори и рискови групи с описание на риска,
- Съгласие/несъгласие за донорство.
- Поставени до момента диагнози.
- Алергии.
- Имунизации, в това число дати на направени имунизации, търговско наименование на ваксината, количество и партидният номер на използваната ваксина.
- История на предписаните и отпуснати лекарствени продукти, медицински изделия и храни за специални медицински цели.
- Прегледи с информация за направени амбулаторни прегледи, която съдържа данните от амбулаторните листове.
- Назначени и изпълнени медико-диагностични дейности.
- Диспансеризация и хоспитализации.
- Фамилна обремененост и наследствени заболявания.
- Остри заразни заболявания, временна или трайна неработоспособност.

Очевидно е, че се касае за една сравнително широка систематика от записи в реално време, целяща всеобхватност на клиничния статут и медицинската история на лицето, създадена с цел незабавно доставяне на информация до оторизираните потребители. Като свързан с възможно най-точна и актуална информация за здравето и статуса на пациентите чрез него се цели осигуряване на бърз достъп в условията на координирано здравно обслужване, както и облекчаване на административната тежест при оказване на първична и вторична медицинска помощ, профилактика и превенция на заболяванията. Както се отбелязва в Националната здравна стратегия, по този начин се „дава възможност да се извършват онлайн повече административни и здравни услуги в сектора, осигурява се достъп до информация на пациента за собственото му здраве, подобряват се взаимовръзките между отделните нива на системата, подобрява се качеството на медицинските услуги и ефективността на разходването на публичните средства за здравеопазване“.

От друга страна обаче, повече от безспорно е, че правилното обработване и съхраняване на данните следва да е свързано с високи нива на сигурност на споделянето на медицинска информация, както и непрекъснато подобряване на сигурността и поверителността на данните за пациента.

2. Принципи при обработка и достъп на електронни здравни записи в контекста на защита на личните данни

Както вече се спомена, предвидено е европейското пространство на здравни данни да се базира на принципите за прозрачност и защита в ползването и преносимостта на данните, както и на основните стълбове – стабилна система за управление на данните и правила за обмена на данните, качество на данните, стабилна инфраструктура и оперативна съвместимост.

Съгласно Регламент (ЕС) 2016/679 личните данни за здравословното състояние на лицата следва да обхващат всички данни, свързани със здравословното състояние на субекта на данните, които разкриват информация за физическото или психическото му здравословно състояние в миналото, настоящето или бъдещето. В този смисъл обемът на събираната информация в хода на регистрацията за здравни услуги или тяхното предоставяне следва да се отнасят до характеристики, определени за дадено физическо лице с цел уникалното му идентифициране за здравни цели, информация, касаеща генетични данни и биологични проби, заболяване, увреждане, риск от заболяване, медицинска история, клинично лечение или физиологично или биомедицинско състояние на субекта на данните, независимо от източника на информация, в частност – лекар или друг медицински специалист, болница, медицинско изделие или инвитро диагностично изследване.

Общите принципи, свързани с обработването на лични данни, заложи в регламента са законосъобразно, добросъвестно и по прозрачен по отношение на субекта на данните начин обработване и събиране за конкретни, изрично указани и легитимни цели – *свеждане на данните до минимум*, точност и актуалност, съхраняване във форма, позволяваща идентифицирането на субекта на данните за период, не по-дълъг от необходимото за целите, за които се обработват личните данни, обработване по начин, който гарантира подходящо ниво на сигурност, включително защита срещу неразрешено или незаконосъобразно обработване и срещу случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически или организационни мерки (*цялостност и поверителност*). (Александров 2016; Александров 2017; Александров 2018; Александров 2020; Andreeva, Mateeva 2018).

При това в чл. 9, по повод обработване на специални категории

лични данни, в което число следва да се отнасят и данните, свързани със здравния статус на лицата, е изрично предвидена забраната за обработването на генетични данни, биометрични данни за целите единствено на идентифицирането на физическото лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

Забраната не се прилага при алтернативност на условията – обработването да е необходимо за целите на превантивната или трудова медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, за целите на управлението на услугите и системите за здравеопазване или социални грижи въз основа на правото на Съюза, правото на държава членка или договор с медицинско лице. От друга страна, дерогиране на забраната е допустима, в случай че обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, осигуряването на високи стандарти за качество и безопасност на здравните грижи, лекарствените продукти или медицинските изделия, но при едновременно и навременно прилагани подходящи мерки за гарантиране на правата и свободите на субекта на данните и, по-специално, опазването на професионална тайна.

В чл. 32 на регламента са и предвидените мерки за сигурност при обработването на данните, съгласно който, като се имат предвид достиженията на техническия прогрес, разходите за прилагане и естеството, обхватът, контекстът и целите на обработването, както и рисковете с различна вероятност и тежест за правата и свободите на физическите лица, администраторът и обработващият лични данни следва да прилагат подходящи мерки за осигуряване на съобразено с този риск ниво на сигурност, в частност – псевдонимизация и криптиране на личните данни, способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване, способност за своевременно възстановяване на наличността и достъпа до личните данни в случай на физически или технически инцидент, процес на редовно изпитване, преценяване и оценка на ефективността на техническите и организационните мерки с оглед да се гарантира сигурността на обработването.

При това, при оценката на подходящото ниво на сигурност, се вземат предвид по-специално рисковете от случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или

достъп до прехвърлени, съхранявани или обработени по друг начин лични данни.

На национално ниво стабилитетът и законосъобразността при ползване на данни от здравните записи се гарантират, от една страна, от общите рамки за функциониране на Националната здравноинформационна система, която съгласно чл. 28г ЗЗ следва да се основава на принципите – гарантиране на актуалност и точност на предоставените и съхраняваните данни, осигуряване на подходяща среда за обмен на данни, гарантиране на регламентиран достъп, осигуряване на оперативна съвместимост и информационна сигурност.

От друга страна и в конкретика, защитата на данните по здравни записи следва да се гарантира и от правилата и механизмите за достъп. Така съгласно чл. 28д, ал.1 ЗЗ право на безвъзмезден достъп до Националната здравноинформационна система, в това число и до електронните здравни записи, имат гражданите – до информацията в неговия електронен здравен запис, лечебните и здравните заведения и Националната здравноосигурителна каса при и по повод осъществяване на функциите си, застрахователните дружества, лицензирани по отделни видове медицински застраховки, както и държавни органи, за които в закона е предвиден достъп до регистри с национално значение.

Предоставянето на достъп до информацията в електронния здравен запис на гражданите и на лечебните и здравните заведения, на Националната здравноосигурителна каса, застрахователните дружества и държавните органи се извършва само след изрично писмено съгласие при условия и по ред, определени с наредба на министъра на здравеопазването. (Андреева, Йолова 2020).

В технологичен порядък е предвидено пациентите да могат получават достъп до порталния интерфейс след регистрация, като използват квалифициран електронен подпис за идентификация – КЕП или до националната система за електронна идентификация, но само относно записите за тях или за лицата, на които са родители, настойници или попечители. Медицинските специалисти от своя страна трябва да достъпват системата и здравната информация след предварителна регистрация, като се идентифицират с електронен подпис, като прегледът на здравната информация следва да се осъществява след изрично съгласие от пациента. Във всички случаи достъпът до здравната информация трябва да се управлява от пациента и, като ми-

нимум, да се дефинират конкретният медицински специалист, който да достъпва здравната информация, конкретната здравна информация в досието на пациента, за която се дава съгласие за достъп, както и периодът от време за достъп до данни. Всеки достъп до данните следва да се регистрира в контролната част на портала.

Заклучение

Цифровизацията на здравните услуги и нейното качествено и в интерес на всички участници изграждане безспорно предполага такива механизми и средства, които взети в своята систематика, следва да допринесат за едно ново и качествено по-добро ниво на здравна грижа (Андреева, Йолова 2021). Същевременно обаче прилагането и развитието ѝ в практиките на здравните системи следва да е функционално на адекватни нива на гарантиране правата, достойнството и личното пространство на индивида чрез висока степен – и законодателна, и технологична, на защита при обработването, съхраняването и запазване поверителността на личните данни.

Досега установените – и европейски, и на национално ниво разпоредби и законови механизми очертават една добра нормативна рамка, въпреки че електронните здравни записи съдържат в максималната възможна степен чувствителна лична информация, на чието обработване следва да отговаря значително по-висок праг за законосъобразност при съхраняването, ползването и обmena. От друга страна, предизвикателства пред нормативната рамка и адекватното ѝ приложение са недобрата технологична готовност, слабото ниво на защита на програмните продукти, недобрата координираност в отделните сегменти на електронното здравеопазване, създаващи реални заплахи както за злоупотреба с данни или неправомерното им разпространяването, така и за кибератаки и здравен тероризъм.

Използвана литература

Andreeva, A., Z. Mateeva. Employers as Personal Data Administrators – Specifics and Requirements in the Context of the Information Society. // Globalization, the State and the Individual, 2018, Vol.2, №18, pp. 139 – 147.

Александров, А. (2016). Защита на личните данни на работници-

те и служителите. София: Труд и право.

Александров, А. (2017). Новият Общ регламент за защита на личните данни в ЕС и какво трябва да знаят работодателите за него. София: Труд и право, с. 1 – 28.

Александров, А. (2018). Общият регламент за защита на личните данни в ЕС: нови изисквания и предизвикателства за работодателите. // Сборник доклади от Юбилейна международна научна конференция на тема „Ролята и значението на международното и наднационалното право в съвременния свят. София: УНСС, с. 202 –217.

Александров, А. (2020). Защо вътрешното ни законодателство по защита на личните данни (отново) не покрива изискванията на правото на ЕС. Сборник доклади от научна конференция на тема „Традиция и развитие на законодателството в сферата на икономиката. София: ИК УНСС, с. 33 – 43).

Андреева, А., Г. Йолова. Изграждане на Националната здравно-информационна система – тенденции и правна рамка. // Медицински мениджмънт и здравна политика. 2020, том 51, №1, с. 27 – 51.

Андреева, А., Г. Йолова (2021). Цифровата трансформация в здравеопазването в контекста на правото на достъп до медицинска помощ. // Медицинско право и здравеопазване, 2021, №1, 20 – 37.

Йолова, Г. (2020). Еволюция на правната рамка за развитие на електронното здравеопазване. // Правото и бизнесът в съвременното общество. Сборник с доклади от 3-та Национална научна конференция. Варна: Наука и икономика, с. 324 – 329.

Национална здравна стратегия 2020, с. 90, (https://www.mh.government.bg/media/filer_public/2016/09/12/nzs_2020.pdf)

Health informatics — Electronic health record — Definition, scope, and context, ISO TC 215, ISO/TR 20514, ISO TC 215/WG 1, 2005-01-22.

Министерство на здравеопазването – Техническо задание по обособена позиция № 4 „избор на изпълнител на дейност 9 – Изграждане на единно национално електронно медицинско досие/ електронен здравен запис“ – приложение № 4, (https://www.mh.government.bg/media/filer_public/2018/08/28/tekhnicheskoe_zadanie_po_obosobena_pozitsiia_4-prilozhenie_4.pdf).

За контакти: доц. д-р Галина Йолова
Икономически университет – Варна
e-mail: ina_yolova@ue-varna.bg