MedicaTest

Доклад

за

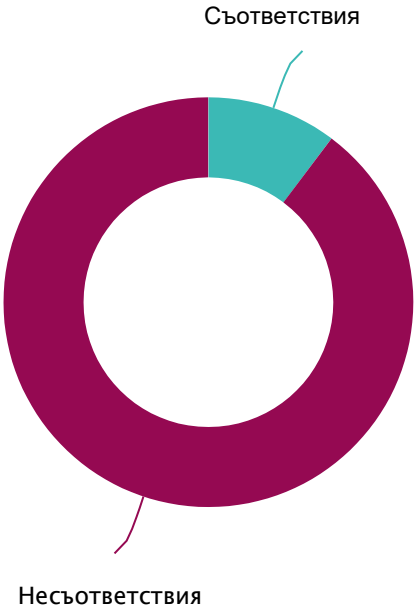
Оценка на GDPR *съответствие на вашата практика*

Лекар специалист

(*Дата*: 01-10-2018)

Лекар специалист

Графика на съответствие



Несъответствие: 90%

Поздравления, вие успешно завършихте вашия Medica Test. Резултатите показват, че вашата организация попада в обхвата на GDPR регламента, относно защитата на данните (ЕС 2016/679) на Европейския парламент и на Съвета на Европейския съюз.

За да съобразите начина, по който обработвате и съхранявате лични данни, с изискванията на GDPR регламента, е необходимо да се запознаете подробно със съдържанието на този документ. Първата приложена графика показва процентното съответствие на вашата организация спрямо изискванията на GDPR регламента.

В страниците след приложената графика ще намерите анализ, даващ цялостна и подробна експертиза на лекарската ви практика, изготвена съобразно отговорите от попълнения въпросник. Обърнете специално внимание на несъответствията и приложените към тях юридически и експертни съвети, за да избегнете последици, санкции и глоби.

1. **Извършвате ли дейност, която можете да определите като "обработка на лични данни"?** - Положителният отговор на въпрос №1 от системата на "Медика тест" означава, че Вие сте администратор на лични данни на Вашите пациенти, съобразно законовата дефиниция, която е залегнала в чл. 4, т. 7 от Регламента.

Препоръка: Като лица предоставящи медицински услуги на пациенти, Вие в ежедневната си медицинска практика неминуемо осъществявате обработка на една от най-чувствителните групи лични данни, които са обект на регулация по новия Регламент (ЕС) 2016/679, а именно: генетични данни, биометрични данни и данни за здравословното състояние на Вашите пациенти. Именно затова Регламентът класифицира тези данни като „специална категория лични данни“ и за тях са предвидени редица специални изисквания по отношение на сигурност и поверителност, с които следва да се запознаете и съответно да спазвате. Непознаването на новите нормативни изисквания за защита на специалната категория лични данни, които обработвате, може да доведе но нарушения на Регламента и респективно до налагане на съществени по своя размер административни санкции от страна на надзорния орган – Комисия за защита на личните данни /КЗЛД/. Нарушаването на поверителността на личните данни на Вашите пациенти може също така да е основание за търсене от Вас на гражданска отговорност за обезщетение по общия гражданскоправен ред от страна на лица, които са претърпели преки имуществени и неимуществени вреди.

Решение 1: Бланка 1 Обучителни материали за запознаване с основните принципи за обработка на ЛД

5. **При обработка на личните данни на вашите пациенти, въвели ли сте организационни и/или технически мерки за защита на същите от случайна загуба, унищожаване или повреждане, включително от незаконосъобразно и неразрешено обработване?** - Отрицателният отговор на въпрос № 5 от системата на "Медика тест" означава, че Вие нарушавате изискванията на Член 5 от Регламента относно въвеждане на организационни и/или технически мерки за защита на същите от случайна загуба, унищожаване или повреждане, включително от незаконосъобразно и неразрешено обработване.

Препоръка: Необходимо е да предприемете своевременни действия за отстраняване на несъответствието, като въведете необходимите организационни и технически мерки, които да осигуряват подходящо ниво на защита на личните данни на Вашите пациенти от случайна загуба, унищожаване или повреждане, включително от незаконосъобразно и неразрешено обработване. В тази връзка следва да се запознаете своевременно с принципите на обработка на личните данни на Вашите пациенти, които са залегнали в чл. 5 от Регламента, както и да извършвате периодична проверка на текущото си ниво на съответствие, за да избегнете налагане на административни санкции от страна на КЗЛД като надзорен орган, от една страна, а от друга страна да възпрепятствате възможността от съдебен иск от страна на Ваши пациенти във връзка с нарушение на правата им във връзка със защитата на личните им данни.

Решение 1: Бланка 8 Процедура за организационни и технически мерки за защита на ЛД от случайна загуба, унищожаване или повреждане
Решение 2: Бланка 1 Обучителни материали за запознаване с основните принципи за обработка на ЛД

10. **Обработвате ли лични данни на ненавършили пълнолетие лица?** - В случай, че сте дали положителен отговор на въпрос № 10 от системата на "Медика тест", и в този случай сте потвърдили, че обработвате лични данни на деца /съгласно Закона за закрила на детето – това са лица на възраст под 18 год./, то тогава следва да се запознаете с изискванията на Регламента относно спицифичните права на тези пациенти и свързаните с това средства за закрила.

Препоръка: Съгласно съображение № 38 от Преамбюла на Регламента, на децата се полага специална защита на личните данни, тъй като те не познават достатъчно добре съответните рискове, последици и гаранции, както и своите права, свързани с обработването на личните им данни. Тази специална защита следва да се прилага по-специално при предоставяне пряко на онлайн услуги на лица под 16 год., включително при предоставяне на медицински услуги на деца под 18 год., за което се изисква изричното съгласие на лицето, носещо родителска отговорност за съответния малолетен или непълнолетен пациент.

Решение 1: Бланка 5 Бланка за даване на родителско съгласие за обработка на ЛД на дете

13. **Обработват ли се лични данни на вашите пациенти от или под ръководството на ваш служител (административен персонал и др.), който не отговаря на задължението за професионална тайна**? - Даденият отговор от Вас на въпрос № 13 от системата на "Медика тест" означава, че не отговаряте на изискванията на Член 9, параграф 3 "Обработване на специални категории лични данни" от Регламента, тъй като обработването на специални категории лични данни на пациенти от страна на определени служители във Вашата организация е допустимо, когато служителите Ви са обвързани от задължението за спазване на професионална тайна.

Препоръка: Необходимо е да предприемете своевременни действия за отстраняване на несъответствието. За да обработвате специална категория лични данни по законосъобразен начин, е необходимо да въведете вътрешни правила, които да гарантират, че данните се обработват от или под ръководството на професионален работник, обвързан от задължението за професионална тайна. Това може да бъде реализирано с помощта на правилно изговена длъжностна характеристика и процедура за обработката, както и назначаването на лица, които да са професионални работници, обвързани от задължението да съдействат в рамките на вашата медицинска практика за спазване на поверителността на данните на вашите пациенти.

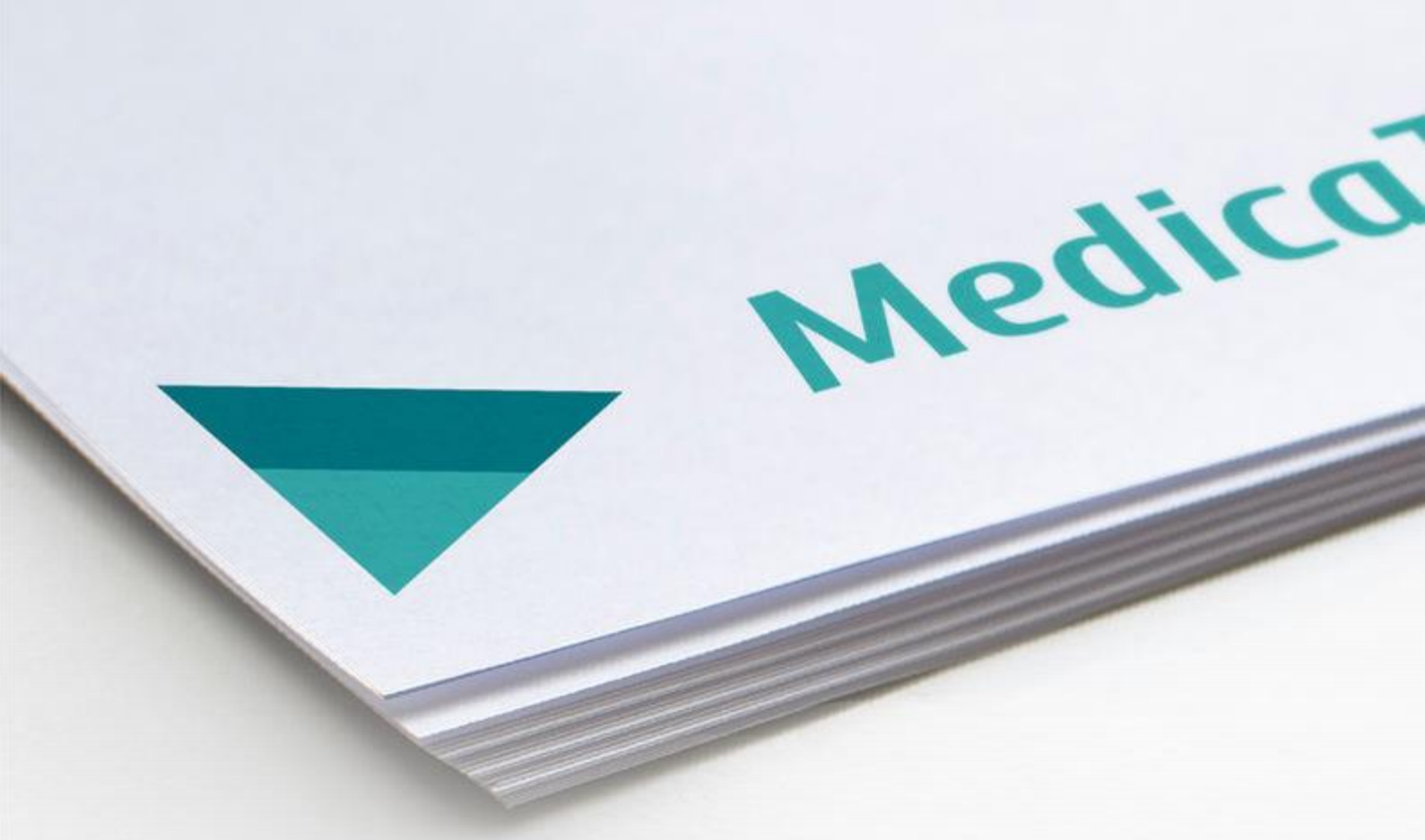
Решение 1: Бланка 11 Длъжностна характеристика на служител по защита на ЛД
Решение 2: Бланка 1 Обучителни материали за запознаване с основните принципи за обработка на ЛД

29. **В рамките на вашата медицинска практика, имате ли въведена процедура за своевременно уведомяване на надзорния орган /КЗЛД/ относно всяко нарушаване на сигурността на личните данни на вашите пациенти**? Даденият от Вас отрицателен отговор на въпрос № 35 от системата на "Медика тест" означава, че съгласно Член 33 от Регламента, НЕ отговаряте на изискванията, доколкото не разполагате с процедура за уведомяване на надзорния орган относно всяко нарушаване на сигурността на личните данни.

Препоръка: Необходимо е на основание чл. 33 от Регламента да разработите и имплементирате във вашата медицинска практика процедура, на базата на която да можете при констатирано нарушение на сигурността на личните данни, без ненужно забавяне (не по-късно от 72 часа след констатиране на нарушението) да уведомите за него надзорния орган /КЗЛД/. В случай, че не сте администратор на лични данни, а имате качеството „обработващ лични данни“ на пациенти на друго медицинско лице, което е администратор, то вие следва да уведомите без ненужно забавяне администратора за констатираното нарушение на сигурността. В уведомлението до КЗЛД трябва да посочите най-малко следната информация:

а) Описание на естеството на нарушението на сигурността на личните данни, включително, ако е възможно, категориите и приблизителния брой на засегнатите пациенти, категориите и приблизителното количество на засегнатите записи на лични данни;
б) Посочване на името и координатите за връзка на лице за контакт, от което може да се получи детайлна информация за нарушението;
в) Описание на евентуалните последици от нарушението на сигурността на личните данни;
г) Описание на предприетите или предложените от администратора мерки за справяне с нарушението на сигурността на личните данни, включително по целесъобразност мерки за намаляване на евентуалните неблагоприятни последици.

Решение 1: Бланка 26 Процедура и Бланка за уведомяване на КЗЛД относно нарушение сигурността на ЛД



Заключение

Благодарим ви, че се доверихте на Medica Test. Желаем ви успех в процеса по внедряване на изискванията на Регламента и се надяваме, че сме успели да ви дадем ясен отговор и посока за справяне с предизвикателствата на новата нормативна уредба, която влиза в сила на 25 май 2018 г.

Моля, имайте предвид, че резултатите от Medica Test не представляват задълбочен правен анализ на юридическите аспекти, свързани с дейността ви на медицински специалист, а обхващат общите правила и процедури, които следва да спазвате. Затова препоръчваме, след получаване и анализиране на резултатите от Medica Test, допълнително да обсъдите детайлите с вашите юридически и/или технически консултанти, за да изпълните максимално изискванията на Регламента и отразите всички специфични характеристики на медицинска ви практика.

В случай, че е останало нещо неясно, не се колебайте да се свържете с нас на info@medicatest.bg. Екипът ни от специалисти ще отговори на всеки ваш въпрос в обхвата на Medica Test и GDPR регламента.

ДО

.....

/администратор на лични данни/

ВЪЗРАЖЕНИЕ СРЕЩУ ОБРАБОТКА НА ЛИЧНИ ДАННИ НА ПАЦИЕНТ на основание чл. 21 от Регламент (ЕС) 2016/679

От……

ЕГН:……

/данни на пациент/

С настоящата молба и на основание чл. 21 от Регламент (ЕС) 2016/679, долуподписаният……
(изписват се данните на пациента) възразявам срещу обработката на личните ми данни, които данни съм Ви предоставил като Ваш пациент */поставете отметка на избраното от Вас решение/*:

□ срещу цялостната обработка на личните ми данни

□ срещу обработката на личните ми данни за целите на вземане на автоматизирани решения, включващи профилиране

□ срещу обработката на личните ми данни за целите на предоставяне на услуги на информационното общество /онлайн услуги/

Във връзка с горното и на основание чл. 21 от Регламент (ЕС) 2016/679, моля незабавно след получаване на настоящата молба да прекратите обработката на личните ми данни.

С оглед направеното възражение, ☐**ЖЕЛАЯ/**☐**НЕ ЖЕЛАЯ** /отбележете избраното от Вас решение/ личните ми данни да бъдат изтрити без ненужно забавяне на основание чл.17, параграф 1, б.“в“ от Регламент (ЕС) 2016/679.

Уведомен съм, че администраторът на лични данни може да откаже да прекрати обработването на личните ми данни, ако съществуват убедителни законови основания за обработването, които имат предимство пред моите интереси, права и свободи, или за установяването, упражняването или защита на правни претенции.

Уведомен съм, че администраторът на лични данни може да откаже да прекрати обработката на личните ми данни за целите на вземане на автоматизирани решения, включващи профилиране при наличие на някоя от хипотезите на чл.22, параграф 2 от Регламент (ЕС) 2016/679.

Уведомен съм, че администраторът на лични данни може да откаже да изтрие личните ми данни ако са налице някои от основанията посочени в чл.17, параграф 3" от Регламент (ЕС) 2016/679.

Дата: ……

С уважение:……