

Одобрявам:

Директор на НЦЗПБ

Проф. д-р Тодор Кантарджиев, дмн, мзм

ИНСТРУКЦИЯ

За събиране, обработка и защита на личните данни в НАЦИОНАЛЕН ЦЕНТЪР ПО
ЗАРАЗНИ И ПАРАЗИТНИ БОЛЕСТИ (НЦЗПБ) и реда за достъп до тях

I. ОБЩИ ПОЛОЖЕНИЯ

Предмет на ИНСТРУКЦИЯТА

1. Настоящата инструкция се издава от Директора на НЦЗПБ в качеството му на администратор на лични данни.
2. В нея се определя редът за събиране, обработка, съхраняване и защита на личните данни, във връзка с изискванията на ЗЗЛД;
3. Инструкцията урежда правата и задълженията на носителите на лични данни, правата и задълженията на обработващите и операторите на личните данни, както и реда за реализиране на отношенията на Директора в качеството му на Администратор с Комисията за защита на личните данни.
4. Инструкцията се издава в съответствие с ЗЗЛД и подзаконовите нормативни актове по тяхното прилагане.

Приложение на ИНСТРУКЦИЯТА

1. Инструкцията се прилага по отношение на администратора, обработващите и операторите на личните данни в НЦЗПБ.
2. Инструкцията се прилага по отношение на всички лица, чиито лични данни се събират, обработват и съхраняват в НЦЗПБ, както и по отношение на всички трети лица, които на действително основание имат право да оперират с чужди лични данни.
3. Посочените в Инструкцията субекти са длъжни да спазват правилата установени в нея от момента, в който се запознаят с нея.
4. Администраторът е длъжен да доведе Инструкцията до знанието на посочените в нея лица.

II. ВИДОВЕ ЛИЧНИ ДАННИ СЪБИРАНИ, ОБРАБОТВАНИ И СЪХРАНЯВАНИ В НЦЗПБ

1. В НЦЗПБ могат да се събират, обработват и съхраняват лични данни относно физическа идентичност като: име, презиме, фамилия, ЕГН и постоянен адрес на всички изследвани лица;
2. Име, адрес и телефон на личния лекар;

3. Възраст и пол;
4. Епидемиологични данни и анамнези;
5. Резултати от проведените изследвания;
6. Епикризи на пациенти при необходимост;
7. Мета-данни;

Ш. ДОКУМЕНТИ, СЪДЪРЖАЩИ ЛИЧНИ ДАННИ СЪБИРАНИ, ОБРАБОТВАНИ И СЪХРАНЯВАНИ В НЦЗПБ

1. Амбулаторен журнал (хартиен носител);
2. Амбулаторна карта (хартиен носител);
3. Бързо известие (хартиен и/или електронен носител);
4. Платежни документи;
5. Декларация за информирано съгласие;
6. Документи в резултат от вторична и/или последваща обработка на лични данни (хартиен и/или електронен носител);
7. Договори с физически лица.

IV. ЛИЦА, ОПРАВМОЩЕНИ ДА ОБРАБОТВАТ ЛИЧНИ ДАННИ В НЦЗПБ

1. „Длъжностно лице“ са служителите на длъжност: Директор, зам. директор, юрист, главен счетоводител, човешки ресурси, зав. лаборатория и зав. отдел.

1.1. Служебни задължения:

1.1.1 Да организира и създава всички необходими по смисъла на ЗЗЛД условия и предпоставки за законосъобразното събиране, обработване и съхранение на личните данни.

1.1.2 Да осъществява цялостен контрол върху изпълнението на задължението за информация при предоставяне на личните данни.

1.1.3 Да осъществява цялостен контрол върху дейността на всички обработващи и оператори на лични данни за правилното прилагане на ЗЗЛД.

1.1.4 Да организира и осъществява цялостен контрол върху дейността по предоставяне на достъп на лицата до личните данни.

1.1.5 Да организира и осъществява контрол върху дейността по воденето на регистри за достъп до личните данни; върху извеждането на заявленията, издаването на документи или отказите за предоставяне на достъп до исканата информация по смисъла на ЗЗЛД.

1.1.6 Да предоставя при необходимост информация относно дейността по прилагане на ЗЗЛД в отдела и за проблемите свързани с нея.

1.1.7 Да дава указания на обработващите и операторите за правилно прилагане на ЗЗЛД и настоящата ИНСТРУКЦИЯ.

1.1.8 Да упражнява текущ и инцидентен контрол по повод реда и начина, по който се реализира достъпа до личните данни.

1.1.9 Да предоставя достъп до личните данни само на оправомощените лица.

1.1.10 Да издава разрешение за достъп до лични данни.

1.1.11 Да издава разрешение за достъп до лични данни на инцидентно обработващи или трети лица.

1.1.12 Всички лични данни, които стават достъпни на длъжностното лице при или по повод изпълнение на задълженията му, са служебна тайна. Длъжностното лице не може да разпространява под каквато и да е форма и пред когото и да е факти и сведения, които представляват лични данни по смисъла на ЗЗЛД.

2. „Обработващ лични данни“ са служители на длъжност: зав. отдел, зав. лаборатория, лекар, биолог, ИТ – специалист, счетоводител, лаборант, деловодител.

2.1. Задължения на служителите:

2.1.1. Да събират, обработват и съхраняват личните данни, като спазват изискванията на ЗЗЛД.

2.1.2. Да информират всяко лице, чиито данни се събират, за правата му по ЗЗЛД.

2.1.3. Да реализират правото на достъп до личните данни съгласно ЗЗЛД

2.1.4. Да водят регистър за подадените заявления за достъп до лични данни; да разглеждат и проверяват законосъобразността на поисканата информация; да съставят отказ или да предоставят исканата информация; да връчват на лицето информацията.

2.1.5. Да осигуряват необходимите технически и организационни мерки, включително и специални при предаване на данните по електронен път, за защитата им от случайно или незаконно нарушение, незаконно разкриване или достъп, нерегламентирано изменение или разпространение, както и други незаконни форми на обработване на лични данни.

2.1.6. Да не изготвят и съхраняват копия от носители, съдържащи обработени лични данни, след като оригиналите бъдат предадени на длъжностното лице.

2.1.7. Да пазят всички лични данни, до които имат достъп при или по повод изпълнение на служебните им задължения, в служебна тайна.

2.1.8. Да не разпространяват под каквато и да е форма и пред когото и да е факти и сведения, които представляват лични данни по смисъла на ЗЗЛД и са узнати от тях при или по повод изпълнението на задълженията им.

2.1.9. Обработващите на лични данни носят отговорност пред Длъжностните лица за причинени в резултат на неправомерни действия или бездействия имуществени и неимуществени вреди.

3. „Оператор на лични данни“ са служители на длъжност: лекар, биолог, ИТ – специалист, счетоводител, лаборант, деловодител.

3.1. Задължения на оператора на лични данни:

3.1.1. Да ползва личните данни така, че да предотвратят тяхното разпространение или узнаване от трети лица, които нямат право на това.

3.1.2. Да ползва само тези лични данни, до които имат право на достъп, във връзка с изпълнение на служебните си задължения.

3.1.3. Да реализира необходимите технически и организационни мерки за защита на данните от незаконно разкриване или достъп.

3.1.4. Да не предоставя информация или достъп до обработваните лични данни на трети лица без получаване на предварително разрешение от страна на Длъжностното лице или обработващия.

3.1.5. Да не изготвят и съхраняват копия от носители, съдържащи обработени лични данни, след като оригиналите бъдат предадени на длъжностното лице.

3.1.6. Да пазят всички лични данни, до които имат достъп при или по повод изпълнение на служебните им задължения, в служебна тайна.

3.1.7. Обработващите на лични данни носят отговорност пред Длъжностните лица и Администратора за причинени в резултат на неправомерни действия или бездействия имуществени и неимуществени вреди.

V. ИНФОРМИРАНЕ НА ЛИЦАТА, ЧИИТО ДАННИ СЕ СЪБИРАТ В НЦЗПБ

1. Администраторът има задължение да информира всяко лице, когато събира неговите лични данни, освен в случаите, когато Администраторът унаследява правата за работа с личните данни от посредник при условията предвидени в ЗЗЛК.

2. Задължението за информиране се извършва и удостоверява чрез попълнена от лицето, собственик на личните данни или от негов законен представител/настоятник, Декларация за информирано съгласие (Приложение 1).

VI. СЪБИРАНЕ НА ЛИЧНИ ДАННИ

1. Личните данни в НЦЗПБ се събират от съответните оправомощени лица по отдели.

2. Документите на хартиен носител се събират и подреждат в амбулаторен журнал, амбулаторна карта, бързо известие, талон за изследване, платежни документи, договори с физически лица.

3. Личните данни от хартиен носител могат да се въвеждат в софтуерен продукт за последваща обработка и ползване. Достъп до данни имат съответните служители по отдели във връзка с изпълнение на служебните им задължения.

VII. СЪХРАНЯВАНЕ И ЗАЩИТА НА ЛИЧНИ ДАННИ

1. Регистрите с лични данни могат да се водят на хартиен и/или на електронен носител.
2. Документите на хартиен носител, съдържащи лични данни се съхраняват в картотечен шкаф, определен от Длъжностното лице за отдела, достъпа до който е ограничен само до оправомощения персонал.
3. Операционните системи на локалните терминали, съдържащи файлове с лични данни, са защитени с парола за достъп, с която разполагат единствено оправомощените служители в отдела.
4. Достъпът до сървър-базираните софтуерни системи за обработка и съхранение на лични данни е защитен с персонални потребителско име и парола за всеки служител с права за достъп.
 - 4.1. Системите, опериращи на глобално ниво по отношение на вътрешната мрежа на НЦЗПБ, разполагат с йерархия на правата за достъп на потребителите в зависимост от информационните нужди на съответните служители във връзка с изпълнение на служебните им задължения.
 - 4.2. Достъпът до тези системи е ограничен във вътрешната мрежа на НЦЗПБ.
5. Сървър-базираните софтуерни системи за обработка и съхранение на лични данни във вътрешната мрежа на НЦЗПБ нямат директна свързаност с глобалната мрежа.
6. При предоставяне на електронни услуги за достъп до информация, намиращи се на някоя от електронните системи на НЦЗПБ, от крайните потребители се изисква идентификация чрез предварително предоставени им параметри за достъп.
7. В случаи, когато лични данни по смисъла на ЗЗЛК в електронен формат се разпространяват и/или събират на платформи администрирани или собственост, но извън вътрешната мрежа, на НЦЗПБ или сървъра за електронна поща на хостинга това става единствено по HTTPS, sFTP или чрез криптирани файлове с предварително уговорени с получателите параметри за достъп до съдържанието.
 - 7.1. Данните за достъп до съдържанието се уточняват с получателите в различни от сесията по прехвърляне на файловото съдържание комуникационни сесии.
8. Механизмите за предотвратяване на неправомерен достъп, повреждане, изгубване или унищожаване се осигурява посредством поддържане на актуални антивирусни програми и периодично архивиране на данните на отделни електронни и/или хартиени носители.
9. При настъпване на непредвидимо обстоятелство, което би могло да засегне сигурността на данните, служителят, регистрирал инцидента докладва незабавно на Директора на НЦЗПБ.
10. Минималното съдържание на доклада включва данни за лицето, регистрирало инцидента, възможните последствия от него и предложение за предприемане на мерки за предотвратяване или ограничаване на последствията.

VIII. АРХИВИРАНЕ

1. Лабораторните журнали и протоколите от изследванията се съхраняват с продължителност 10 години;

2. Данните, запазени на електронни носители, се съхраняват с продължителност не повече от 10 години.

IX. ДОСТЪП ДО ЛИЧНИ ДАННИ

1. Всяко лице, чиито данни се намират в НЦЗПБ има право на достъп до тях.
2. Лицето, което иска достъп, може да го направи лично, като попълни заявление.
3. След получаване на заявлението Длъжностното лице преценява законосъобразността на поискания достъп и го разрешава или забранява.

X. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

1. Инструкцията влиза в сила от 11.06.2018. г., след като всички лица, за които тя създава субективни права и задължения, са се запознали с нея.
2. Копие от инструкцията е на разположение на служителите на НЦЗПБ.

Приложение 1 – Декларация за информирано съгласие

ДЕКЛАРАЦИЯ

Подписаният/та.....

Декларирам, че съм информиран по смисъла на чл. 19, ал. 1 от ЗЗЛД

Декларирам, че на основание чл.5, ал.2, т.2 от Закона за защита на личните данни **ДАВАМ СЪГЛАСИЕТО СИ** НЦЗПБ да обработва личните ми данни в качеството на администратор на лични данни.

Известно ми е, че мои лични данни, съдържащи здравна информация, могат да бъдат предоставени на трети лица само при наличие на хипотезите, посочени в чл.28, ал.1 от Закона за здравето (в случай, че:

- *лечението продължи в друго лечебно заведение;*
- *съществува заплаха за здравето или живота на други лица;*
- *необходимост при идентификация на човешки труп или за установяване на причините за смъртта;*
- *за нуждите на държавния здравен контрол за предотвратяване на епидемии и разпространение на заразни заболявания;*
- *за нуждите на медицинската експертиза и общественото осигуряване;*
- *за нуждите на медицинската статистика или за медицински научни изследвания, след като данните, идентифициращи пациента, са заличени;*
- *за нуждите на Министерството на здравеопазването, Националния център по здравна информация, НЗОК, регионалните здравни инспекции и Националния статистически институт.)*

Информиран съм, че в случай на съществуваща заплаха за здравето или живота на други лица, преди да предостави мои лични данни, съдържащи здравна информация, на основание чл. 28, ал. 2 от Закона за здравето, администраторът на лични данни НЦЗПБ е длъжен да ме уведоми за това обстоятелство.

Декларатор:.....