УТВЕРЖДАЮ
Главный врач
ЧУЗ «КБ «РЖД-Медицина»
г. Астрахань
_____ В.А.Бондарев
11 января 2021
М.П.

ПОЛОЖЕНИЕ
о защите, хранении, обработке и передаче персональных данных работников и пациентов

Частное учреждение здравоохранения
«Клиническая больница «РЖД-Медицина» города «Астрахань»

1. Общие положения

1.1. Настоящее Положение регламентируется Конституцией Российской Федерации, Трудовым кодексом РФ, Федеральным законом "Об информации, информационных технологиях и о защите информации" N 149-ФЗ от 27.07.2006 года, 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 работника** - информация, необходимая для ЧУЗ «КБ «РЖД-Медицина» г. Астрахань» (далее - медицинская организация) в связи с трудовыми отношениями и касающаяся конкретного работника.

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

1.3. К персональным данным работника относятся:
- фамилия, имя, отчество;
- дата рождения;
- гражданство;
- номер страхового свидетельства;
- ИНН;
- знание иностранных языков;
- данные об образовании (номер, серия дипломов, год окончания);
- данные о приобретенных специальностях;
- семейное положение;
- данные о членах семьи (степень родства, Ф. И. О., год рождения, паспортные данные, включая прописку и место рождения);
- фактическое место проживания;

- контактная информация;
- данные о военной обязанности;
- данные о текущей трудовой деятельности (дата начала трудовой деятельности, кадровые перемещения, оклады и их изменения, сведения о поощрениях, данные о повышении квалификации и т. п.).

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;
- сведения о социальных льготах;

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

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

1.6. Персональные данные работников и пациентов 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 работников и пациентов медицинская организация руководствуется настоящим Положением, Конституцией РФ, Трудовым кодексом РФ, иными федеральными законами.

1.8. Медицинская организация разрабатывает меры защиты персональных данных работников и пациентов.

1.9. Работники и пациенты не должны отказываться от своих прав на сохранение и защиту тайны.

2. Хранение, обработка и передача персональных данных работника

2.1. Обработка персональных данных работников осуществляется исключительно в целях обеспечения соблюдения законов и иных нормативных правовых актов, содействия работникам в трудоустройстве, обучении и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы и обеспечения сохранности имущества.

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

2.2. Персональные данные работников хранятся в отделе кадров, в сейфе на бумажных носителях: трудовая книжка, личная карточка и на электронных

носителях с ограниченным доступом.

Персональные данные пациентов хранятся в [**вписать нужное**] на бумажных носителях и электронных носителях с ограниченным доступом.

Право доступа к персональным данным работников имеют:

- руководитель медицинской организации;
- начальник отдела кадров медицинской организации;
- сотрудники отдела кадров.

2.3. Начальник кадровой службы 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 работников и пациентов третьим лицам, только если это необходимо в целях предупреждения угрозы их жизни и здоровья, а также в случаях, установленных законодательством.

2.5. Медицинская организация осуществляет передачу персональных данных работников и пациентов только при наличии согласия указанных лиц на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.6. Согласие работника или пациента на обработку персональных данных, разрешенных им для распространения, оформляется отдельно от иных согласий субъекта персональных данных на обработку его персональных данных.

2.7. Медицинская организация обязана обеспечить работникам и пациентам возможность определить перечень персональных данных по каждой категории персональных данных, указанной в согласии на обработку персональных данных, разрешенных субъектом персональных данных для распространения.

2.8. Молчание или бездействие работника или пациента ни при каких обстоятельствах не может считаться согласием на обработку персональных данных, разрешенных им для распространения.

2.9. В согласии работника или пациента на обработку персональных данных, разрешенных им для распространения, работник или пациент вправе установить запреты на передачу (кроме предоставления доступа) этих персональных данных медицинской организацией неограниченному кругу лиц, а также запреты на обработку или условия обработки (кроме получения доступа) этих персональных данных неограниченным кругом лиц.

Отказ медицинской организации в установлении работником или пациентом запретов и условий, предусмотренных настоящем пункте, не допускается.

2.10. Медицинская организация в срок не позднее трех рабочих дней с момента получения соответствующего согласия работника или пациента публикует информацию об условиях обработки и о наличии запретов и условий на обработку неограниченным кругом лиц персональных данных, разрешенных этим работником или пациентом для распространения.

2.11. Установленные работником или пациентом запреты на передачу (кроме предоставления доступа), а также на обработку или условия обработки (кроме

получения доступа) персональных данных, разрешенных им для распространения, не распространяются на случаи обработки персональных данных в государственных, общественных и иных публичных интересах, определенных законодательством Российской Федерации.

2.12. При передаче персональных данных работников и пациентов медицинская организация предупреждают 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.

2.13. Иные права, обязанности, действия работников, в трудовые обязанности которых входит обработка персональных данных работников и пациентов, определяются должностными инструкциями.

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

2.15. Начальник кадровой службы обязан предоставлять персональную информацию о работниках в пенсионный фонд, фонд обязательного медицинского страхования (ФОМС), фонд социального страхования (ФСС) по форме, в порядке и объеме, установленных законодательством РФ.

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. Определение уровня специального оборудования помещения осуществляется специально создаваемой комиссией. По результатам определения класса и обследования помещения на предмет его соответствия такому классу составляются акты.

3.4. Кроме указанных мер по специальному оборудованию и охране помещений, в которых устанавливаются криптографические средства защиты информации или осуществляется их хранение, реализуются дополнительные требования, определяемые методическими документами Федеральной службы безопасности России.

4. Обязанности медицинской организации по хранению и защите персональных данных работников и пациентов

4.1. Медицинская организация обязана за свой счет обеспечить защиту персональных данных работников и пациентов 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 работников и пациентов только в соответствии с настоящим Положением и

законодательством РФ.

4.5. Медицинская организация обязана предоставлять персональные данные работников и 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.

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

В случаях, непосредственно связанных с вопросами трудовых отношений, медицинская организация вправе получать и обрабатывать персональные данные работников о их личной жизни, только с письменного согласия работников.

4.7. Медицинская организация не имеет права получать и обрабатывать персональные данные работников о их членстве в общественных объединениях или профсоюзной деятельности, за исключением случаев, предусмотренных законодательством РФ.

4.8. Медицинская организация не вправе предоставлять персональные данные работников и пациентов в коммерческих целях без их письменного согласия.

4.9. Медицинская организация обязана обеспечить работникам и пациентам 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 работников и пациентов предоставить им полную информацию о их персональных данных и обработке этих данных.

5. Права работников и пациентов на защиту их персональных данных

5.1. Работники и пациенты 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 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 работников и пациентов, работники и 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 работников и пациентов, обо всех произведенных в них исключениях, исправлениях или

дополнениях.

5.2. Если работники и 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.

5.3. Работник или пациент вправе обратиться с требованием прекратить передачу (распространение, предоставление, доступ) своих персональных данных, ранее разрешенных им для распространения, к любому лицу, обрабатывающему его персональные данные, в случае несоблюдения положений Федерального закона или обратиться с таким требованием в суд.

6. Порядок уничтожения, блокирования персональных данных

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

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

6.3. В случае подтверждения факта неточности персональных данных медицинская организация на основании сведений, представленных работниками и пациентами, 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 поступления требования работника или пациента о прекращении распространения его персональных данных передача (распространение, предоставление, доступ) персональных данных, разрешенных таким работником или пациентом для распространения, должна быть прекращена в любое время.

Действие согласия работника или пациента на обработку персональных данных, разрешенных им для распространения, прекращается с момента поступления в медицинскую организацию указанного требования.

6.5. 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.

6.6. 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.

6.7. Об устранении допущенных нарушений или об уничтожении персональных данных медицинская организация обязана уведомить работников и пациентов.

6.8. 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.

6.9. В случае отзыва работниками и пациентами 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, если иное не предусмотрено трудовым договором.

6.10. 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 работников и пациентов

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

7.2. Моральный вред, причиненный работникам и пациентам 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 работниками и пациентами 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.