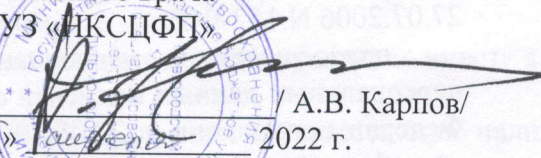


УТВЕРЖДАЮ

И. о. главного врача
ГБОУЗ «НКСЦФП»


/ А.В. Карпов/
«25» 2022 г.



ПОЛОЖЕНИЕ О ЗАЩИТЕ, ХРАНЕНИИ, ОБРАБОТКЕ И ПЕРЕДАЧЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ ГБОУЗ «НОВГОРОДСКИЙ КЛИНИЧЕСКИЙ СПЕЦИАЛИЗИРОВАННЫЙ ЦЕНТР ФТИЗИОПУЛЬМОНОЛОГИИ»

1. Общие положения

1.1. Настоящее Положение регламентируется Конституцией Российской Федерации, Федеральным законом «Об информации, информационных технологиях и о защите информации» N 149-ФЗ от 27.07.2006 года, Федеральным законом от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом «О персональных данных» N 152-ФЗ от 27.07.2006 года, Федеральным законом от 22.10.2004 N 125-ФЗ «Об архивном деле в Российской Федерации» и другими нормативными правовыми актами.

1.1. Настоящим Положением определяется порядок обработки персональных данных пациентов ГБОУЗ «НКСЦФП» (Далее – Медицинская организация, оператор).

1.2. Обработка персональных данных пациентов осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов.

2. Основные понятия. Состав персональных данных пациентов

2.1. Для целей настоящего Положения используются следующие основные понятия:

персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) (п. 1 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

персональные данные, разрешенные субъектом персональных данных для распространения, - персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном Федеральным законом от 27.07.2006 N 152-ФЗ (далее - персональные данные, разрешенные для распространения) (п. 1.1. ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ).

оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными (п. 2 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обработка персональных данных пациента - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных (п. 3 ст. 3 Федерального закона

от 27.07.2006 N 152-ФЗ);

распространение персональных данных - действия, направленные на раскрытие персональных данных пациента неопределенному кругу лиц (п. 5 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

предоставление персональных данных - действия, направленные на раскрытие персональных данных пациента определенному лицу или определенному кругу лиц (п. 6 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

блокирование персональных данных - временное прекращение обработки персональных данных пациентов (за исключением случаев, если обработка необходима для уточнения персональных данных) (п. 7 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

уничтожение персональных данных - действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных пациентов и (или) в результате которых уничтожаются материальные носители персональных данных пациентов (п. 8 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

обезличивание персональных данных - действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному пациенту (п. 9 ст. 3 Федерального закона от 27.07.2006 N 152-ФЗ);

врачебная тайна - сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении (ст. 13 Федерального закона от 21 ноября 2011 г. N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»).

2.2. Под персональными данными пациентов понимается любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, в том числе, его фамилия, имя, отчество, пол, год, месяц, дата и место рождения, адрес места жительства и регистрации, контактные телефоны, реквизиты полиса ОМС (ДМС), индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), паспортные данные, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью, данные о составе семьи, прочие сведения, которые могут идентифицировать человека.

Персональные данные пациентов относятся к специальной категории персональных данных, обработка таких персональных данных должна осуществляться лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну.

Персональные данные пациентов являются конфиденциальными сведениями.

Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении срока хранения, если иное не определено законодательством РФ.

Обеспечение конфиденциальности персональных данных не требуется:

- в случае обезличивания персональных данных;
- в отношении общедоступных персональных данных.

3. Хранение, обработка и передача персональных данных работника

3.1. Все персональные сведения о пациентах Медицинская организация может получить только от них самих. В случаях, когда Медицинская организация может получить необходимые персональные данные пациентов только у третьего лица, Медицинская организация должна уведомить об этом пациентов и получить от них письменное согласие.

3.2. Медицинская организация обязана сообщить пациентам о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа пациентов дать письменное согласие на их получение.

3.3. Пациент принимает решение о предоставлении его персональных данных и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных даётся в письменной форме и должно быть конкретным,

информированным и сознательным.

В случае получения согласия на обработку персональных данных от представителя субъекта персональных данных полномочия данного представителя на дачу согласия от субъекта персональных данных проверяются оператором.

Согласие пациента на обработку его персональных данных должно храниться вместе с его иной медицинской документацией.

Обработка персональных данных пациентов без их согласия допускается при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

Кроме того, предоставление сведений о факте обращения пациента за оказанием медицинской помощи, сведений о состоянии его здоровья и диагнозе, иных сведений, полученных при его медицинском обследовании и лечении (врачебная тайна), без согласия гражданина или его законного представителя допускается:

1) в целях проведения медицинского обследования и лечения пациента, который в результате своего состояния не способен выразить свою волю, если медицинское вмешательство необходимо по экстренным показаниям для устранения угрозы жизни человека и если его состояние не позволяет выразить свою волю или отсутствуют его законные представители.

2) при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

3) по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органа уголовно-исполнительной системы в связи с исполнением уголовного наказания и осуществлением контроля за поведением условно осужденного, осужденного, в отношении которого отбывание наказания отсрочено, и лица, освобожденного условно-досрочно;

4) в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 Федерального закона от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ», для информирования одного из его родителей или иного законного представителя;

5) в целях информирования органов внутренних дел о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий;

6) в целях проведения военно-врачебной экспертизы по запросам военных комиссариатов, кадровых служб и военно-врачебных (врачебно-летных) комиссий федеральных органов исполнительной власти, в которых предусмотрена военная и приравненная к ней служба;

7) в целях расследования несчастного случая на производстве и профессионального заболевания;

8) при обмене информацией медицинскими организациями, в том числе размещенной в медицинских информационных системах, в целях оказания медицинской помощи с учетом требований законодательства Российской Федерации о персональных данных;

9) в целях осуществления учета и контроля в системе обязательного социального страхования;

10) в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в РФ».

3.4. Согласие на обработку персональных данных может быть отозвано пациентом. В случае отзыва пациентом согласия на обработку персональных данных оператор вправе продолжить обработку персональных данных без согласия пациента при наличии оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи 10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных". Обязанность предоставить доказательство получения согласия пациента на обработку его персональных данных или доказательство наличия оснований, указанных в пунктах 2 - 11 части 1 статьи 6, части 2 статьи

10 и части 2 статьи 11 Федерального закона от 27.07.2006 № 152-ФЗ "О персональных данных", возлагается на оператора.

3.4. Персональные данные пациентов являются конфиденциальной информацией и не могут быть использованы Медицинской организацией или любым иным лицом в личных целях.

3.5. Медицинская организация разрабатывает меры защиты персональных данных пациентов.

3.6. Пациенты не должны отказываться от своих прав на сохранение и защиту тайны.

3.7. Персональные данные пациентов хранятся в регистратурах амбулаторно-поликлинических отделений Медицинской организации, стационарных отделениях, организационно-методическом отделе на бумажных носителях и электронных носителях с ограниченным доступом.

Право доступа к персональным данным пациентов имеют: главный врач Медицинской организации (исполняющий обязанности), заместитель главного врача по лечебной работе, по поликлинической работе, заведующие подразделениями, филиалами, медицинские работники (заведующие отделениями, врачи, старшие мед. сестры, главная мед. сестра, другие мед. работники отделения); медицинский статистик, медицинский регистратор, юрисконсульт, программист / системный администратор, менеджер по платным услугам (к тем данным, которые необходимы для выполнения конкретных функций), сами пациенты (носители данных).

3.8. Медицинская организация может передавать персональные данные пациентов третьим лицам, только если это необходимо в целях предупреждения угрозы их жизни и здоровья, а также в случаях, установленных законодательством.

3.9. Персональные данные вне Медицинской организации могут представляться в государственные и негосударственные функциональные структуры (внешний доступ): правоохранительные органы; органы статистики; органы социального страхования; органы статистики; управление Роспотребнадзора, Росздравнадзора по Новгородской области; министерство здравоохранения Новгородской области; органы опеки и попечительства; комиссии по делам несовершеннолетних и защите их прав; другие лечебно-профилактические учреждения.

3.10. Учреждение осуществляет передачу персональных данных работников и пациентов только при наличии согласия указанных лиц на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

3.11. Обработка персональных данных, разрешенных для распространения, из числа специальных категорий персональных данных, указанных в ч. 1 ст. 10 Федерального закона от 27.07.2006 N 152-ФЗ, допускается, если соблюдаются запреты и условия, предусмотренные ст. 10.1 указанного Закона.

3.12. Медицинская организация обязана обеспечить пациентам возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

3.13. В согласии пациента на обработку персональных данных, разрешенных им для распространения, пациент вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных Медицинской организации неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Отказ Медицинской организации в установлении работником или пациентом запретов и условий, предусмотренных настоящим пунктом, не допускается.

3.14. При передаче персональных данных пациентов Медицинская организация предупреждает лиц, получающих данную информацию, о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требуют от этих лиц письменное подтверждение соблюдения этого условия.

4. Требования к помещениям, в которых производится обработка персональных данных.

4.1. Размещение оборудования информационных систем персональных данных, специального оборудования и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

4.2. Помещения, в которых располагаются технические средства информационных систем персональных данных или хранятся носители персональных данных, должны соответствовать требованиям пожарной безопасности, установленным действующим законодательством Российской Федерации.

4.3. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

4.4. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

5. Обязанности Медицинской организации по хранению и защите персональных данных пациентов.

5.1. Медицинская организация обязана за свой счет обеспечить защиту персональных данных пациентов от неправомерного использования или утраты в порядке, установленном законодательством РФ.

5.2. Медицинская организация обязана принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Медицинская организация самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

5.3. Медицинская организация обязана осуществлять передачу персональных данных пациентов только в соответствии с настоящим Положением и законодательством РФ.

5.4. Медицинская организация обязана предоставлять персональные данные пациентов только уполномоченным лицам и только в той части, которая необходима им для выполнения их трудовых обязанностей, в соответствии с настоящим Положением и законодательством РФ.

5.5. Медицинская организация не имеет права получать и обрабатывать персональные данные пациентов об их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

5.6. Медицинская организация не имеет права получать и обрабатывать персональные данные пациентов о его расовой, национальной принадлежности, политических взглядах, религиозных и философских убеждениях, состоянии здоровья, интимной жизни, за исключением случаев, предусмотренных Трудовым кодексом РФ и другими федеральными законами.

5.7. Медицинская организация не имеет права получать и обрабатывать персональные данные пациентов о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

5.8. Медицинская организация не должна оказывать препятствие пациентам в получении бесплатной информации, содержащей персональные данные пациента, включая право на

получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

5.9. Медицинская организация обязана по требованию пациентов предоставить им полную информацию об их персональных данных и обработке этих данных.

6. Права пациентов на защиту их персональных данных

6.1. Пациенты в целях обеспечения защиты своих персональных данных, хранящихся у Медицинской организации, имеют право:

- получать полную информацию о своих персональных данных, их обработке, хранении и передаче;
- определять своих представителей для защиты своих персональных данных;
- на доступ к относящимся к ним медицинским данным с помощью медицинского специалиста по их выбору;
- требовать исключения или исправления неверных или неполных персональных данных, а также данных, обработанных с нарушениями настоящего Положения и законодательства РФ.

При отказе Медицинской организации исключить или исправить персональные данные пациентов, пациенты вправе заявить Медицинской организации в письменном виде о своем несогласии с соответствующим обоснованием;

- требовать от Медицинской организации извещения всех лиц, которым ранее были сообщены неверные или неполные персональные данные пациентов, обо всех произведенных в них исключениях, исправлениях или дополнениях.

6.2. Если пациенты считают, что Медицинская организация осуществляет обработку их персональных данных с нарушением требований Федерального закона или иным образом нарушает их права и свободы, они вправе обжаловать действия или бездействие Медицинской организации в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке.

6.3. Пациент вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных им для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона или обратиться с таким требованием в суд.

7. Порядок уничтожения, блокирования персональных данных

7.1. В случае выявления неправомерной обработки персональных данных при обращении пациентов Медицинская организация обязана осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этим пациентам, с момента такого обращения на период проверки.

7.2. В случае выявления неточных персональных данных при обращении пациентов Медицинская организация обязана осуществить блокирование персональных данных, относящихся к этим пациентам, с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы пациентов или третьих лиц.

7.3. В случае подтверждения факта неточности персональных данных Медицинская организация на основании сведений, представленных пациентами, или иных необходимых документов обязано уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

7.4. В случае поступления требования пациента о прекращении распространения его персональных данных, передача (распространение, предоставление, доступ) персональных данных, разрешенных таким пациентом, для распространения, должна быть прекращена в любое время.

Действие согласия пациента на обработку персональных данных, разрешенных им для распространения, прекращается с момента поступления в Медицинскую организацию указанного требования.

7.5. В случае выявления неправомерной обработки персональных данных, осуществляемой Медицинской организацией, Медицинская организация в срок, не превышающий трех рабочих дней, начиная от даты этого выявления, обязано прекратить неправомерную обработку персональных данных.

7.6. В случае, если обеспечить правомерность обработки персональных данных невозможно, Медицинская организация в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязано уничтожить такие персональные данные.

7.7. Об устранении допущенных нарушений или об уничтожении персональных данных Медицинская организация обязана уведомить пациентов.

7.8. В случае достижения цели обработки персональных данных Медицинская организация обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней от даты достижения цели обработки персональных данных.

7.9. В случае отзыва пациентами согласия на обработку их персональных данных Медицинская организация обязана прекратить их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожить персональные данные в срок, не превышающий тридцати дней от даты поступления указанного отзыва.

7.10. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 7.4-7.9 настоящего Положения, Медицинская организация осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

8. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациентов

8.1. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациентов, привлекаются к дисциплинарной, материальной, гражданско-правовой, административной и уголовной ответственности в порядке, установленном действующим законодательством РФ.

8.2. Моральный вред, причиненный пациентам вследствие нарушения их прав, нарушения правил обработки персональных данных, установленных Федеральным законом, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных работниками и пациентами убытков.

9. Заключительные положения

9.1. Настоящее Положение вступает в силу с момента его утверждения.

9.2. Медицинская организация обеспечивает неограниченный доступ к настоящему документу.