

Положение о порядке обработки и обеспечении безопасности персональных данных Потребителей

1. Общие положения

1.1. Положение об обработке и защите персональных данных Потребителей (далее - Положение) издано и применяется ООО «ЭКМЕД» в соответствии с п. 2 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

1.2. Настоящее Положение определяет порядок получения, обработки, учёта, накопления, хранения и защиты от несанкционированного доступа и разглашения сведений, составляющих персональные данные Потребителей ООО «ЭКМЕД» (далее - «оператор»),

1.3. Обработка персональных данных пациентов организована оператором на принципах:

1.3.1. законности и справедливости;

1.3.2. обработки только персональных данных, которые отвечают целям их обработки;

1.3.3. соответствия содержания и объема обрабатываемых персональных данных заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки;

1.3.4. недопустимости объединения баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.

1.3.5. обеспечения точности персональных данных, их достаточности, а в необходимых случаях и актуальности по отношению к целям обработки персональных данных. Оператор принимает необходимые меры либо обеспечивает их принятие по удалению или уточнению неполных, или неточных данных;

1.3.6. хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели обработки персональных данных.

1.4. Обработка персональных данных пациентов оператором осуществляется с соблюдением принципов и правил, предусмотренных Конституцией РФ, Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.11.2010 № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации», Федеральным законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации», Федеральным законом от 22.10.2004 № 125-ФЗ «Об архивном деле в Российской Федерации», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства РФ от 11 мая 2023 № 736 «Об утверждении Правил предоставления медицинскими организациями платных медицинских услуг» и настоящим Положением.

1.5. При обработке персональных данных оператор применяет правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

2. Понятие, сбор и обработка персональных данных

2.1. Под персональными данными Потребителей 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 ДМС, паспортные данные, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью, данные о составе семьи, прочие сведения, которые могут идентифицировать человека. Персональные данные Потребителей относятся к специальной категории персональных данных, обработка таких персональных данных должна осуществляться лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну. Персональные данные Потребителей 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.

2.2. Обработка персональных данных Потребителей - 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 пациентов.

2.3. Целью обработки персональных данных Потребителей является обеспечения соблюдения законов и иных нормативных правовых актов, установление медицинского диагноза и оказания медицинских услуг.

2.4. Потребитель дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку персональных данных даётся в письменной форме. Согласие Потребителя на обработку его персональных данных должно храниться вместе с его иной медицинской документацией. Обработка персональных данных Потребителей 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:

2.4.1. 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.

2.4.2. при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений;

2.4.3. 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;

2.4.4. 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;

2.4.5. 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;

2.4.6. 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;

2.4.7. в целях расследования несчастного случая на производстве и профессионального заболевания;

2.4.8. 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;

2.4.9. в целях осуществления учета и контроля в системе обязательного социального страхования;

2.4.10. 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».

2.5. Согласие на обработку персональных данных может быть отозвано Потребителем. 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.

2.6. Все персональные данные Потребителя следует получать у него самого. Персональные данные могут быть получены оператором от лица, не являющегося субъектом персональных данных, при условии предоставления оператору подтверждения 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».

2.7. В случае недееспособности Потребителя согласие на обработку его персональных данных дает его законный представитель.

2.8. Оператор не имеет право получать и обрабатывать персональные данные Потребителя о его политических, религиозных и иных убеждениях и частной жизни.

2.9. При передаче персональных данных Потребителя третьим лицам оператор должен соблюдать следующие требования:

2.9.1. не сообщать персональные данные Потребителя третьей стороне без письменного согласия Потребителя, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью Потребителя, а также в других случаях, предусмотренных Федеральным законодательством РФ;

2.9.2. предупредить лиц, получающих персональные данные Потребителя, 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 Потребителя, обязаны соблюдать режим секретности (конфиденциальности).

2.9.3. разрешать доступ к персональным данным Потребителей только специально уполномоченным лицам, при этом указанные лица должны иметь право получать только те персональные данные, которые необходимы для выполнения конкретных функций. Согласие Потребителя на передачу персональных данных не требуется, если законодательством РФ установлена обязанность предоставления оператором персональных данных.

2.10. Передача персональных данных Потребителя сотрудникам оператора для выполнения должностных обязанностей должна осуществляться только в объеме, необходимом для выполнения их работы.

2.11. Доступ к персональным данным Потребителей должен быть ограничен и регламентирован для предотвращения утечки данных. При хранении материальных носителей с персональными данными Потребителей должны соблюдаться условия, обеспечивающие сохранность персональных данных и исключающие несанкционированный доступ к ним.

2.12. Персональные данные вне Учреждения могут представляться в государственные и негосударственные функциональные структуры (внешний доступ):

- правоохранительные органы;
- страховые медицинские организации;
- органы социального страхования;
- вышестоящие подразделения муниципальных органов управления;
- управление Росздравнадзора по Удмуртской Республике;
- Министерство здравоохранения Удмуртской Республики;
- Территориальный фонд ОМС по Удмуртской республике;
- отделы опеки и попечительства;
- комиссии по делам несовершеннолетних и защите их прав;

2.13. Персональные данные Потребителя могут быть предоставлены его законному представителю, а также родственникам или членам его семьи, иным представителям только с письменного разрешения самого Потребителя либо его законного представителя.

2.14. Лица, получившие доступ к персональным данным пациентов, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

2.15. Хранение персональных данных Потребителей должно осуществляться в форме, позволяющей их идентифицировать.

2.16. Хранение персональных данных Потребителей должно происходить в порядке, исключающим их утрату или их неправомерное использование.

2.17. Срок хранения персональных данных Потребителей определяется целью обработки персональных данных. По истечению срока хранения или утраты цели обработки персональные данные подлежат уничтожению, обезличиванию или передаче в архив.

3. Права и обязанности оператора, пациентов в целях обеспечения защиты персональных данных пациентов

3.1. Оператор при обработке персональных данных обязан:

3.1.1. Принимать необходимые правовые, организационные и технические меры 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 пациентов.

3.1.2. Издавать документы, определяющие политику оператора в отношении обработки персональных данных Потребителей.

3.1.3. Осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Федеральному законодательству и принятыми в соответствии с ним нормативными правовыми актами, требованиям к защите персональных данных, локальным актам оператора.

3.1.4. Сообщать в порядке, предусмотренном статьей 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Потребителю или его представителю информацию о наличии персональных данных, относящихся к соответствующему Потребителю, а также предоставить возможность ознакомления с этими персональными данными безвозмездно при его обращении или обращении его представителя либо в течение тридцати дней с даты получения запроса субъекта персональных данных или его представителя.

3.1.5. Вносить в срок, не превышающий семи рабочих дней со дня предоставления Потребителем или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, необходимыми изменения в них. В срок, не превышающий семи рабочих дней со дня представления Потребителем или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить Потребителя или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого пациента были переданы.

3.1.6. В случае выявления неправомерной обработки персональных данных при обращении пациента или его представителя либо по запросу Потребителя или его представителя либо уполномоченного

органа по защите прав субъектов персональных данных осуществлять блокирование неправомерно обрабатываемых персональных данных, относящихся к этому Потребителю, с момента такого обращения или получения указанного запроса на период проверки.

3.1.7. В случае выявления неточных персональных данных при обращении Потребителя или его представителя либо по их запросу или по запросу уполномоченного органа по защите прав субъектов персональных данных осуществлять блокирование персональных данных, относящихся к этому Потребителю, с момента такого обращения или получения указанного запроса на период проверки, если блокирование персональных данных не нарушает права и законные интересы Потребителя или третьих лиц.

3.1.8. В случае подтверждения факта неточности персональных данных Потребителя уточнять персональные данные на основании сведений, представленных Потребителем или его представителем либо уполномоченным органом по защите прав субъектов персональных данных, или иных необходимых документов в течение семи рабочих дней со дня представления таких сведений и снять блокирование персональных данных.

3.1.9. Прекращать неправомерную обработку персональных данных в случае выявления неправомерной обработки персональных данных Потребителей, в срок, не превышающий трех рабочих дней с даты такого выявления, в случае, если обеспечить правомерность обработки персональных данных невозможно, оператор в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, обязан уничтожить такие персональные данные. Об устранении допущенных нарушений или об уничтожении персональных данных оператор обязан уведомить пациента или его представителя, а в случае, если обращение пациента или его представителя либо запрос уполномоченного органа по защите прав субъектов персональных данных были направлены уполномоченным органом по защите прав субъектов персональных данных, также указанный орган.

3.1.10. В срок, не превышающий семи рабочих дней со дня предоставления Потребителем или его представителем сведений, подтверждающих, что персональные данные являются неполными, неточными или неактуальными, оператор обязан внести в них необходимые изменения. В срок, не превышающий семи рабочих дней со дня представления пациентом или его представителем сведений, подтверждающих, что такие персональные данные являются незаконно полученными или не являются необходимыми для заявленной цели обработки, оператор обязан уничтожить такие персональные данные. Оператор обязан уведомить Потребителя или его представителя о внесенных изменениях и предпринятых мерах и принять разумные меры для уведомления третьих лиц, которым персональные данные этого Потребителя были переданы.

3.2. В целях обеспечения защиты персональных данных, хранящихся у оператора, Потребители имеют право:

3.2.1. на получение информации, касающейся обработки его персональных данных, в том числе содержащей:

- 1) подтверждение факта обработки персональных данных оператором;
- 2) правовые основания и цели обработки персональных данных;
- 3) цели и применяемые оператором способы обработки персональных данных;
- 4) наименование и место нахождения оператора, сведения о лицах (за исключением работников оператора), которые имеют доступ к персональным данным или которым могут быть раскрыты персональные данные на основании договора с оператором или на основании федерального законодательства РФ;

5) обрабатываемые персональные данные, относящиеся к соответствующему Потребителю, источник их получения, если иной порядок представления таких данных не предусмотрен федеральным законодательством РФ;

6) сроки обработки персональных данных, в том числе сроки их хранения;

7) иные сведения, предусмотренные федеральным законодательством РФ, за исключением случаев, предусмотренных ч. 8 ст. 14 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». Вышеуказанные сведения должны быть предоставлены Потребителю оператором в доступной форме, и в них не должны содержаться персональные данные, относящиеся к другим субъектам персональных данных, за исключением случаев, если имеются законные основания для раскрытия таких персональных данных.

3.2.2. Потребитель вправе требовать от оператора уточнения его персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

3.2.3. Сведения, указанные в п. 3.2.1. ст. 3.2. настоящего Положения, предоставляются Потребителю или его представителю оператором при обращении либо при получении запроса Потребителя или его представителя. Запрос должен содержать номер основного документа, удостоверяющего личность пациента или его представителя, сведения о дате выдачи указанного документа и выдавшем его органе, сведения, подтверждающие участие пациента в отношениях с оператором (номер договора, дата заключения договора, условное словесное обозначение и (или) иные сведения), либо сведения, иным образом подтверждающие факт обработки персональных данных оператором, подпись Потребителя или его

представителя. Запрос может быть направлен в форме электронного документа и подписан электронной подписью в соответствии с законодательством Российской Федерации.

3.2.4. В случае, если сведения, указанные в п. 3.2.1. ст. 3.2. настоящего Положения, а также обрабатываемые персональные данные были предоставлены для ознакомления Потребителю по его запросу, Потребитель вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 3.2.1. ст. 3.2. настоящего Положения, и ознакомления с такими персональными данными не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством или договором, стороной которого является Потребитель.

3.2.5. Потребитель вправе обратиться повторно к оператору или направить ему повторный запрос в целях получения сведений, указанных в п. 3.2.1. ст. 3.2. настоящего Положения, а также в целях ознакомления с обрабатываемыми персональными данными до истечения срока, указанного в п. 3.2.4. ст. 3.2. настоящего Положения, в случае, если такие сведения и (или) обрабатываемые персональные данные не были предоставлены ему для ознакомления в полном объеме по результатам рассмотрения первоначального обращения. Повторный запрос наряду со сведениями, указанными в п. 3.2.3. ст. 3.2. настоящего Положения, должен содержать обоснование направления повторного запроса.

3.2.6. Оператор вправе отказать Потребителю в выполнении повторного запроса, не соответствующего условиям, предусмотренным п. 3.2.4., п. 3.2.5. ст. 3.2. настоящего Положения. Такой отказ должен быть мотивированным. Обязанность представления доказательств обоснованности отказа в выполнении повторного запроса лежит на операторе.

3.2.7. Решение, порождающее юридические последствия в отношении Потребителя или иным образом затрагивающее его права и законные интересы, может быть принято на основании исключительно автоматизированной обработки его персональных данных только при наличии согласия в письменной форме пациента или в случаях, предусмотренных федеральными законами, устанавливающими также меры по обеспечению соблюдения прав и законных интересов пациентов. Оператор обязан разъяснить пациенту порядок принятия решения на основании исключительно автоматизированной обработки его персональных данных и возможные юридические последствия такого решения, предоставить возможность заявить возражение против такого решения, а также разъяснить порядок защиты пациентом своих прав и законных интересов. Оператор обязан рассмотреть указанное возражение в течение тридцати дней со дня его получения и уведомить пациента о результатах рассмотрения такого возражения.

3.2.8. Если Потребитель считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Положения или иным образом нарушает его права и свободы, пациент вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных, также пациент имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда, в судебном порядке.

4. Ответственность

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