

Приложение №1
к приказу от 19.04.2019г. № 87/од



Положение
о защите, хранении, обработке и передаче персональных пациентов (клиентов)
Государственного унитарного предприятия Республики Крым
«Поликлиника медицинских осмотров»

1. Общие положения

1.1. Настоящее Положение регламентируется Конституцией Российской Федерации, Трудовым кодексом РФ, 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 (далее - Федеральный закон) и другими нормативными правовыми актами.

1.2. **Персональные данные пациента (клиента)** - информация, полученная медицинской организацией при первоначальном поступлении пациента, при заключении с пациентом договора на оказание медицинских услуг; а также информация, полученная в процессе оказания платных медицинских услуг.

1.3. К персональным данным пациента (клиента) относятся: фамилия, имя, отчество; год рождения; месяц рождения; дата рождения; место рождения; адрес; профессия; состояние здоровья; паспортные данные, гражданство, данные свидетельств о браке, данные пенсионных страховых свидетельств, данные миграционных карт, данные видов на жительство и разрешений на временное проживание, данные документов, подтверждающих инвалидность, персональный номер телефона.

1.4. Все персональные сведения пациентах (клиентах) медицинская организация может получить только от них самих. В случаях, когда медицинская организация может получить необходимые персональные данные пациентов (клиентов) только у третьего лица, медицинская организация должна уведомить об этом пациентов (клиентов) и получить от них письменное согласие.

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

1.6. Персональные данные пациентов (клиентов) являются конфиденциальной информацией и не могут быть использованы медицинской организацией или любым иным лицом в личных целях.

1.7. При определении объема и содержания персональных данных пациентов (клиентов) медицинская организация руководствуется настоящим Положением, Конституцией РФ, Трудовым кодексом РФ, иными федеральными законами.

1.8. Медицинская организация разрабатывает меры защиты персональных данных пациентов (клиентов).

1.9. Пациенты (клиенты) не должны отказываться от своих прав на сохранение и защиту тайны.

2. Хранение, обработка и передача персональных данных пациентов (клиентов)

2.1. Обработка персональных данных пациентов (клиентов) осуществляется в целях обеспечения соблюдения законов и иных нормативных правовых актов.

2.2. Персональные данные пациентов (клиентов) хранятся в регистратуре Государственного унитарного предприятия Республики Крым «Поликлиника медицинских осмотров» на бумажных носителях с ограниченным доступом.

Право доступа к персональным данным пациентов (клиентов) имеют:

- руководитель медицинской организации;
- главный бухгалтер медицинской организации;
- сотрудники регистратуры медицинской организации

2.3. Сотрудники регистратуры медицинской организации вправе передавать персональные данные работников в бухгалтерию медицинской организации в случаях, установленных законодательством, необходимых для исполнения обязанностей работников бухгалтерии.

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

2.5. При передаче персональных данных пациентов (клиентов) 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.

2.6. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных пациентов (клиентов), определяются должностными инструкциями.

2.7. Все сведения о передаче персональных данных пациентов (клиентов) учитываются для контроля правомерности использования данной информации лицами, ее получившими.

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

3.1. 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.

3.2. 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.

3.3. Кроме указанных мер по специальному оборудованию и охране помещений, в которых осуществляется хранение персональных данных, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

4. Обязанности медицинской организации по хранению и защите персональных данных пациентов (клиентов)

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

4.2. 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. К таким мерам могут, в частности, относиться:

1) назначение ответственного за организацию обработки персональных данных;

2) издание документов, определяющих его политику в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

3) применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

4) осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

5) оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом;

6) ознакомление работников медицинской организации, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

4.3. Медицинская организация обязана ознакомить работников и их представителей с настоящим Положением и их правами в области защиты персональных данных под расписку.

4.4. Медицинская организация обязана осуществлять передачу персональных данных пациентов (клиентов) только в соответствии с настоящим Положением и законодательством РФ.

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

4.6. Медицинская организация не вправе получать и обрабатывать персональные данные пациентов (клиентов) о их политических, религиозных и иных убеждениях и частной жизни.

4.7. Медицинская организация не вправе предоставлять персональные данные пациентов (клиентов) в коммерческих целях без их письменного согласия.

4.9. Медицинская организация обязана обеспечить пациентам (клиентам) свободный бесплатный доступ к своим персональным данным, включая право на получение копий любой записи, содержащей их персональные данные, за исключением случаев, предусмотренных законодательством.

4.10. Медицинская организация обязана по требованию пациентов (клиентов) предоставить им полную информацию о их персональных данных и обработке этих данных.

5. Права пациентов (клиентов) на защиту их персональных данных

5.1. Пациенты (клиенты) 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 нему 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 (клиентов), пациенты (клиенты) 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 (клиентов), обо всех произведенных в них исключениях, исправлениях или дополнениях.

5.2. Если пациенты (клиенты) 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. Порядок уничтожения, блокирования персональных данных

6.1. В случае выявления неправомерной обработки персональных данных при обращении пациентов (клиентов) медицинская организация обязана осуществить блокирование неправомерно обрабатываемых персональных данных, относящихся к этим пациентам (клиентам), с момента такого обращения на период проверки.

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

6.3. В случае подтверждения факта неточности персональных данных медицинская организация на основании сведений, представленных пациентами (клиентами), или иных необходимых документов обязана уточнить персональные данные в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

6.4. В случае выявления неправомерной обработки персональных данных, осуществляемой медицинской организацией, медицинская организация в срок, не превышающий трех рабочих дней с даты этого выявления, обязана прекратить неправомерную обработку персональных данных.

6.5. 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, обязана уничтожить такие персональные данные.

6.6. Об устранении допущенных нарушений или об уничтожении персональных данных медицинская организация обязана уведомить пациентов (клиентов).

6.7. В случае достижения цели обработки персональных данных медицинская организация обязана прекратить обработку персональных данных и уничтожить персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных, если

иное не предусмотрено трудовым договором.

6.8. В случае отзыва пациентами (клиентами) 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 с даты поступления указанного отзыва.

6.9. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 6.4-6.8 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.

7. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных пациентов (клиентов)

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

7.2. Моральный вред, причиненный пациентам (клиентам) 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 пациентами (клиентами) убытков.

8. Заключительные положения

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

8.2. Медицинская организация обеспечивает неограниченный доступ к настоящему документу.

8.3. Настоящее Положение доводится до сведения всех работников персонально под роспись.