Утверждено приказом ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации от 01 марта 2023г. № 24

ПОЛОЖЕНИЕ

о защите, хранении, обработке и передаче персональных данных пациентов ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Целью положения об обработке персональных данных (далее – Положение) является защита персональных данных пациентов ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации (далее – Санаторий) от несанкционированного доступа, неправомерного их использования или утраты, а также установление ответственности должностных лиц, имеющих доступ к персональным к персональным данным пациентов, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

Положение разработано в соответствии со следующими нормативными правовыми актами: Настоящее Положение определяется в соответствии со следующими нормативными правовыми актами:

– Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных";

– Указ Президента Российской Федерации от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера";

– Постановление Правительства РФ от 15 сентября 2008 г. № 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации";

–Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных";

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

- Федеральный закон от 25.07.2011 № 261-ФЗ «О внесении изменений в Федеральный закон «О персональных данных»;

- Федеральный закон от 21.07.2014 № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»;

- Постановление Правительства Российской Федерации от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технология хранения таких данных вне информационных систем персональных данных»;

- Приказ Роскомнадзора от 30.05.2017 №94 «Об утверждении методически х рекомендаций по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения»;

- Приказ Роскомнадзора от 30.10.2018 № 159 «О внесении изменений в Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения, утвержденные приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 30.05.2017 № 94»;

- Приказ Роскомнадзора от 24.02.2021 № 18 «Об утверждении требований к содержанию согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения»;

- Приказ Роскомнадзора от 21.06.2021 № 106 «Об утверждении Правил использования информационной системы Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, в том числе порядка взаимодействия субъекта персональных данных с оператором»;

- Постановление Правительства Российской Федерации от 29.062021 №1046 «О федеральном государственном контроле (надзоре) за обработкой персональных данных».

1.2 Порядок ввода в действие и изменения Положения:

1.2.1 Положение вступает в силу с момента утверждения его директором Санатория и действует бессрочно, до замены его новым положением.

1.2.2 Все изменения в Положении вносятся соответствующим приказом.

1.3 Персональные данные пациентов относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечивается отнесением их к сфере негосударственной (служебной, профессиональной) тайны.

2. СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

2.1 В состав персональных данных пациентов ФГБУ «Санаторий «Красные камни» Управления делами Президента Российской Федерации входят:

- фамилия, имя, отчество;
- пол;
- дата рождения;
- место рождения;
- гражданство;
- данные документа, удостоверяющего личность;
- место жительства;
- место регистрации;
- дата регистрации;
- страховой номер индивидуального лицевого счета;
- номер полиса обязательного медицинского страхования застрахованного лица;
- анамнез;
- диагноз;
- сведения об организации, осуществляющей медицинскую деятельность;
- вид оказанной медицинской помощи;
- условия оказания медицинской помощи;
- сроки оказания медицинской помощи;
- объем оказанной медицинской помощи, включая сведения об оказанных медицинских услугах;
- результат обращения за медицинской помощью;
- сведения о медицинском работнике или медицинских работниках, оказавших медицинскую помощь;
- иные сведения, необходимые медицинской организации в соответствии с действующим законодательством Российской Федерации в области персональных данных, с помощью которых можно идентифицировать субъекта персональных данных.

2.2 Данные документы являются конфиденциальными, при этом, учитывая их массовость и единое место обработки и хранения – соответствующий гриф ограничения на них не ставится;

2.3 Оператор может предусматривать необходимость предъявления дополнительных документов.

3. ОБРАБОТКА ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1 В целях обеспечения прав и свобод пациентов Санатория при обработке персональных данных пациентов обязаны соблюдать следующие требования:

- Обработка персональных данных пациента может осуществляться исключительно в общих целях обеспечения соблюдения законов и иных нормативных правовых актов, оказания платных медицинских услуг;
- При определении объема и содержания обрабатываемых персональных данных пациента Санаторий руководствуется положениями Конституции Российской Федерации и иными федеральными законами;
- Получение персональных данных может осуществляться как путем представления их самим пациентом, так и путем получения их из иных источников;
- Персональные данные пациента следует получать у него самого. Если персональные данные пациента возможно получить только у третьей стороны, то пациент должен быть уведомлен об этом заранее и от него должно быть получено письменное согласие. Санаторий должен сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствиях отказа пациента дать письменное согласие на их получение;
- Санаторий не имеет право получать и обрабатывать персональные данные пациента о его политических, религиозных и иных убеждениях и частной жизни;
- Санаторий не имеет право получать и обрабатывать персональные данные пациента о его членстве в общественных объединениях или его профсоюзной деятельности, за исключением случаев, предусмотренных федеральным законом.

3.2 Использование персональных данных возможно только в соответствии с целями, определившими их получение.

3.3 Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации прав и свобод граждан Российской Федерации. Ограничение прав граждан Российской Федерации на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с действующим законодательством.

3.4 Передача персональных данных возможна только с согласия пациента или в случаях, прямо предусмотренных законодательством.

3.4.1 При передаче персональных данных пациента Санаторий должен соблюдать следующие требования:

– Не сообщать персональные данные пациента третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента, а также в случаях, установленных федеральным законом;
– Не сообщать персональные данные пациента в коммерческих целях без его письменного согласия;
– Предупредить лиц, получающих персональные данные пациента о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены, и требовать от этих лиц подтверждения того, что это правило соблюдено. Лица, получающие персональные данные пациента, обязаны соблюдать режим секретности (конфиденциальности). Данное положение не распространяется на обмен персональными данными пациентов в порядке, установленным федеральными законами;
– Разрешать доступ к персональным данным пациентов только специально уполномоченным лицам, определенным приказом по организации, при этом указанные лица должны иметь право получать только те персональные данные пациента, которые необходимы для выполнения конкретных функций;

3.4.2 Передача персональных данных от держателя или его представителей внешнему потребителю может допускаться в минимальных объемах и только в целях выполнения задач, соответствующих объективной причине сбора этих данных.
3.4.3 При передаче персональных данных пациента (в том числе и в коммерческих целях) за пределы организации Санаторий не должен сообщать эти данные третьей стороне без письменного согласия пациента, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью пациента или в случаях, установленных федеральным законом.

3.5 Все меры конфиденциальности при сборе, обработке и хранении персональных данных распространяются как на бумажные, так и на электронные (автоматизированные) носители информации.
3.6 Не допускается отвечать на вопросы, связанные с передачей персональной информации по телефону или факсу.
3.7 Хранение персональных данных должно происходить в порядке, исключающем их утрату или их неправомерное использование.

4. ПОЛУЧЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТОВ

4.1 Получение персональных данных пациента преимущественно осуществляется путем предоставления их пациентом на основании его письменного согласия при посещении Санатория.
4.2 В случае необходимости проверки персональных данных пациента Санаторий должен заблаговременно сообщить пациенту о целях, предполагаемых источниках и способах получения персональных данных, а также о характере подлежащих получению персональных данных и последствия отказа пациента дать письменное согласие на их получение.

5. ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ

5.1 Внутренний доступ:
5.1.1 Право доступа к персональным данным пациента имеют:
–директор Санатория;
– Сам пациент, носитель данных;
– Другие сотрудники Санатория при выполнении ими своих служебных обязанностей.
5.1.2 Перечень лиц, имеющих доступ к персональным данным пациента, определяется приказом директора Санатория.
5.2 Внешний доступ:
5.2.1 Надзорно-контролирующие органы имеют доступ к информации только в сфере своей компетенции.
5.2.2 Персональные данные пациента могут быть предоставлены родственникам или членам его семьи только с письменного разрешения самого пациента.

6. ЗАЩИТА ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1 Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и производственной деятельности Санатория.
6.2 Защита персональных данных пациента от неправомерного их использования или утраты должна быть обеспечена Санаторием за счет его средств в порядке, установленном федеральным законом.

6.3 Внутренняя защита:

6.3.1 Для обеспечения внутренней защиты персональных данных необходимо соблюдать ряд мер:

– Ограничение и регламентация состава работников, функциональные обязанности которых требуют доступа к персональным данных сотрудников.
– Строгое избирательное и обоснованное распределение документов и информации между работниками;
– Рациональное размещение рабочих мест работников, при которым исключалось бы бесконтрольное использование защищаемой информации;
– Знание работниками требований нормативно-методических документов по защите информации и сохранения тайны;
– Наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
– Определение и регламентация состава работников, имеющих право доступа (входа) в помещение, в котором находится вычислительная техника;
– Организация порядка уничтожения информации;
– Своевременное выявление нарушения требований разрешительной системы доступа работниками подразделения;
– Воспитательная и разъяснительная работа с сотрудниками подразделения по предупреждению утраты ценных сведений при работе с конфиденциальными документами.

6.3.2 Защита персональных данных пациентов на электронных носителях. Все документы, содержащие персональные данные пациента, должны иметь ограниченный доступ.

6.4 Внешняя защита:

6.4.1 Для обеспечения внешней зашиты персональных данных пациентов необходимо соблюдать ряд мер:

– Порядок приема, учета и контроля деятельности посетителей;
– Технические средства охраны (электронный ключ, сигнализации);
– Порядок охраны территории, зданий, помещений.

6.5 Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны не разглашать персональные данные пациентов.

6.6 Кроме мер защиты персональных данных, установленных законодательством, Санаторий, сотрудники Санатория, пациенты и их представители могут вырабатывать совместные меры защиты персональных данных пациентов.

6.7 Оператор, допустивший утечку персональных данных, обязан в течение 24 часов сообщить об этом в Роскомнадзор, а в течение 72 часов предоставить в ведомство результаты внутреннего расследования инцидента с указанием причины и виновных лиц.

6.8 Оператор обязан сообщить субъекту персональных данных или его представителю информацию о наличии персональных данных, относящихся к соответствующему субъекту персональных данных, а также предоставить возможность ознакомления с этими персональными данными при обращении субъектов персональных данных или его представителя, в течение десяти рабочих дней с момента получения запроса субъекта персональных данных или его представителя.

7. ПРАВА И ОБЯЗАННОСТИ ПАЦИЕНТОВ

7.1 В целях защиты персональных данных, хранящихся в Санатории, пациент имеет право:

– Требовать исключения или исправления неверных или неполных данных;
– Получать доступ к своим персональным данным, включая право на получение копии любой записи, содержащей персональные данные, только с письменного заявления на имя директора Санатория;

– Персональные данные оценочного характера дополнить заявлением, содержащим его собственную точку зрения;
– Определять своих представителей для защиты своих персональных данных;
– На сохранение и защиту своей личной жизни и семейной тайны.

7.2 Пациент обязан передавать Санаторию комплекс достоверных, документированных персональных данных, а также своевременно сообщать об изменениях своих персональных данных.

7.3 Пациент ставит Санаторий в известность об изменении фамилии, имени, отчества, даты рождения, что получает отражение в медицинской документации на основании представленных документов.

8. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ ПЕРСОНАЛЬНЫХ ДАННЫХ ПАЦИЕНТА

8.1 Директор Санатория, разрешающий доступ к конфиденциальному документу, несет персональную ответственность за данное разрешение.

8.2 Каждый сотрудник Санатория, получающий для работы конфиденциальный документ, несет единоличную ответственность за сохранность носителя и конфиденциальность информации.

8.3 Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных пациента, несут дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами.