«УТВЕРЖДАЮ»

Директор ООО «Центр врачебной практики и реабилитации»

_____ Буруцкая О.В.

10 января 2022 года

Положение
об обработке персональных данных пациентов

1. Общие положения

1.1. Настоящее Положение устанавливает порядок действий, 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 (предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных граждан, обращающихся за получением медицинской помощи, медико-социальных услуг (далее – пациентов) в ООО «Центр врачебной практики и реабилитации» (далее – Организация).

1.2. Цель настоящего Положения – защита персональных данных пациентов, обращающихся в Организацию от несанкционированного доступа и разглашения. Персональные данные всегда являются конфиденциальной, строго охраняемой информацией.

1.3. Положение разработано в соответствии с Конституцией Российской Федерации, Федеральным законом № 323-ФЗ от 21.11.2011 г. «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом № 152-ФЗ от 27.07.2006 г. «О персональных данных», Постановлением Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и других действующих нормативно-правовых актов Российской Федерации.

1.4. Все изменения в положение вносятся соответствующим приказом.

1.5. Персональные данные пациентов относятся к категории конфиденциальной информации. Конфиденциальность, сохранность и защита персональных данных обеспечивается отнесением их к служебной, профессиональной и врачебной тайне.

1.6. При определении объема и содержания персональных данных пациентов медицинская организация руководствуется настоящим Положением, Конституцией РФ, иными федеральными законами.

2. Понятие персональных данных

2.1. Персональные данные пациентов - информация, полученная медицинской организацией при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг, а также информация полученная

в процессе лечения (сведения о фактах, событиях и обстоятельствах частной жизни пациента, а также биометрических данных, сведения о состоянии его здоровья, в целях выполнения функций учреждения здравоохранения: оказания доврачебной, первичной врачебной медико-санитарной помощи, специализированной медицинской помощи).

2.2. К персональным данным пациента относятся:

- анкетные данные (фамилия, имя, отчество, число, месяц, год рождения и др.);

- паспортные данные;

- адрес регистрации;

- адрес места жительства;

- данные о состоянии здоровья;

- иные данные, необходимые для оказания доврачебной, первичной врачебной медико-санитарной помощи, специализированной медицинской помощи.

2.3. Все персональные сведения о пациентах работники организации могут получить только от них самих. В случаях, когда работники организации могут получить необходимые персональные данные пациентов только у третьего лица, необходимо уведомить об этом и пациентов и получить от них письменное согласие.

2.4. Работники организации обязаны 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.

2.5. Представление пациентом подложных документов или ложных сведений при оформлении документов для оказания медицинской помощи является основанием для отказа в оказании медицинской помощи.

2.6. Работник ответственный за сбор информации, при получении персональных данных пациента обязан проверить достоверность сведений, сверяя данные, предоставленные пациентом, с имеющимися у пациента документами.

2.7 Работник ответственный за сбор информации при оформлении медицинской документации использует только оригиналы паспортов, СНИЛС и полисов ОМС пациентов в их присутствии. Запрещается снимать копии документов любым способом.

2.8. Персональные данные являются строго конфиденциальными, и не могут быть использованы работниками организации в личных целях.

2.9. Ответственные лица, получившие доступ к персональным данным пациентов, обязаны хранить эти данные в тайне в течение установленного законом срока.

2.10. Режим конфиденциальности персональных данных снимается в случаях обезличивания или по истечении соответствующего срока хранения.

2.11. В случае выявления неправомерных действий с персональными данными пациента:

- пациент или его законный представитель обращается к главному врачу с заявлением;

- главный врач издает приказ о проведении служебного расследования если в ходе служебного расследования подтвердился факт неправомерных действий с персональными данными, то работник, ответственный за получение персональных данных, несет ответственность в установленном законом порядке.

3. Носители персональных данных

3.1. Бумажные носители персональных данных:

- амбулаторная медицинская карта пациента;

- история болезни;

- прочая медицинская документация;

- санаторно-курортные карты, справки о состоянии здоровья;

- талон амбулаторного пациента;

- результаты медицинских исследований;

- льготные рецептурные бланки;

- выписки из амбулаторных карт и историй болезни;

- счет за медицинскую помощь по ОМС.

3.2. Электронные носители персональных данных – информационные системы баз данных.

3.3. Персональные данные на бумажных носителях (амбулаторные карты, истории болезни, другая медицинская документация) хранятся в регистратурах, помещениях архивов, в кабинетах с режимом сохранности.

3.4. При осуществлении амбулаторного приема, обработке медицинской документации, составленной по итогам осмотров, документы, находящиеся в работе у врачей, среднего медицинского персонала, администраторов, оператора ПК, экономиста могут находиться на рабочих столах или в специальных папках только в течение рабочего дня. По окончании рабочего дня данные документы должны убираться в запирающиеся шкафы, регистратуры.

3.5. Персональные данные на электронных носителях защищены паролем доступа, доступ к специализированным информационным системам обрабатывающими персональные данные предоставляется с использованием персонального идентификатора и пароля, право на использование персональных данных имеют только работники, ответственные за обработку персональных данных.

4. Перечень действий с персональными данными и способы обработки персональных данных

4.1. С персональными данными пациента могут осуществляться действия, предусмотренные п. 1 настоящего Положения.

Организация формирует массивы персонифицированных данных для передачи во внешние организации (страховые медицинские организации, территориальный фонд ОМС), данные передаются по защищенным каналам связи (VIPnet).

4.2. Персональные данные обрабатываются:

- для проведения оценки состояния здоровья пациента – полная обработка данных в соответствии с законодательством Российской Федерации;

- других мероприятий, возникающих в процессе выполнения функций организации, в соответствии с законодательством Российской Федерации.

5. Хранение и использование персональных данных пациентов

5.1. Персональные данные пациентов хранятся на бумажных и электронных носителях, в специально предназначенных для этого помещениях.

5.2. В процессе хранения персональных данных пациентов должны обеспечиваться:

- требования нормативных документов, устанавливающих правила хранения конфиденциальных сведений;

- сохранность имеющихся данных, ограничение доступа к ним, в соответствии с законодательством РФ и настоящим Положением;

- контроль над достоверностью и полнотой персональных данных, их регулярное обновление и внесение по мере необходимости соответствующих изменений.

5.3. Ответственное лицо 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.

5.4. При передаче персональных данных пациентов работник организации 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.

5.5. Все сведения о передаче персональных данных пациентов учитываются для контроля правомерности использования данной информации лицами, ее получившими.

6. Право доступа к персональным данным пациентов имеют

6.1. Полный внутренний доступ (доступ внутри организации):

- главный врач, заведующий отделением – к персональным данным пациентов в соответствии со спецификой оказываемых услуг;

- врачи и медицинский персонал – к персональным данным пациентов при оказании медицинских услуг;

- сам пациент, носитель данных.

6.2. Частичный внутренний доступ (доступ внутри организации) к тем данным, которые необходимы для выполнения конкретных функций:

- старший администратор; администраторы; оператор ПК; системный администратор; экономист; главный бухгалтер, директор.

6.3. Внешний доступ. Массовые потребители персональных данных вне организации государственные и негосударственные функциональные структуры:

- страховые медицинские организации;

- территориальный фонд ОМС;

- органы социального страхования;

- органы дознания и следствия, суда, прокуратуры.

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

7.1. Организация режима безопасности технических средств задействованных в обработке персональных данных, информационных систем персональных данных, средств вычислительной техники, а также охрана помещений, в которых ведется работа с персональными данными должны обеспечивать сохранность носителей персональных данных и средств защиты информации, а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

7.2. 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.

8. Обязанности медицинской организации по хранению и защите персональных данных пациентов

8.1. Руководитель организации обязан за счет средств организации обеспечить защиту персональных данных пациентов от неправомерного использования или утраты в порядке, установленном законодательством РФ.

8.2. Руководитель организации обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами.

8.3. Ответственное лицо обязано ознакомить работников с настоящим Положением и их правами в области защиты персональных данных под роспись.

8.4. Ответственное лицо обязано осуществлять передачу персональных данных пациентов только в соответствии с настоящим Положением и законодательством РФ.

8.5. Ответственное лицо обязано 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.

8.6. Ответственное лицо не вправе получать и обрабатывать персональные данные пациентов о их политических, религиозных и иных убеждениях и личной жизни.

8.7. Ответственное лицо не вправе предоставлять персональные данные пациентов в коммерческих целях без их письменного согласия.

8.8. Ответственное лицо обязано обеспечить пациентам свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

8.9. Ответственное лицо обязано по требованию пациентов предоставить им полную информацию о их персональных данных и обработке этих данных.

9. Меры по обеспечению безопасности персональных данных при их обработке

9.1. Ответственное лицо при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

9.2. Обеспечение безопасности персональных данных достигается, в частности:

- определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

- применением организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, необходимых для выполнения требований к защите персональных данных, исполнение которых обеспечивает установленные Правительством Российской Федерации уровни защищенности персональных данных;

- применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

- оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;

- учетом машинных носителей персональных данных;

- обнаружением фактов несанкционированного доступа к персональным данным и принятием мер, в том числе мер по обнаружению, предупреждению и ликвидации последствий компьютерных атак на информационные системы персональных данных и по реагированию на компьютерные инциденты в них;

- восстановлением, по возможности, персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

- установлением правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечением регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных;

- контролем за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных.

9.3. Использование и хранение персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, их уничтожения, изменения, блокирования, копирования, предоставления, распространения.

10. Соблюдение врачебной тайны

10.1. Сведения о факте обращения пациента за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну.

10.2. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при исполнении, должностных обязанностей, за исключением случаев, предусмотренных законодательством.

10.3. Разглашение сведений, составляющих врачебную тайну, другим гражданам, в том числе должностным лицам, в целях медицинского обследования и лечения пациента, проведения научных исследований, их опубликования в научных изданиях, использования в учебном процессе и в иных целях допускается с письменного согласия гражданина или его законного представителя. Согласие на разглашение сведений, составляющих врачебную тайну, может быть выражено также в информированном добровольном согласии на медицинское вмешательство.

10.4. После смерти гражданина допускается разглашение сведений, составляющих врачебную тайну, супругу (супруге), близким родственникам (детям, родителям, усыновленным, усыновителям, родным братьям и родным сестрам, внукам, дедушкам, бабушкам) либо иным лицам, указанным гражданином или его законным представителем в письменном согласии на разглашение сведений, составляющих врачебную тайну, или информированном добровольном согласии на медицинское вмешательство, по их запросу, если гражданин или его законный представитель не запретил разглашение сведений, составляющих врачебную тайну.

10.5. Предоставление сведений, составляющих врачебную тайну, без согласия гражданина или его законного представителя допускается:

- в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю, с учетом положений пункта 1 части 9 стать 20 настоящего Федерального закона;

- при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

- по запросу органов дознания и следствия, суда в связи с проведением расследования или судебным разбирательством, по запросу органов прокуратуры в связи с осуществлением ими прокурорского надзора, 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, а также в связи с исполнением осужденным обязанности пройти лечение от наркомании и медицинскую и (или) социальную реабилитацию;

- в случае оказания медицинской помощи несовершеннолетнему в соответствии с пунктом 2 части 2 статьи 20 настоящего Федерального закона, а также несовершеннолетнему, не достигшему возраста, установленного частью 2 статьи 54 настоящего Федерального закона, для информирования одного из его родителей или иного законного представителя;

- в целях информирования органов дознания и следствия:

1) о поступлении пациента, в отношении которого имеются достаточные основания полагать, что вред его здоровью причинен в результате противоправных действий,

2) о поступлении пациента, который по состоянию здоровья, возрасту или иным причинам не может сообщить данные о своей личности;

3) о смерти пациента, личность которого не установлена;

4) 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;

5) в целях осуществления учета и контроля в системе обязательного социального страхования.

11. Права пациентов на защиту их персональных данных

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

- получать полную информацию о своих персональных данных и их обработке;
- определять своих представителей для защиты своих персональных данных;
- на доступ к относящимся к нему медицинских данных 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.

11.2. 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.

12. Порядок уничтожения, уточнения и блокирования персональных данных

12.1. В случае выявления неправомерной обработки персональных данных при обращении пациентов работник организации обязан осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этим пациентам, с момента такого обращения на период проверки.

12.2. В случае выявления неточных персональных данных при обращении пациентов работник организации обязан 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.

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

12.4. В случае поступления требования пациента о прекращении предоставления его персональных данных передача (предоставление, доступ) персональных данных, разрешенных таким пациентом для обработки, должна быть прекращена.
Действие согласия пациента на обработку персональных данных прекращается с момента поступления в медицинскую организацию указанного требования.
12.5. В случае выявления неправомерной обработки персональных данных, осуществляемой работником организации, работником организации в срок, не превышающий трех рабочих дней с даты этого выявления, обязан прекратить неправомерную обработку персональных данных.
12.6. В случае если обеспечить правомерность обработки персональных данных невозможно, работник организации в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные.
12.7. Об устранении допущенных нарушений или об уничтожении персональных данных работник организации обязан уведомить пациентов.
12.8. В случае достижения цели обработки персональных данных работник организации обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.
12.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанных в п. 12.4-12.8 настоящего Положения, работник организации осуществляет блокирование таких персональных данных и обеспечивает уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

13. Ответственность за нарушение норм, регулирующих обработку персональных данных пациентов

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.

14. Порядок взаимодействия с Роскомнадзором по фактам неправомерной или случайной передачи персональных данных.

14.1. Организация обязана с момента выявления инцидента уведомить территориальный орган Роскомнадзора в течение 24 часов относительно:

- ✓ факта произошедшего инцидента;
- ✓ предполагаемых его причин и вреда;
- ✓ принятых мер по устранению последствий инцидента, а также предоставить сведения о лице, которое оно уполномочивает контактировать с сотрудниками территориального Роскомнадзора по этому инциденту.

14.2. В течение 72 часов необходимо:

- ✓ отчитаться перед территориальным органом Роскомнадзора о результатах внутреннего расследования по факту инцидента;

- ✓ предоставить (при наличии) сведения о виновных лицах.

14.3 На все поступающие письменные запросы территориального органа Роскомнадзора ответ дается в течение 10 рабочих дней с даты получения.

15. Заключительные положения

15.1. Настоящее Положение вступает в силу с момента его подписания директором и действует бессрочно, до замены его новым положением.
15.2. Организация обеспечивает неограниченный доступ к настоящему документу.
15.3. Настоящее Положение доводится до сведения всех работников персонально под роспись.