

УТВЕРЖДЕНА
приказом Главного врача
НУЗ «Дорожная клиническая больница
на ст. Самара ОАО «РЖД»
от «22» 05 2015 г. № 2420/п

ПОЛИТИКА
НУЗ «Дорожная клиническая больница на ст. Самара
ОАО «РЖД»
в отношении обработки персональных данных

Оглавление

Общие положения:	3
1. Основания и цели обработки персональных данных	4
2. Принадлежность персональных данных	5
3. Перечень действий с персональными данными, описание способов обработки персональных данных	6
4. Принципы обработки персональных данных	7
5. Условия обработки персональных данных.....	8
6. Обеспечение конфиденциальности персональных данных	10
7. Прекращение обработки персональных данных.....	13
8. Права субъекта персональных данных и учреждения здравоохранения.....	14
9. Обеспечение безопасности персональных данных	15
10. Заключительные положения	17

Общие положения:

Настоящая Политика в отношении обработки персональных данных (далее по тексту – Политика) разработана в соответствии с Федеральным законом «О персональных данных» № 152-ФЗ от 27 июля 2006 года и действует в отношении всех персональных данных, обрабатываемых в НУЗ «Дорожная клиническая больница на ст. Самара ОАО «РЖД» (далее по тексту – учреждение здравоохранения).

Политика устанавливает:

- цели обработки персональных данных;
- принадлежность персональных данных;
- перечень действий с персональными данными и способы их обработки
- общие принципы обработки персональных данных;
- условия обработки персональных данных и обеспечение их конфиденциальности;
- права субъектов персональных данных и учреждения здравоохранения;
- меры по обеспечению безопасности персональных данных.

Политика определяет принципы, порядок и условия обработки персональных данных пациентов и работников учреждения, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни.

Положения настоящей Политики являются основой для организации работы по обработке персональных данных, разработки внутренних нормативных документов, регламентирующих порядок обработки персональных данных.

Положения настоящей Политики являются обязательными для исполнения всеми работниками учреждения, имеющими доступ к персональным данным.

Ознакомление Работников учреждения здравоохранения с положениями настоящей Политики осуществляется под роспись.

1. Основания и цели обработки персональных данных

1.1. Учреждение здравоохранения осуществляет обработку персональных данных в соответствии с требованиями следующих документов:

Конституции Российской Федерации, принята всенародным голосованием 12 декабря 1993 года;

Гражданского кодекса Российской Федерации от от 30 ноября 1994 года № 51-ФЗ;

Налогового кодекса Российской Федерации от 05 августа 2000 года № 117-ФЗ;

Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ;

Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»;

Федерального закона от 29 ноября 2010 года № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»;

Федерального закона от 24 июля 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования»;

Федерального закона от 10 января 2003 года № 17-ФЗ «О железнодорожном транспорте в Российской Федерации»;

Устава учреждения здравоохранения;

Лицензии на осуществление медицинской деятельности.

1.2. Обработка персональных данных осуществляется с целью: исполнения требований законодательства Российской Федерации; защиты законных прав и интересов граждан при оказании медицинской помощи и медицинских услуг, проведении медицинских осмотров и установления медицинского диагноза;

исполнения договорных обязательств перед учреждениями и организациями, заключившими договора на оказание медицинских услуг своим сотрудникам,

осуществления и выполнения, возложенных законодательством Российской Федерации, на оператора функций, полномочий и обязанностей по выполнению трудового законодательства, осуществления бухгалтерской и кадровой деятельности.

2. Принадлежность персональных данных

К персональным данным относится любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), обрабатываемая учреждением здравоохранения - Оператором персональных данных, для достижения заранее определенных целей.

2.1. В учреждении здравоохранения обрабатываются следующие персональные данные:

специальная категория персональных данных, касающейся состояния здоровья субъектов персональных данных, не являющихся сотрудниками оператора;

иная категория персональных данных сотрудников оператора.

2.2. Персональные данные принадлежат:

физическим лицам - гражданам Российской Федерации, проходящим медицинские осмотры, обследования, лечение;

работникам учреждения здравоохранения – гражданам Российской Федерации, состоящим в трудовых отношениях с учреждением здравоохранения.

3. Перечень действий с персональными данными, описание способов обработки персональных данных

Обработка персональных данных производится в смешанном (автоматизированном и неавтоматизированном) режиме.

Автоматизированная обработка персональных данных осуществляется в многопользовательском режиме с разграничением прав доступа, информация доступна лишь для строго определенных сотрудников.

Неавтоматизированная обработка персональных данных осуществляется работниками учреждения без использования средств автоматизации.

Перечень действий, осуществляемых с персональными данными:

сбор персональных данных;

запись персональных данных;

систематизация персональных данных;

накопление персональных данных;

хранение персональных данных;

уточнение (обновление, изменение) персональных данных;

использование персональных данных;

распространение персональных данных;

блокирование персональных данных;

уничтожение персональных данных.

4. Принципы обработки персональных данных

Обработка персональных данных в учреждении здравоохранения осуществляется на основе принципов:

законности заранее определенных конкретных целей и способов обработки персональных данных;

соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных;

соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

обеспечения надлежащей защиты персональных данных;

недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

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

уничтожения по достижении целей обработки персональных данных, если срок хранения персональных данных не установлен законодательством Российской Федерации, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект персональных данных;

обеспечения конфиденциальности обрабатываемых персональных данных.

Доступ к обрабатываемым персональным данным, предоставляется только тем работникам учреждения здравоохранения, которым он необходим в связи с исполнением ими трудовых обязанностей.

Работники учреждения здравоохранения, допущенные к обработке персональных данных, информируются об условиях и правилах обработки персональных данных, режимах защиты информационных систем персональных данных, порядке хранения материальных носителей персональных данных.

Работниками учреждения даются письменные обязательства о неразглашении персональных данных и конфиденциальной информации, соблюдении врачебной тайны.

5. Условия обработки персональных данных

Обработка персональных данных субъектов персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных, за исключением следующих случаев:

Обработка персональных данных субъектов проходящих медицинские осмотры, медицинские исследования и лечение осуществляется без согласия субъектов персональных данных в следующих случаях:

5.1. В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому, является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем;

обработка персональных данных необходима для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных, если получение согласия субъекта персональных данных невозможно;

обработка персональных данных осуществляется в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что обработка персональных данных осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным в соответствии с законодательством Российской Федерации сохранять врачебную тайну;

обработка персональных данных осуществляется в соответствии с законодательством о государственной социальной помощи, трудовым законодательством, законодательством Российской Федерации о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях;

обработка персональных данных осуществляется в соответствии с законодательством об обязательных видах страхования, со страховым законодательством.

5.2. В соответствии с требованиями Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ, Федерального закона от 10 января 2003 года № 17-ФЗ «О железнодорожном транспорте в Российской Федерации»:

обработка персональных данных осуществляется при проведении обязательных предварительных (при поступлении на работу) и периодических медицинских осмотров (обследований) для определения

пригодности работников для выполнения поручаемой работы и предупреждения профессиональных заболеваний.

5.3. В соответствии с требованиями Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» учреждение здравоохранения:

имеет право создавать локальные информационные системы, содержащие данные о пациентах и об оказываемых им медицинских услугах, с соблюдением установленных законодательством Российской Федерации требований о защите персональных данных и соблюдением врачебной тайны;

обязано организовывать и осуществлять медицинскую деятельность в соответствии с законодательными и иными нормативными правовыми актами Российской Федерации, в том числе порядками оказания медицинской помощи, и на основе стандартов медицинской помощи;

обязано вести медицинскую документацию в установленном порядке и представлять отчетность по видам, формам, в сроки и в объеме, которые установлены уполномоченным федеральным органом исполнительной власти;

Обработка персональных данных работников учреждения здравоохранения осуществляется без их согласия в соответствии с требованиями Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ, Федерального закона от 10 января 2003 года № 17-ФЗ «О железнодорожном транспорте в Российской Федерации» в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, получении образования и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

6. Обеспечение конфиденциальности персональных данных

В соответствии с требованиями Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных» Операторы и иные лица, получившие доступ к персональным данным, обязаны не раскрывать третьим лицам и не распространять персональные данные без согласия субъекта персональных данных, если иное не предусмотрено федеральным законом.

В соответствии с требованиями Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» сведения о факте обращения гражданина за оказанием медицинской помощи, состоянии его здоровья и диагнозе, иные сведения, полученные при его медицинском обследовании и лечении, составляют врачебную тайну. Не допускается разглашение сведений, составляющих врачебную тайну, в том числе после смерти человека, лицами, которым они стали известны при обучении, исполнении трудовых, должностных, служебных и иных обязанностей, за исключением случаев, установленных настоящим законом.

С письменного согласия гражданина или его законного представителя допускается 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;

В соответствии с требованиями статьи Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ при передаче персональных данных работника работодатель должен соблюдать следующие требования:

не сообщать персональные данные работника третьей стороне без письменного согласия работника, за исключением случаев, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами;

не сообщать персональные данные работника в коммерческих целях без его письменного согласия.

6.1. Передача персональных данных субъектов персональных данных проходящих медицинские осмотры, медицинские исследования и лечение третьим лицам без согласия субъекта персональных данных осуществляется в следующих случаях:

6.1.1. В соответствии с требованиями Федерального закона от 29 ноября 2010 № 326 «Об обязательном медицинском страховании в Российской Федерации» и договорами, заключаемыми субъектами

(работодателем) со страховыми компаниями, в целях ведения персонифицированного учета сведений о медицинской помощи, оказанной застрахованным лицам, осуществляется передача сведений о субъекте персональных данных в территориальные фонды ОМС, ДМС, негосударственные страховые компании.

6.1.2. В соответствии с требованиями Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»:

в целях проведения медицинского обследования и лечения гражданина, который в результате своего состояния не способен выразить свою волю;

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;

в случае оказания медицинской помощи несовершеннолетнему, для информирования одного из его родителей или иного законного представителя;

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;

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

в целях расследования несчастного случая на производстве и профессионального заболевания, а также несчастного случая с обучающимся во время пребывания в организации, осуществляющей образовательную деятельность;

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;

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

в целях осуществления контроля качества и безопасности медицинской деятельности в соответствии с настоящим Федеральным законом (в

Региональную дирекцию медицинского обеспечения, в Региональную врачебно-экспертную комиссию, в Центральную врачебно-экспертную комиссию).

медицинская организация обязана вести медицинскую документацию в установленном порядке и представлять отчетность по видам, формам, в сроки и в объеме, которые установлены уполномоченным федеральным органом исполнительной власти.

6.1.3. В соответствии с требованиями Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ, Федерального закона от 10 января 2003 года № 17-ФЗ «О железнодорожном транспорте в Российской Федерации» передача сведений о состоянии здоровья субъекта персональных данных осуществляется в учреждения и организации, в целях организации допуска к исполнению трудовых обязанностей.

6.2. Передача персональных данных работников учреждения здравоохранения без их согласия осуществляется в следующих случаях:

6.2.1. В соответствии с требованиями Трудового кодекса Российской Федерации от 30 декабря 2001 года № 197-ФЗ в случае, когда это необходимо в целях предупреждения угрозы жизни и здоровью работника, а также в других случаях, предусмотренных настоящим Кодексом или иными федеральными законами.

6.2.2. В соответствии с требованиями Налогового кодекса Российской Федерации от 05 августа 2000 года № 117-ФЗ представляются в налоговый орган по месту своего учета сведения о доходах физических лиц истекшего налогового периода и суммах начисленных, удержанных и перечисленных в бюджетную систему Российской Федерации за этот налоговый период.

6.2.3. В соответствии с требованиями Федерального закона от 24 июля 2009 года № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования и территориальные фонды обязательного медицинского страхования» представляется отчетность в орган контроля за уплатой страховых взносов по месту своего учета.

6.2.4. В соответствии с пунктом 5 статьи 19, пункта 1 статьи 21 Федерального закона от 21 ноября 2011 года № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» в целях информационного обеспечения пациентов в учреждении здравоохранения могут создаваться общедоступные источники персональных данных о врачах-специалистах (доска объявлений, информация на сайте и т.п.). В общедоступные источники персональных данных без согласия субъекта персональных данных могут включаться фамилия, имя, отчество, структурное подразделение, должность, сведения о квалификации врача-специалиста, стаж работы.

7. Прекращение обработки персональных данных

7.1. Прекращение автоматизированной обработки персональных данных субъектов персональных данных, проходящих медицинские осмотры, медицинские исследования и лечение в информационных системах персональных данных осуществляется:

по письменному требованию субъектов персональных данных, немедленно, после завершения производства расчетов за оказанные медицинские и медико-социальные услуги;

по истечению сроков хранения первичных медицинских документов и составляют от одного года до двадцати пяти лет.

7.2. Прекращение неавтоматизированной обработки персональных данных субъектов, проходящих медицинские осмотры, медицинские исследования и лечение, и уничтожение документов, содержащих персональные данные, осуществляется по истечению сроков хранения первичных медицинских документов, которые составляют от одного года до двадцати пяти лет, с момента оказания последней медицинской услуги в соответствии с требованиями приказов Министерства здравоохранения и бухгалтерской отчетности.

7.3. Прекращение автоматизированной обработки персональных данных работников учреждения в информационных системах персональных данных осуществляется:

при прекращении договорных отношений с работниками и физическими лицами;

по истечению сроков представления бухгалтерской отчетности.

7.4. Прекращение неавтоматизированной обработки персональных данных работников учреждения и уничтожение документов, содержащих персональные данные, осуществляется:

по истечению сроков хранения документов по личному составу и бухгалтерской отчетности, которые составляют до семидесяти пяти лет.

при ликвидации учреждения.

8. Права субъекта персональных данных и учреждения здравоохранения

8.1. Субъект персональных данных имеет право:

получать информацию, касающуюся обработки его персональных данных, в порядке, форме и сроки, установленные Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными, не являются необходимыми для заявленной цели обработки или используются в целях, не заявленных ранее при предоставлении субъектом персональных данных согласия на обработку персональных данных;

отозвать свое согласие на обработку персональных данных;

обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных.

8.2. Учреждение здравоохранения имеет право:

обрабатывать персональные данные субъекта персональных данных в соответствии с заявленной целью;

требовать от субъекта персональных данных предоставления достоверных персональных данных, необходимых для исполнения договора, оказания услуги, идентификации субъекта персональных данных, а также в иных случаях, предусмотренных Федеральным законодательством Российской Федерации;

обрабатывать персональные данные субъекта, предоставлять персональные данные субъекта третьим лицам без его согласия, если это предусмотрено Федеральным законодательством Российской Федерации;

поручать обработку персональных данных другим лицам с согласия субъекта персональных данных;

отказывать в предоставлении персональных данных в случаях предусмотренных законодательством.

9. Обеспечение безопасности персональных данных

Важнейшим условием реализации целей деятельности учреждения здравоохранения, является обеспечение необходимого и достаточного уровня защищенности информационных систем персональных данных, соблюдения конфиденциальности, целостности и доступности обрабатываемых персональных данных, сохранности материальных носителей сведений, содержащих персональные данные, на всех этапах работы с ними.

Обеспечение безопасности обрабатываемых персональных данных осуществляется с применением комплексной системы организационно-технических и правовых мероприятий по защите информации, с учетом требований законодательства Российской Федерации о персональных данных, принятых в соответствии с ним нормативных правовых актов. Система информационной безопасности непрерывно развивается и совершенствуется на базе требований стандартов информационной безопасности.

В целях организации и обеспечения безопасности персональных данных обеспечиваются следующие меры:

назначение должностных лиц, ответственных за организацию обработки и защиты персональных данных;

определение и оценка угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

разработка организационно-распорядительных документов по защите персональных данных;

ограничение круга должностных лиц, имеющих доступ к персональным данным;

ознакомление работников с требованиями федерального законодательства и нормативных документов по обработке и защите персональных данных;

реализация разрешительной системы доступа пользователей к информационным ресурсам, программно-аппаратным средствам обработки и защиты информации;

регистрация и учёт действий пользователей информационных систем персональных данных;

применение средств разграничения и контроля доступа к информации, информационным ресурсам, информационным системам, коммуникационным портам, устройствам ввода-вывода информации, съёмным машинным носителям и внешним накопителям информации;

реализация парольной защиты при осуществлении доступа пользователей к информационной системе персональных данных;

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

применение средств межсетевое экранирования;

осуществление антивирусного защиты, предотвращение внедрения вредоносных программ;

применение средств криптографической защиты информации для обеспечения безопасности персональных данных при передаче по открытым каналам связи;

учет и хранение материальных носителей персональных данных в условиях, обеспечивающих их сохранность;

резервное копирование информации и восстановления персональных данных;

централизованное управление системой защиты персональных данных;

обучение работников, использующих средства защиты информации, применяемые в информационных системах персональных данных, правилам работы с ними;

оценка эффективности принимаемых мер по обеспечению безопасности персональных данных;

обнаружение фактов несанкционированного доступа к персональным данным и принятие мер;

размещение технических средств обработки персональных данных, в пределах границ охраняемой территории;

обеспечение пропускного режима на территорию учреждения;

обеспечение контроля за порядком обработки персональных данных и обеспечения их безопасности, поддержания установленного уровня защищенности информационных систем персональных данных.

10. Заключительные положения

НУЗ «Дорожная клиническая больница на ст. Самара ОАО «РЖД», а также его работники в соответствии с законодательством Российской Федерации несут гражданско-правовую, административную и уголовную ответственность за несоблюдение принципов и условий обработки персональных данных, а также за разглашение или незаконное использование персональных данных.

Настоящая Политика является общедоступной и размещается в открытом доступе (на официальном сайте, стендах информирования и т.п.) или иным образом обеспечивается неограниченный доступ к данной Политике.