АСПЕКТИ НА ЗАЩИТАТА НА ЛИЧНИТЕ ДАННИ ПРИ ОБРАБОТКА НА КАРДИОЛОГИЧНИ ДАННИ

Росен Радков[1], Йото Йотов[2]

[1]Катедра „Компютърни науки и технологии“, Техничеки университет - Варна

[2]УС Кардиология, Катедра „Вътрешни болести“, Факултет Медицина, МУ-Варна

РЕЗЮМЕ

Сърдечната недостатъчност като крайна фаза на всички сърдечни заболявания е проблем, за решаването на който е необходимо лекарят да притежава голям обем информация, свързана със състоянието на пациентите. Процесите на консултации, диагностика и лечение са свързани с обработка на специални категории лични данни, която трябва да бъде приведена в съответствие с общия регламент относно защитата на данните на физическите лица, приет на 4 май 2016г и влизащ в сила от 25 Май 2018г. В доклада се изясняват задължителните изисквания, които е необходимо да бъдат изпълнени, и се дават препоръки за приложимите организационни и технически мерки за постигане на съответствие с регламента.

Ключови думи: лични данни, конфиденциалност, достъпност, цялостност

ВЪВЕДЕНИЕ

На 4 Май 2016г в официалния вестник на Европейския съюз беше публикуван регламент 2016/679, приет на 27 април същата година от Европейския парламент и наречен „Общ регламент относно защитата на данните” – ОРЗД (1), който се отнася до защитата на физическите лица във връзка с обработването на лични данни (ЛД) и свободното движение на такива данни. Регламентът влиза в сила на 25 май 2018 г. и отменя всички досега съществуващи наредби и регламенти, поставяйки редица нови изисквания към администраторите и обработващите лични данни.

Една от основните цели на новия регламент е създаване на единна законова уредба и уеднаквяване на изискванията по отношения на защитата на личните данни на физическите лица във всички страни членки на Европейския съюз. Разширено е определението за лични данни, като според него под лични данни се има предвид всяка информация, отнасяща се до физическо лице, кое-

ASPECTS OF PERSONAL DATA PROTECTION IN HANDLING CARDIAC DATA

Rosen Radkov[1], Yoto Yotov[2]

[1]Department of Computer Science and Engineering, Technical University of Varna

[2]Educational Sector of Cardiology, Department of Internal Diseases, Faculty of Medicine, Medical University of Varna

ABSTRACT

Heart failure as an end stage of all heart cardiovascular diseases is a problem for which a physician needs to have a large amount of information related to the condition of patients. Consultation, diagnosis and treatment processes are related to the processing of special categories of personal data, which must be brought into line with the General Data Protection Regulation of Natural Persons adopted on May 4, 2016 and in force since May 25, 2018. The report clarifies the mandatory requirements that need to be met and provides recommendations on the applicable organizational and technical measures to comply with the Regulation.

Keywords: personal data, confidentiality, availability, integrity

INTRODUCTION

On May 4, 2016, Regulation 2016/679, adopted on April 27, 2006 by the European Parliament, and called the General Data Protection Regulation - GDPR (1) concerning the protection of natural persons in relation to the processing of personal data (PD) and the free movement of such data. The Regulation will be entered into force on May 25, 2018 and repeal all existing ordinances and regulations setting a number of new requirements for data controllers and processors.

One of the main objectives of the new regulation is to establish a uniform legal framework and to align the data protection requirements of natural persons in all the member states of the European Union. The definition of personal data has been expanded and, in its view, personal data refers to any information relating to an individual who is identified or can be identified. Definitions are given in it on what health, genetic and biometric data are. Another goal is to ensure the free transfer of personal data between personal data con-

то е идентифицирано или може да бъде идентифицирано. В него се дават дефиниции и затова какво са данни за здравословното състояние, генетични и биометрични данни. Друга цел е осигуряване на възможността за свободен трансфер на личните данни между администраторите на лични данни (АЛД).

АЛД и обработващите лични данни (ОЛД) на физически лица трябва да се ръководят от следните принципи за обработка на ЛД:

- Законосъобразност, добросъвестност и прозрачност. Това означава, че обработка на данни трябва да се извършва в съответствие с правно задължение, наложено на АЛД, а ако няма такова, единствено ако се защитава живота на субекта на данните (СД) или се обслужва обществен интерес. Принципите на добросъвестно и прозрачно обработване изискват СД да бъде информиран за съществуването на операцията по обработване и за нейните цели;
- Ограничение на целите, което означава, че личните данни могат да се използват само за конкретни, легитимни и предварително указани цели;
- Свеждане на данните до минимум, т.е. да са подходящи и ограничени до необходимото за целите време;
- Точност - изискване да бъдат винаги актуални;
- Ограничение на съхранението, т.е. не повече отколкото е необходимо;
- Цялостност и поверителност. Изисква се осигуряване на защита срещу неоторизирани промяна или обработване, както и срещу загуба, унищожаване или повреждане.

При липсва на посочените по-горе основания за обработка на ЛД, такава може да се извършва единствено след получаване на изрично съгласие от СД. В ОРЗД стриктно са описани начините, по които трябва да бъде взето/дадено/оттеглено съгласието на субекта. Въведени са и нови права, които субекта може да упражнява, като „правото да бъдеш забравен“ и „правото за коригиране на данните“.

Когато организациите обработват лични данни, надхвърлящи определени по обем размери, за тях се въвежда задължението да имат „длъжностно лице по защита на данните“ (ДЛЗД). Това лице има задължения свързани с контрола на правилното изпълнение на процедурите, свързани с обработка на лични данни и даване на препоръки за тяхното подобряване. То е контактна точка с

trollers (PDCs).

PDCs and personal data processors (PDPs) of individuals should be guided by the following principles for processing PD:

- Lawfulness, fairness and transparency. This means that data processing must be done in accordance with a legal obligation imposed on the data controller, and if there is no existing one, exclusively for protection of the data subject‘s life or if the public interest is served. The principles of fairness and transparent processing require the data subject (DS) to be informed about the existence of the processing operation and its purposes;
- Goal limitation, which means that personal data can only be used for specific, legitimate and prespecified purposes;
- Data minimization, that is, it must be appropriate and limited to the time required for the purpose;
- Accuracy - a requirement to always be up to date;
- Storage limitation, i.e. no more than necessary;
- Integrity and confidentiality. Protection against unauthorized alteration or processing, as well as against loss, destruction or damage is required.

In the absence of the above-mentioned grounds for processing a PD, such may be conducted only after obtaining the explicit consent of the DS. GDPR describes strictly the ways in which the consent of the subject should be obtained/withdrawn. New rights that the subject can exercise, such as the „right to be forgotten“ and the „right to correct data“ have been introduced.

When organizations process personal data that exceeds specific volume, they are subject to the obligation to have a data protection officer (DPO). This person has duties related to the control of the proper execution of the procedures linked to the processing of personal data and recommendations for their improvement. It is a contact point with the regulator and has the obligation to report open incidents related to PD processing within a maximum of 72 hours.

The processes related to the diagnosis and treatment of patients with heart disease and the work of researchers working in this field are related to personal data processing. This report aims to indicate what organizational and technical measures can be put in place to process cardiac data in accordance with the GDPR.

регулатора и има задължение да му докладва за открити инциденти във връзка с обработката на ЛД в срок от максимум 72 часа.

Процесите, свързани с диагностиката и лечението на пациенти със сърдечни заболявания, и работата на учените, работещи в тази насока, са свързани с обработка на ЛД. Този доклад има за цел да посочи какви организационни и технически мерки могат да бъдат въведени, за да бъде обработката на кардиологични данни в съответствие с ОРЗД.

ДЕФИНИРАНЕ НА ПРОБЛЕМА

Както е посочено в (2), сърдечната недостатъчност (СН) е крайна фаза на всички сърдечни заболявания и главна причина за заболеваемост и смъртност. Обществената значимост на СН провокира стремежа непрекъснато да се търсят начини за справяне с този проблем и намаляване на лавинообразно нарастващите хоспитализации. В съществуващите специализирани амбулаторни клиники или кабинети за проследяване и наблюдение на болни със сърдечна недостатъчност се обработват следните данни за пациенти със сърдечна недостатъчност:

- Демографски: пол, възраст, населено място (село град, голям град), образование, заетост (пенсионер по болест или по възраст).
- Данни за заболяването: причина (исхемична болест на сърцето, клапни пороци, хипертония, вродени сърдечни пороци), давност (от колко време), функционален клас по класификацията на Нюйорската кардиологична асоциация (New York Heart Association, NYHA)
- Придружаващи заболявания: хронична обструктивна белодробна болест, захарен диабет, анемия, хипертония, бъбречна недостатъчност, заболявания на щитовидната жлеза и др.
- Клиничен преглед: изходни данни за допълнителни сърдечни тонове, шумове, сърдечна честота, артериално налягане, отоци, телесно тегло и др.; също в хода на наблюдението, ако има промяна
- ЕКГ: изходни данни и след това – ритъм, СЧ, наличие на блокове и т.н., Към този раздел – данни от Холтер ЕКГ мониториране (24-48ч.), ако е необходимо.
- Ехокардиография: данни за сърдечни размери, функция на лява камера (Фракция на изтласкване), параметри на диастолно пъл-

PROBLEM DEFINITION

As noted in (2), heart failure (HF) is an end stage of all heart disease and a major cause of morbidity and mortality. The social significance of HF provokes the constant seeking of ways to address this problem and reducing the avalanche of growing hospitalizations. In existing specialized outpatient clinics or offices for follow-up and monitoring of patients with heart failure, the following data are processed for those patients:

- Demographic: gender, age, place of residence (village, town, city), education, occupation (retired due to an illness or age).
- Disease information: cause (ischemic heart disease, valvular defects, hypertension, congenital heart defects), duration (how long), functional class by the New York Heart Association (NYHA) classification.
- Concomitant diseases: chronic obstructive pulmonary disease, diabetes mellitus, anemia, hypertension, kidney failure, thyroid diseases, etc.
- Clinical examination: initial data about additional heart sounds, bruit, heart rate (HR), blood pressure, edema, body weight, etc.; as well as during the follow-up process, if there is any change.
- EKG: initial and subsequent data – rhythm, HR, presence of blocks, etc. To this section belong as well: data from Holter heart monitor (24-48 hrs), if necessary.
- Echocardiogram: data for heart dimensions, left ventricular function (ejection fraction), parameters of the diastolic filling of the left ventricle, presence of stenosis or regurgitations, etc. All this is entered initially and during the follow-up process.
- Laboratory tests: blood count, blood sugar, creatinine, eGFR, ionogram, liver function, uric acid, iron and total iron-binding capacity, etc. (as needed). Initially and during the follow-up process.
- Quality of life: a 6-minute test involving walking, quality of life questionnaires – initially and during the follow-up process.
- Therapy: medicament types: dosage, dosage changes; surgical therapy – date and type of the operation; application of devices – pacemakers, cardiac resynchronization devices, implantable cardioverter defibrillator. For the latter – data from records initially and during follow-up, 24/7, if possible.
- Hospitalizations (hospital admissions): when, with what diagnosis, what kind of therapy (if

нене на лява камера, наличие на стенози или регургитации, и др. Всичко това се въвежда изходно и в хода на проследяването.
- Лабораторни изследвания: Кръвна картина, кръвна глюкоза, креатинин, eGFR, йонограма, чернодробни, пикочна киселина, желязо и параметри на желязна обмяна и др. (по преценка). Изходно и в хода на наблюдение.
- Качество на живот: 6-минутен тест с ходене, въпросници за качество на живот – изходно и при проследяване.
- Лечение: вид медикаменти: дози, промяна в дозата; оперативно лечение – дата и вид на операция; приложение на дивайси – пейсмейкъри, устройства за ресинхронизиращо лечение, имплантируеми кардиовертер-дефибрилатори, За последните – данни от записи изходно и при проследяване, по възможност да са 24-часа, 7 дни в седмицата.
- Хоспитализации (приемания в болница): кога, с каква диагноза, какво лечение (ако е известно).

Посочените по-горе данни спадат към т.нар. специални категории лични данни, които в сферата на общественото здраве се обработват без необходимост от съгласие на субекта, но трябва да бъдат обработвани съгласно принципите, които ОРЗД въвежда. Тези данни са необходими и за научни цели с крайна цел подобряване на начина на живот на хората.

В различните структури (болници, клиники, кабинети), където се извършват медицински консултации, прегледи и лечение на хора, се прилагат различни начини за обработка на тези данни. По принцип, според тълкуване на МЗ, лекарите са АЛД поради естеството на работата си. В кабинетите на личните лекари, както и в специализираните кардиологични кабинети, данните се обработват и съхраняват в програмни продукти на локален компютър. Обичайно тези компютри нямат адекватно системно програмно администриране, което означава, че е налице потенциална уязвимост, а това е предпоставка за изтичане и загуба на ЛД и несъответствие с изискванията на ОРЗД.

В университетските и специализирани клиники, в които обикновено работят по-голям брой лекари специалисти, се използват програмни системи, обединяващи данните, генерирани при прегледите извършени от различни специалисти и различни изследвания, напр. лабораторни, резултати от образна диагностика и др. Има примери, когато се използват и системи, осигуряващи поверителност на лявата камера, наличие на стенози или регургитации, и др. Всичко това се въвежда изходно и в хода на проследяването.
- Лабораторни изследвания: Кръвна картина, кръвна глюкоза, креатинин, eGFR, йонограма, чернодробни, пикочна киселина, желязо и параметри на желязна обмяна и др. (по преценка). Изходно и в хода на наблюдение.
- Качество на живот: 6-минутен тест с ходене, въпросници за качество на живот – изходно и при проследяване.
- Лечение: вид медикаменти: дози, промяна в дозата; оперативно лечение – дата и вид на операция; приложение на дивайси – пейсмейкъри, устройства за ресинхронизиращо лечение, имплантируеми кардиовертер-дефибрилатори, За последните – данни от записи изходно и при проследяване, по възможност да са 24-часа, 7 дни в седмицата.
- Хоспитализации (приемания в болница): кога, с каква диагноза, какво лечение (ако е известно).

The foregoing data are among the so-called special categories of personal data that are processed in the public health field without the consent of the subject but must be processed in accordance with the principles that the GDPR introduces. These data are also needed for scientific purposes with the ultimate goal of improving people‘s lifestyles.

The different structures (hospitals, clinics, offices) where medical consultations, examinations and treatment of people are carried out, have different ways of processing these data. In principle, according to the interpretation of Ministry of Health (MH), doctors are DPAs due to the nature of their work. In the offices of GPs, as well as in specialized cardiology offices, the data is processed and stored using software on a local computer. Typically, these computers do not have adequate system administration, meaning that there is a potential vulnerability, and this is a prerequisite for a leakage and loss of PD, and a noncompliance with GDPR requirements.

In university and specialized clinics, where a larger number of physicians are usually employed, software systems are used that combine the data generated by the examinations carried out by different specialists and various studies, laboratory, results of imaging diagnostics and others. There are examples when using application systems that ensure patient privacy. It is good that, given the greater complexity of IT infrastructures (ITIS) used, systematic program administration is entrusted to professional IT staff. However, due to lack or misallocation of financial resources and/or insufficient competence of IT service staff and/or other reasons, there are cases of unreliable ITIS.

The reporting of the procedures performed to the National Health Insurance Fund (NHIF) requires electronic data exchange, which is also a potential threat to PD.

Besides the data in electronic form, a large amount of information is to be kept in paper form, both as originals and as reports, etc. The processing of these documents is linked to the need for transfer between different units, as well as to storage, which is not always sufficiently protected. It is also a problem to transmit personal documents to patients or their relatives.

The analysis of the way of PD processing and their alignment with the principles laid down in the GDPR leads to a number of issues and problems:
- Are the ITIS-related measures in place to ensure the integrity and confidentiality of the data currently in use?

ността на ЛД за пациентите. Добре е, че предвид по-голямата сложност на използваните ИТ инфраструктури (ИТИС), системното програмно администриране е поверено на професионален ИТ персонал. Но въпреки това, поради липса или неправилно разпределение на финансовите средства и/или недостатъчна компетентност на обслужващия ИТ персонал и/или други причини, се наблюдават случаи на ненадеждни ИТИС.

Отчитането на извършените процедури към Националната здравно осигурителна каса (НЗОК) изисква обмен на данни по електронен път, което също представлява потенциална опасност за ЛД.

Освен данните в електронен вид, задължително се поддържа и голям обем информация в хартиен вид, както като оригинали, така и като отчети и др. Обработката на тези документи е свързано с необходимост от пренасяне между различните звена, както и съхранение, което невинаги е достатъчно защитено. Проблем е и предаването на документи с лични данни на пациентите или на техните близки.

Анализът на начина на обработка на ЛД и съпоставянето им с принципите заложени в ОРЗД поставя множество въпроси и проблеми:

- Приложени ли са в използваните в момента ИТИС адекватни на ОРЗД мерки за осигуряване на цялостността и поверителността на данните?
- Взети ли са необходимите мерки за защита на данните срещу новите предизвикателства, като крипто вирусите, появяващи се всяка секунда и как се адаптират срещу тях?
- Притежава ли персонала, участващ в обработката на ЛД, необходимото ниво на осъзнатост и компетентност?
- Необходимо ли е да се вземат някакви допълнителни мерки за постигане на съответствие с ОРЗД?

ПРЕДЛАГАНО РЕШЕНИЕ

След извършване на подробен анализ на клаузите на ОРЗД (1) са определени задължителните мерки, които трябва да бъдат предприети. Те са представени по-долу заедно с предложения за приложими мерки за реализацията им.

Чл.25 от ОРЗД изисква да бъде осъществена „Защита на данните на етапа на проектиране и по подразбиране“, което означава, че трябва да бъде осигурена постоянна отчетност и поверителност на данните. Това изискване предполага разработчиците на програмни продукти да вложат ре-

- Have the necessary data protection measures been taken against the new challenges such as the crypto viruses occurring every second and how they adapt to them?
- Does the staff involved in the processing of PD have the required level of awareness and competence?
- Is it necessary to take any additional measures to comply with the GDPR?

SUGGESTED SOLUTION

After a detailed analysis of the GDPR clauses (1), the mandatory measures to be taken are laid down. These are presented below together with suggestions for applicable measures for their realization.

Article 25 of the ARRD requires that „Data protection at the design and default stage“ is implemented, which means that permanent accountability and confidentiality of the data must be ensured. This requirement requires software developers to implement solutions that align program products with the principles set out in the GDPR. The applicable measures include the use of anonymisation, pseudonymisation and data encryption, as well as the introduction of access control to information through implementation of a directory services, identity management, access matrix implementation, application of document management systems, etc.

Article 30, entitled „Registry of Processing Activities“, imposes an obligation on the PDC and the PDP to keep a record of the processing activities containing: the name and contact details of the PDC, the purpose of the processing, the description of the categories of DS and PD, the categories of recipients of PD, the deadlines for deleting the different categories of PD. This obligation until May 25, 2018 is of the Commission for Personal Data Protection (CPDP), after which its commitment to maintain it will be dropped. The applicable measures include the creation of an electronic register and possibly the implementation of a document management system.

The application of very serious measures involves Art. 32 of the GDPR entitled „Security of Processing“. Because complete anonymization in the healthcare is almost impossible, the first requirement is to introduce a data pseudonimization that can be done by changing the applied software. The protection of PD can be done with their encryption, which is the second requirement in this article. For this purpose, technical means that exist in database management systems (DBMSs) and operating systems may be applied, or additional software may be used. Security

шения, които да привеждат в съответствие разработените програмни продукти с принципите, заложени в ОРЗД. Приложимите мерки включват използване на анонимизация, псевдонимизация и криптиране на данните, както и въвеждане на контрол на достъпа до информацията чрез прилагане на директорийна услуга, управление на идентичностите, въвеждане на матрица на достъпа, прилагане на системи за управление на документите и др.

В чл.30 е озаглавен „Регистри на дейностите по обработване“ и вменява задължение АЛД и ОЛД да поддържат регистър за дейностите по обработване, който да съдържа: името и координатите за връзка на АЛД, целите на обработването, описание на категориите СД и ЛД, категориите получатели на ЛД, предвидените срокове за изтриване на различните категории ЛД. Това задължение до 25 май 2018 г. е на комисията за защита на личните данни (КЗЛД), след което отпада. Приложимите мерки включват създаване на електронен регистър и по възможност прилагане на система за управление на документите.

Прилагането на много сериозни мерки предполага чл.32 от ОРЗД, който е озаглавен „Сигурност на обработването“. Тъй като пълна анонимизация в сферата на здравеопазването е почти невъзможна, първото изискване е свързано с въвеждане на псевдонимизация на данните, което може да бъде направено с промяна на използваното приложно програмно осигуряване. Защитата на ЛД може да бъде направена и с тяхното криптиране, което е второто заложено в този член изискване. За целта могат да бъдат приложени технически средства, които съществуват в системите за управление на базите от данни (СУБД) и операционните системи или да се използва допълнителен софтуер. Необходимо ще бъде използване на сертификати. Следващото изискване се отнася до способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване на данните. Поверителността може да бъде постигната чрез прилагане на средства за управление на идентичностите и контрол на достъпа до информацията, включително многофакторна автентикация. Цялостност на данните може да бъде осигурена чрез прилагане на средства за защита срещу промени в данните при преноса чрез комуникационните канали и информационните носители – криптиране на комуникационните канали и цифрово подписване. Това ще стане изключително важно след въвеждането на електронно досие на гражданите на

certificaties will be required. The following requirement relates to the ability to ensure consistent confidentiality, integrity, availability and sustainability of data processing systems and services. Confidentiality can be achieved through the use of identity management tools and access control, including multi-factor authentication. Data integrity can be provided by applying means of protection against data traffic changes through communication channels and information carriers - encryption of communication channels and digital signatures. This will become extremely important after the introduction of an electronic dossier for the citizens of the Republic of Bulgaria, as well as the increasing use of different telemedicine channels with online data transmission. By building or using data centers that provide high reliability and availability (2) and implementation of IT solutions providing high availability of the services provided by application processing and storage systems, an adequate level of data availability can be ensured. Sustainability of services and processing systems can be ensured by implementing IT solutions and organizational measures to ensure high reliability and business continuity (3-5). Ability to recover data is possible through the implementation of IT solutions and organizational measures to ensure the rapid recovery of the processing and storage systems of the information and data processed by them. Permanent evaluation of the effectiveness of the measures taken is only possible if IT systems are implemented (SIEM, logging and log management) to detect:

- attempted unauthorized access;
- attacks on the systems;
- attempts to export information using an unauthorized channel;
- behavioral anomalies of the systems;
- behavioral anomalies of the users;
- changing the parameters of the working environment of the equipment;
- change in the state of the equipment.

The measures set out in this article are recommended for an ITIS, irrespective of the nature of the data being processed. The state-of-the-art IT technology offers a wide variety of technical measures and tools, the application of which will ensure the desired compliance with the requirements of the Regulation. It is recommended that a complex solution is implemented to assess the information received from different sources and to correlate the registered events to develop a solution for adequate management of ITIS.

РБ, както и с все по-засилващото се използване на различни канали за телемедицина с пренос на данни онлайн. Чрез изграждане или използване на дейта центрове осигуряващи висока надеждност и достъпност (2) и прилагане на ИТ решения осигуряващи висока наличност на услугите предоставяни от приложните системи за обработка и съхранение на данните може да бъде осигурено адекватно ниво на наличност на данните. Устойчивостта на услугите и системите за обработка може да се осигури, ако се приложат ИТ решения и организационни мерки, осигуряващи висока надеждност (непрекъсваемост) на системите за обработка и съхранение на информацията (business continuity) (3-5). Способност за възстановяване на данните е възможна чрез прилагане на ИТ решения и организационни мерки осигуряващи възможности за бързо възстановяване на системите за обработка и съхранение на информацията и данните обработвани от тях. Постоянно оценяване на ефективността на предприетите мерки е възможно само ако в ИТИС се внедрят системи (SIEM, наблюдение и управление на логовете) за откриване на:

- опити за неоторизиран достъп;
- атаки към системите;
- опити за изнасяне на информация по неразрешен канал;
- аномалии в поведението на системите;
- аномалии в поведението на потребителите;
- промяна на параметрите на работната среда на оборудването;
- промяна в състоянието на оборудването.

Мерките, заложени в този член, са препоръчителни за всяка една ИТИС, независимо от характера на данните, които се обработват. Съвременното ниво на ИТ технологиите предлага богато разнообразие от технически мерки и средства, чието прилагане ще осигури желаното съответствие с изискванията на регламента. Препоръчително е да се приложи комплексно решение, чрез което да се оценява информацията, получена от различни източници и чрез корелация на регистрираните събития да изработи решение за адекватно управление на ИТИС.

ЗАКЛЮЧЕНИЕ И ИЗВОДИ

Справянето с проблема сърдечна недостатъчност изисква индивидуално постоянно и дългосрочно наблюдение на редица клинични, лабораторни и инструментални параметри, които независимо къде се извършват са свързани с обработка на ЛД

CONCLUSIONS

Dealing with the heart failure problem requires individual consistent and long-term monitoring of a number of clinical, laboratory and instrumental parameters that, regardless of where they are performed, are related to a patient‘s personal data processing.

The analysis of the requirements laid down by the GDPR states that achieving compliance with them is only possible as a result of the introduction of adequate organizational and technical measures. The most successful case would be if a system based on a process-oriented approach is introduced for PD processing. Successful compliance with the GDPR can only be ensured if there is support from management and if it is realized that the implementation of technical measures only is not sufficient and a continuous assessment of the operation of the controls introduced is needed, as well as that of the results of the management and decision-making for their improvement.

These measures should be creatively applied in order to not to hinder and interfere with the work of medical professionals.

Address for correspondence:
Rosen Radkov
Department of Computer Science and Engineering
Technical University of Varna
1 Studentska Str.
9010 Varna
Bulgaria
e-mail: rossen.radkov@tu-varna.bg

REFERENCES

1. European Union, “Regulation 2016/679 of the European parliament and the Council of the European Union,” Off. J. Eur. Communities, vol. 2014, no. April, pp. 1–88, 2016.
2. Radkov R, Yotov Y. High Reliability Data Center for Cardiology. Heart-Lung (Varna) 2012;18;3-4,10–21.
3. BDS, БДС ISO/IEC 27001. Bulgaria, 2014, p. 30.
4. ANSI/TIA, TIA-942-A Telecommunications Infrastructure Standard for Data Centers, no.March. USA, 2012, p. 120
5. ANSI/BICSI, ANSI/Bicsi 002. 2011

на пациентите.

Извършеният анализ на изискванията, поставяни от ОРЗД, показва, че постигане на съответствие с тях е възможно само в резултат от въвеждане на адекватни организационни и технически мерки. Най-голям успех ще има, ако за обработката на ЛД се въведе система, която е базирана на процесно ориентиран подход. Успешно постигане на съответствие с ОРЗД може да бъде осигурено само ако има подкрепа от ръководството и ако се осъзнае, че прилагането само на технически мерки не е достатъчно, както и това, че трябва да се извършва постоянна оценка за работата на въведените контроли, прегледи на резултатите от ръководството и вземане на решение за тяхното подобряване.

Посочените мерки трябва да бъдат творчески прилагани, за да не затруднява и пречи на работата на медицинските работници.

Адрес за кореспонденция:
Росен Радков
Катедра Компютърни науки и технологии
Технически Университет, Варна
Ул. "Студентска" 1
9010 Варна
e-mail: rossen.radkov@tu-varna.bg